A Guidebook for Electronic Court Filing

Authors

James E. McMillan
Senior Technology Associate
Director, Court Technology Laboratory
National Center for State Courts

J. Douglas Walker
Acting Director of Technology
National Center for State Courts

and

Lawrence P. Webster
Director of Administrative Office of the Courts, Delaware
(formerly, Executive Director of Court Technology Programs,
National Center for State Courts)

ISBN 0-314-23340-7

This Guidebook was developed by National Center for State Courts staff under a contract with West Group, Inc. Points of view expressed herein are those of the authors and do not necessarily represent the official position or policies of either the National Center for State Courts or West Group, Inc.

Table of Contents

Chapter 1: Introduction

Welcome to the national dialogue on the role of electronic filing in court automation. You are about to embark on a process of planning and implementation that promises dramatic savings and improvements in the work of the courts and the practice of law. This guidebook can help you answer questions, frame the issues and prioritize your next steps as you lead your courts into the 21st Century.

What Does this Guidebook Cover?

Electronic filing is far more than a single new technology, and for this reason, the amount of work required for implementation is far greater than most court leaders imagine. Eventually, every clerical and judicial task that relates to information about cases, and many that do not, will require reengineering.

This guidebook has been created to assist courts leaders with this huge yet exciting challenge, specifically to:

- Explain electronic filing.
- Create a strategic vision and enthusiasm for electronic filing.
- Describe the technical requirements and policy issues.
- Document the implementation process leading to success.
- Create realistic expectations about the journey ahead.

Who Should Study this Guidebook?

This guidebook is written primarily for policy makers in the court, government and law firms who must decide if, when and how to begin electronic filing. It is written for the lawyers, administrators, technologists, judges, and others charged with making it happen.

This document is a publication of West Group, Inc., and was prepared primarily by staff of the National Center for State Courts. It is divided into seven main sections, with supplementary materials added. The main sections describe:

- How to sell the electronic filing concept.
- How court rules have been developed in various parts of the country to support this work.
- How electronic filing affects document workflow.
- The technology infrastructure needed to make it succeed.
- How to budget for an electronic filing project.
- Steps in the implementation process.

Appendices have been added to provide further information about the laws, court rules and regulations that have been developed to move courts in the direction of conducting business electronically, and to show the data often needed with documents arriving at the court.

Starting the Journey

This guidebook takes a step-by-step approach to electronic court filing. As a first step, we should define in general terms *"What is electronic filing?"*

> **Definition.** Electronic filing is the process of transmitting documents and other court information to the court through an electronic medium, rather than on paper. Electronic filing lets people get more of their work done with their PCs, to send and receive documents, pay filing fees, notify other parties, receive court notices, and retrieve court information.

Today, most attorneys prepare documents with word processing software, print them out and have someone carry them to the courthouse with the appropriate court fees and instructions. Once at the court, staff reviews the paper pleadings, processes payment, makes entries into the case management system database, and places them in the file jacket for the case. The case files are routed to the appropriate judge or staff for processing. Eventually the documents may be routed to appellate courts or to archives.

With electronic filing, the document is prepared in the same way by filers, but *sent* electronically. The attorney then transmits the word processing and other computer files to the court through a dial-up modem, leased line or the Internet using electronic mail, or uploaded with file transfer protocol (FTP) or a World Wide Web browser. Information is exchanged with the computer case management system programmatically. The information is retained, organized by case and routed to court staff, but all of the work is done directly on computer screens, rather than by referring to paper documents. Electronic filing eliminates the time and cost of paper handling.

What Generally Are the New Requirements for Courts?

An important component of electronic filing is the document management system. This is the place where electronic pleadings are stored. It doesn't make sense for a court to accept documents electronically if it is not prepared to use them in their electronic form. If the court were to establish electronic filing without a document management system, it would simply transfer the expense of printing from the law firms to the judiciary.

In theory, it would be possible to operate a document management system without electronic filing in place, but this would entail a tremendous expense in scanning each page submitted to the court. Electronic filing and a document management system go hand in hand; one cannot exist without the other.

In the same manner, a modern case management system also is required. Case management systems currently are responsible for tracking all cases, documents, filing fees, judge and jury assignments, just to name a few of the features available with modern case management. These systems generate statistical and financial reports that

assist with court administration. Unfortunately, all of the data must be typed into these systems by hand. Not only is the work redundant, but it can introduce inaccuracies from input errors.

In an electronic filing environment, the case management and document management systems must be integrated. Data can be shared between these systems without re-keying.

The benefits of this integration include significantly faster and more accurate access to case information. For example, while it will be possible to perform text searches in the document management system to find papers, using this approach exclusively could prove inefficient because the same data formatted for document retrieval may exist in many other pleadings. In other words, every attempt to find a specific paper would produce multiple documents. The user would be required to sort through them to find the correct one. The case management system addresses this concern and provides a retrieval mechanism that serves as an index to the documents.

Case management systems are therefore another cornerstone component of the new information management and retrieval mechanisms, which must be in place lest electronic documents have no value.

Other systems and technical components necessary for electronic filing are described in this guidebook. Just as important as the cables and boxes, however, are the people required to manage, provide customer training and support, and keep the system operational. This guidebook gives equal importance to the staff, policy and technical aspects of electronic court filing.

Where Is Electronic Filing Today?

If electronic filing is so great, why aren't we all using it? The answer is that many small projects have been initiated in the United States. Unfortunately, most have either failed, been terminated or are defined as "requirements definition" projects for future systems. None have delivered a sufficient bottom-line gain to court efficiency to command support for funding the necessary infrastructure.

The primary problems relate to the technology. While many of the components of electronic filing have been available for some time, the lack of standards, difficulty of integration, insufficient training and customer support, and equipment and software costs have been limiting factors. In the last few years, the power and cost of personal computer technology have improved significantly. Data storage costs have dropped from more than $1,000 per megabyte on early PCs, to less than five cents per megabyte today. This price is dropping about 50 percent each year. Only a few years ago there was no universal communications network, with standard protocols and interfaces, available to link our systems together. Even today, security and scalability issues on the Internet have not been completely resolved.

Display technology limitations, another significant barrier to successful, large-scale implementation of electronic filing, still exist in the nation's courts, but hopefully will be solved soon. The resolution of today's PC monitors is not high enough to display a printed page in readable form. The size and weight of the monitor restricts it to a fixed location, making the viewing of lengthy documents on the screen almost impossible. While liquid crystal display panels are an attractive alternative that will solve many of these problems, they lack the high resolution needed and still are far too expensive to be

practical. Planners should therefore expect that a significant amount of printing may be done for judges and members of the public.

At the forefront of all the technology will be the people that manage and facilitate these systems. Encouraging progress has been made in understanding that electronic filing is not solely about technology. Like any other service, it involves marketing, training, customer support, value-added benefits, and good working relations with the providers of court technology.

Share the "Vision" of Electronic Court Filing

Electronic filing is not just a new technology; it is a revolutionary approach to conducting court business that will change the way courts work in the future. For example, when all the papers in a case are available as searchable text, it will be possible to integrate these documents with databases of legal precedent, courtroom testimony and evidence in its electronic form. This will allow the creation of sophisticated decision support systems.

The nature of documents also will change. With paper as a medium, documents are designed to be read from beginning to end. In the future, electronic documents might be prepared in layers accessible through hypertext links. Readers can *drill down* to view further detail if they don't understand something or if they disagree with something they read. Conversely, if a judge is familiar with aspects of a case, he or she can skip over this detail and evaluate the arguments at a higher level. Footnotes will be links to other documents that are immediately accessible, even though they may be stored in other parts of the world. Concepts such as these reflect the rightful optimism of those who have championed electronic filing for the past decade.

Moreover, even before the strategic implications of electronic filing are fully realized, there are many near-term tactical advantages to be gained by adopting the technology. Most costs associated with paper handling and storage are eliminated. Case materials are instantly accessible and protected from loss or destruction. Court employees who work with the records will find that more time can be directed to other tasks once paper handling is eliminated. Attorneys will save time and the costs of transporting materials to the courthouse. In addition, they will have greater access to court materials stored in electronic format. Finally, document processing will be easier to manage, resulting in greater productivity and effectiveness in doing the court's work.

Just as the advent of court automation created opportunities for the development of sophisticated caseflow management techniques, electronic filing will make similar feats possible with document processing. These new techniques, called workflow in their present form, have shown themselves to be far superior and less costly in courts that are already using them. With appropriate staffing and training, courts can transition quickly to this new model of delivering service internally and to the public.

In all, the benefits of electronic court filing appear dramatically large for the leaders ready to take the necessary steps.

Chapter 2: Selling the Idea

Electronic filing often initially is perceived as an entirely new technology. Because of the mixed track record of previous automation efforts, it may be difficult for many courts to acquire funding and support for something seen as a bold, unproven venture. In addition, courts usually have many existing needs already competing for scarce funding and support.

The purpose of this chapter is to provide practical and realistic information to help a court promote a plan that satisfies the needs and goals of all constituents. A clear, explicit approach will help to persuade key facilitators to lend support, convince funding bodies to allocate resources to the project, encourage the providers of the necessary products and services, and recruit law firms to serve as partners in the endeavor. Courts should prepare and implement a marketing strategy for their plan.

Define the Audience for Your Plan

Your audience includes those who pay for, support, promote, and use electronic filing. Remember that funding is only part of the equation. Rules and statutes may require modification. Take a moment to create a checklist of the groups and individuals that should have a clear understanding of your goals. The list may include:

- The clerk of court.
- Judges and judicial committees.
- Court administrators.
- Current technology staff.
- Local and state legislators.
- Attorneys.
- Suppliers of products and services to courts.
- The public.

Complete this checklist by deciding what stage of the process involves which of these participants. For instance, depending on your situation, selecting a vendor to supply components of these systems may be perceived as premature, or it may help speed things up by showing the interest your project has generated in the market.

Understand the Dynamic of Your Audience

It is important to understand that individuals within each of these groups will likely react to your plan based on their perception of the risks involved. Some will be enthusiastic about using technology – any technology -- to try to solve problems. Others will be skeptical about the ability of technology to increase efficiency. A few may initially see electronic court filing as a threat to the status quo under which they prosper, and they may work subtly to derail the project. Most, however, will simply want to be convinced that the project can be completed within the planned budget, that existing operations will not suffer during the transition, and that the projected benefits are likely to be achieved.

Using the technology options and financial plans developed through this guidebook, you should be able to articulate clearly the projected impact, timeframes and savings to these groups.

Be Specific about Your Current Costs of Operations

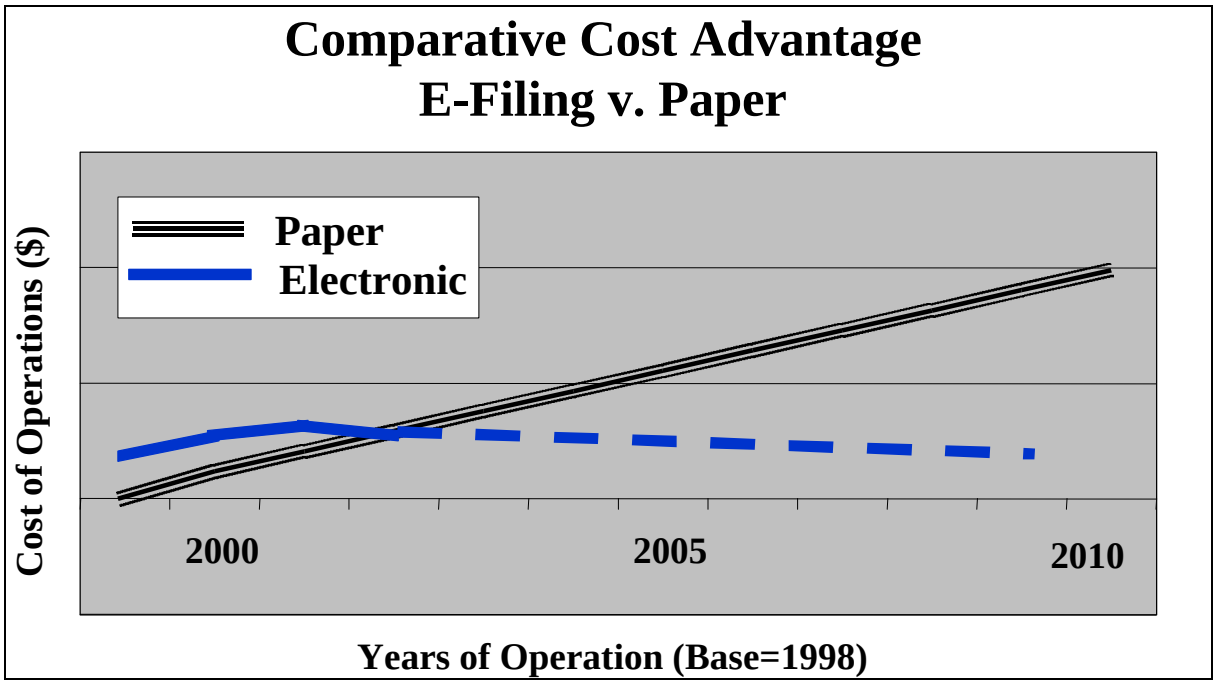
Technology generally receives a significant share of the non-personnel budget today, but existing case management systems, personal computer networks and computer systems also require resources and staff to keep them running. Because electronic filing is a supplement to, rather than a replacement for, a case management system, it is important that there be sufficient funding available to support all of this work.

Also, current staff levels and work classifications need to be charted, and projections made for future operations both with and without electronic filing. All changes that can be reasonably anticipated to occur should be clearly described, including growth in case loads and increases in *pro se/pro per* filings.

Be Specific about Projected Benefits

If the court is prepared to initiate an electronic filing project, the next step is to persuade those who will supply funding. Legislatures, county commissions, boards of supervisors, city councils, or whatever group makes budget decisions should be involved in studying the need for the technology. Most often funding bodies are convinced to provide resources if they see the court studying the issues methodically and making rational choices, rather than if they perceive the court to be on a quest to acquire the latest technology toys.

Selling the idea of electronic filing will require making assumptions based on facts, leading to projections that show the long-term cost advantage of replacing the paper-based process with electronic filing. The following chart shows this projection by contrasting the cost of a paper operation with that of an electronic filing front-end feeding into the case management system.



The chart should be regarded as illustrative only, as circumstances and related cost factors vary widely from court to court. It is based on the premise of level caseloads and reflects, for both methods of operation, non-personnel costs such as:

- Space.
- Utilities.
- Materials.
- Equipment.
- Software.
- Services.

Court managers should be able to project the actual costs of their current operation with a fair degree of accuracy. They know how much they are paying for paper, copiers, storage, utilities, and other expenses. They also can determine what those costs are likely to be in the next few years, based on information from past budgets and current trends.

When electronic filing is implemented, there is an initial increase in the total cost of operations because of the start-up expenses associated with planning, acquiring and implementing the new technology. Chapter 7 identifies the key cost categories that a

court is likely to encounter during this period, and the chart above illustrates this pattern of temporarily rising costs. In subsequent years, however, the total cost of operation begins dropping as the start-up costs are absorbed and operational efficiencies begin to have an impact. At some point the lines on the graph intersect each other, with the electronic operation costing less than the paper one. Depending upon the approach the court takes to implementation, the nature of the conversion process, and other varying factors, the crossing point could be as soon as three years after initial implementation.

While the relative costs of the two operational methods continue to diverge, the actual cost of the electronic filing operation could vary from a slight upward trend to a continual decrease over time. Constantly improving price/performance ratios for technology exert a downward pressure on overall costs. If rising caseloads are factored in and human resources expenses are included, the cost of both types of operations will rise. In that case, however, the gap widens even more dramatically, because the cost of the paper-based operations will rise much more sharply.

Maintain the Interest and Enthusiasm of Supporters

It is important that there be sufficient political support within the court for electronic filing to keep it a high priority for funding for more than a single budget cycle. It may take several years to fully implement electronic filing and to start to receive benefits from the technology.

Explain Benefits to External Users

A major group that needs to be convinced of the value of electronic filing is the attorneys who will be primary users of the system. Often, this is the group that encourages the court to explore the technology, though when presented with the hard

realities of implementation, maintaining a high level of commitment and enthusiasm in this group is not so simple.

It is critical that those law firms who will participate in electronic filing projects be involved in policy discussions and system design, vendor selection and project implementation at every step. Based on early pilot tests of electronic filing, a court that believes it can order attorneys to adopt its technology standards will not succeed. Law firms will expect to be provided with a clear explanation of benefits (i.e., "marketing"), opportunities to receive regular staff training at their firms at convenient times, fast-reliable customer support, and integration with the technology systems that they have in their firms. The law firms should be partners with the judiciary in developing and deploying electronic filing technology.

Explain the Risk Factors

Before promoting your plan, identify as many risk factors as possible and develop plans and alternatives to minimize their impact. Examples of risk factors are those that arise from the technologies and vendors chosen, the new requirements on court staff, the effect of possible changes in project staff or loss of project proponents, and the impact of funding changes.

For instance, depending on the amount of technology and services the court chooses to manage in house *versus* outsource, a court may need to give careful consideration to whether the court can attract and keep necessary technical staff, customer support staff, training staff, marketing staff and so forth.

Promoting the plan also requires investigating other e-filing projects that have been undertaken and determining, for example, whether the court might expect delays in start

up, and inadequate attention to potential users, to be significant contributing factors to the failure of many projects.

Articulate the Goals

An electronic filing project should expect to demonstrate new efficiencies in court administration, and fully leverage investments in computerized back office technology such as case management systems to better serve internal users. The goals also should include designing an approach to electronic filing that gives filers the range of service choices they have today, but with optional computer-based efficiencies. For instance, courts can expect to work with their constituents, existing technology providers and their partners on the following goals:

- Provide e-filing/retrieval access to many divisions of law.
- Ensure security of court back office.
- Utilize advanced architecture and integrate disaster recovery.
- Ensure accurate and timely electronic court fee payment.
- Maintain high availability and accuracy of filing confirmation.
- Require quality support and service.
- Include government agencies needs in development process.
- Develop open standards for electronic filing and retrieval.
- Develop the appropriate *pro se* e-filing modules and the appropriate exceptions to mandatory e-filing.
- Maintain the high quality of services provided today.

Customize a Model Business Case to Your Court

A plan for electronic filing is basically a "business case," outlining cost *versus* return, risk *versus* benefit. A clear business plan can be used best to convince the constituent groups of the value of the technology, which can be built in several parts. First, it is necessary to explore the benefits of electronic commerce to the courts, the attorneys using it, the parties involved in cases, and the citizens of the state, and their representatives, who must pay for the system. Second, it is important to assess the technology and

services that are available for implementation, and the vendors that supply it. In most cases, there are several alternative approaches to implementing electronic filing. Each should be explored. Third, it is essential to document the life cycle costs of the specific approach or approaches under consideration. With a complete business case, the court is in a better position to sell the project internally and externally. The remainder of this chapter will explore some components of this business case in more detail.

Benefits of electronic filing

A case management system contains only a small amount of important information about a case. This data allows certain functions to be performed, like generating calendars, monitoring caseload growth and tracking restitution payments.

An important component of electronic filing is the document management system, the database of pleadings and other papers prepared by or submitted to the court. When a document management system exists, all case papers and case information is available and searchable electronically. Instead of storing a small fraction of the information from a case file, the document management system makes everything available.

Although the benefits of electronic filing in the justice system need to be categorized in many ways, this section will view the multiple advantages as they relate to documents, staff, attorneys, and management issues.

Documents

Most courts, particularly large ones, expend significant resources on file management. This includes creating files, pulling and filing case jackets for court events, placing new documents in file folders, maintaining indexing systems, monitoring the location of files as they are used by various individuals, purging, microfilming, and

archiving. An important benefit of electronic filing is that all of these activities are eliminated or streamlined.

Storage space, as will be shown later in this document, is expensive. New courthouses are now being built for more than $300 per square foot in some parts of the country, and leased space can run well over $15 per square foot annually. Electronic filing eliminates much of the paper in the courthouse, and changes the retention methods and timing for that which remains. For example, the court may still receive papers from parties, but can scan them and store them by date received, rather than being required to track down the case file in which to place them. At the same time, security of records is higher in an electronic system, since no user ever has physical custody of a pleading. Wear and tear on papers and folders also is eliminated, since a digital document does not deteriorate with use.

Staff

Electronic filing eliminates redundant work. In today's systems, an attorney places information in a document and sends it to the court. A clerk reads the paper and records the information in a computer system. In an electronic system, the attorney's keystrokes are transferred to the court's computer, and never have to be repeated. This results in less data entry to support court clerical operations.

Courts that have experimented with imaging technology have documented the tremendous price of paper handling.[1] With electronic filing, since most of the paper is eliminated, so are paper handling costs.

[1] See Lawrence P. Webster and James E. McMillan, Document Imaging in the Orange County, California Superior Court Probate Department: An Evaluation (Williamsburg, National Center for State Courts, 1993).

Another benefit of electronic filing is workflow. Once the court stores documents electronically, it is possible to route them to the appropriate staff immediately, eliminating processes that can add many days to the life of a case.

Attorneys

Electronic filing helps attorneys get documents to the courthouse more quickly. Many steps in the process, such as printing and transporting papers, are eliminated, saving time and money. Postage costs also are reduced, particularly when service also can be completed electronically.

Because the court has an electronic case file, the attorney can access it without leaving his or her office. This may result in the elimination of many paper records in law firms. With the access mechanisms that allow attorneys to see court case files, they also should be able to view calendars and other important records. Many individuals can access these materials simultaneously from different locations, a feat that is impossible in a paper environment.

Court management

In addition to work saved by eliminating some of the data entry associated with document filing, other tasks will be removed because the amount of data collected in case management systems will be reduced. Why transfer information from a document to a case management system if the document is available electronically?

When documents are routed electronically, it will be possible to create workflow paths to increase the efficiency and effectiveness of the entire system. Just as computers enabled court administrators to develop sophisticated case management techniques, like differentiated caseflow management (DCM), electronic filing will allow more intricate control over document processing. For example, the same type of document could follow

many different paths through the courthouse, depending on the data it contained. The processing paths also could be reengineered to reflect the improved capacity of staff using the computer tools.

Another benefit of the automation of any process is increased effectiveness. Once information has been converted to an electronic form, it can be used for other purposes. This will allow courts to provide new services and functions that would not have been practical prior to electronic filing.

As imaging systems have demonstrated, document and workflow management data can be used to monitor staff productivity more carefully. It is possible, though not always desirable, to measure the number of seconds a clerk spends on each step of a document processing activity. This can have many benefits for management purposes, including fine tuning of work processes and disciplining of court employees who are not as productive as their peers.

Technology assessment

Five factors should be considered when assessing the value of any technology.[2] They are time, cost, availability, risk, and value.

Time

Time is the most critical element of the technology life cycle. Some technologies have value to courts for years or generations, while others may become obsolete within months. Cost, risk and availability also change over time at varying rates. Despite variations in duration, most technologies pass through similar stages. Court leaders never should purchase equipment or software, or select a technology strategy, without a clear understanding of its life expectancy.

Cost

Cost is the most commonly recognized factor in choosing a technology option. Because courts usually cannot afford the latest and greatest innovations, they often settle for lower-cost, smaller, slower, or older alternatives. Court managers often over-emphasize purchase price and ignore more significant expenses; that is, operational and management costs of the technology through its useful life. In assessing technology options for electronic filing, judicial branch leaders should estimate all costs through the expected period of use, not just the price of acquisition. All costs associated with people, space, supplies, and effects on other court work must be considered.

The cost of a technology is usually highest in the early stages of its life cycle. As development costs are recovered, production volume increases and competitors produce similar products, vendors cut prices. As new alternatives appear, the cost may drop dramatically as demand for the product disappears. Finally, as others stop using the equipment or software, maintenance and operational costs may increase as trained personnel and replacement parts become scarce.

Risk

Risk is the probability of success of implementing and using the technology. Excessive risk taking with emerging or aging technologies can lead to failure. It is important to review projects undertaken by other courts, particularly for a new technology like electronic filing. As others gain experience, risk declines. As a technology nears the end of its useful life, risk begins to increase again because of a growing chance that support may not be available.

[2] Lawrence P. Webster, *Automating Court Systems* (Williamsburg, National Center for State Courts, 1996).

Availability

Availability is a serious problem with very new or very old technologies. Those who have waited months for a product to arrive, after being told by a salesperson that it would ship within days, know these frustrations and headaches. Availability can be a problem very early and, to a lesser extent, very late in the lifecycle.

Value

Value is the most important factor in assessing technology. If a program or product will do the work of the court effectively and efficiently, it does not need to be the latest and greatest option. Too many courts have spent exorbitant amounts of money on enchanting technologies that have not delivered.

The technology life cycle

The technology life cycle consists of four stages: the *future stage*, the *emerging stage*, the *existing stage*, and the *obsolete stage*. While the length of time in any stage will vary, each technology will pass through every stage.

Future technologies are those that are not yet available to the court or other organizations. Cost and risk are not factors, and value may be very high because no one has discovered any problems yet.

Emerging technologies are those that have found success in other organizations, but not in courts. They are usually experimental and expensive. Many less than satisfactory attempts at implementation usually precede a successful application, so risk is very high. As with future technologies, the perceived value of emerging technologies may be inflated due to a lack of experience with the new tools' shortcomings. All of the pieces necessary for successful implementation in a court may not be available.

Existing technologies are those that have found widespread acceptance and use in courts. Most of the difficulties accompanying their installation have been identified and resolved. Costs of these technologies normally decline over time. Availability is high and risks are low.

Obsolete technologies are those that have not adapted to a changing environment or have been superseded by better and more cost-effective alternatives. They are usually inexpensive and carry little risk, other than their short life expectancy.

In general, electronic filing must be considered an emerging technology. Electronic filing systems include a variety of components, e.g., file servers, firewalls, document management software, that individually may cover the full range of the life cycle. Courts should assess every major technology component of their electronic filing project. It doesn't make sense, for example, to try and tie state of the art document management software to an obsolete case management system. In reviewing options, it is advisable to compare the advantages and disadvantages of using service providers for certain parts of the process, much as courts currently rely on the post office and telephone companies in the paper-based world.

Approaches to electronic filing

There are many options to consider when designing an electronic filing system. The computing environment, financial and technical resources, and capabilities of major law firms will dictate some of the choices, so it will not be necessary to assess the hardware and software for all of these methods.

Some of the earliest electronic filing systems used bulletin board software and word processing documents. Users dialed in to the bulletin board and uploaded papers to be

filed for their case. Service, or notification of filing, was accomplished with electronic mail or facsimile.

Another approach is to use personal computer forms packages to generate an electronic cover sheet, to which a word processing document is attached. This provides data for the case management system without keying at the courthouse.

Still another approach is to provide data and documents through electronic mail or work group software. This method can be used in either a private network, or over the Internet.

Still another method, one that may be most attractive presently, is to file documents through the World Wide Web. Browsers can be used as a standard interface, and web-based forms can provide data capture.

Another avenue for filing electronic documents is through kiosks. These multimedia devices allow individuals to receive detailed computer-based assistance in completing and submitting their forms.

A final technique can be combined with several of the approaches listed above to provide formatted data to the case management system that serves as an index to the documents. Tags can be placed on information in the document to identify specific items. These tags are applied in the same manner as one would apply bold, underline, or italic format to a word processing font. The tags would be invisible to the user, but could identify party and attorney names, cause of action, filing date, and other discrete variables needed to populate a database.

Costs of electronic filing

A certain amount of work must be performed whenever information is submitted to the court. It must be read, analyzed, stored, acted upon, and perhaps distributed to others.

This will occur regardless of the medium of exchange, paper or electronic documents. A tremendous amount of work also is required to process the medium, rather than the data. Many of the costs of handling paper are distinguishable from the expenses associated with processing the information it contains. Electronic filing eliminates most of the paper-handling expense. Of course, there are also tasks and costs associated with processing electronic media, but they are typically much lower than for paper. All are part of the cost equation.

As has been mentioned, courts should attempt to document the life cycle costs of components of their electronic filing systems. A solution that costs less initially may cost much more over its useful life.

Components

In general, the court needs a good case management system that can function as an index to documents. A document management system also is necessary. In theory, it would be nice to have the document management system in place and working well before initiating electronic filing. In the real world, most courts cannot afford to manage electronic documents without electronic filing. The paper handling costs are just too high.

Integration of case and document management is necessary. Experience with imaging technology has shown that if the document management system has its own index, then data storage, and possibly data entry, will be duplicated and the systems will never get synchronized.

The electronic filing components that are “behind the scenes” are essential. Though there are other options, this is typically a server (server hardware and server software), or

group of servers, inside and outside of the court security firewall that accepts and does initial processing of the documents.

The other critical component is the network connection to the outside world. This can be a private network or regular phone lines with dialup modems, but the Internet has become a superior choice in almost every circumstance. Courts and their electronic filing service providers should expect to support the user interface with a World Wide Web browser.

The chapters that follow, particularly Chapter 7, will provide specific information for compiling costs for each of these components.

Summarizing the Project Plan

With a clear business case, a court demonstrates that it has given consideration to all realistic approaches that can deliver the benefits of electronic filing to users in law firms, the public and the court. The plan can best be promoted if it can be well summarized.

In summary, there are three basic models for electronic court filing: (1) out-source everything; (2) build and support everything internally; and, (3) maintain tight operational control over the Court's data and technical infrastructure and also encourage private industry to promote new filing/retrieval software services to the public.

Analysis: Outsource All Functions

Most courts in the United States are capable of managing and operating a modern, complex information system for internal users (judges, judicial assistants, and clerks) and providing some information access to external users. Given the critical importance of accurate and reliable court record keeping, most courts today cannot justify "out-

sourcing" these core functions, even if they acquire the software from a commercial vendor.

Analysis: Build and Support Everything

At the same time, however, since courts are not software companies, they are not as well suited to developing and supporting software for private and public attorneys and other citizens.

Based on their frequency of filing, and on their legal specialties, filers will need specialized applications to prepare and submit filings and court fees, to conduct service of process, to electronically retrieve and pay for documents, and perform the many other tasks associated with court filing.

Nor can courts manage the integration of such tools into other law office technologies, such as time and billing systems and attorney case management systems. These realities suggest that many courts will conclude that the resources required to "do everything" are beyond the necessary and appropriate levels required by their Government function. Some well funded courts, however, could probably undertake large parts of these projects.

Analysis: Focus on Core Court Information Systems, Encourage Service Providers

Courts should also conduct research in the marketplace to determine whether the private sector has a new service businesses to develop and support electronic filing/retrieval – connected to, but outside of, a court's own highly secure infrastructure. In such an arrangement, Courts retain operational control over critical data management functions, such as the case management system and the courts document management system.

Under this type of approach, some courts will conclude that the court and the filing community will benefit by attorneys and citizens having high quality software and customer support available from private companies for document filing and document/information retrieval. Just as courts do not pay couriers to bring paper documents for filing today, courts would not pay to bring documents to its "electronic filing counter" tomorrow. This approach will provide clear separation and security for the Court's systems while encouraging rapid rollout of e-filing.

Conclusion

Considerable experimentation will occur in the area of electronic filing over the next couple of years. Some courts will purchase the equipment and hire the staff to build, promote, sell, and support electronic filing from the courthouse. Others will outsource everything.

It has been a common goal of courts to establish some standards in this area. These standards will begin to emerge based on successful projects in the future. Many courts likely will conclude that the most appropriate approach is to secure and enhance their internal computer operations and then create an "electronic filing counter" at which potentially many electronic filing service providers deliver filings and court fees, and pick up and disseminate court documents and notices.

Regardless of approach, courts that develop a comprehensive plan explaining why they are taking a particular approach will most likely reach their project goals.

Chapter 3: Court Rules

State statutes, administrative agency regulations, court rules, and administrative operating procedures help define interactions within and between litigants, courts, and other governmental entities. In the past, these statements of policy have been narrow and specific with respect to court operations, assuming that parties, attorneys, court staff, and elected officials required a great deal of help in playing their parts in the judicial process. These writings also assumed a stable court environment, with minimal and infrequent changes in practice.

In most states, circumstances have changed significantly in the last few decades. Greater specialization of staff, judges, and attorneys; a better-educated workforce; professional administration; higher caseloads and increasingly more complex cases; modern case flow management techniques; and rapidly evolving technology tools have contributed to a more sophisticated and dynamic judicial system. More is changing in our nation's courts than at any time in the past, -- and such change is rapid.

Rules designed to ensure consistent state-of-the-art management of judicial activities have become impediments to change and productivity. Perhaps most troubling is the degree to which state legislatures are responsible for procedural minutiae and administrative trivia in court operations. For example, some state statutes still define the precise nature of paper records (and entries on those records) to be maintained by a clerk, including docket books, paper ledgers, indices, fee books, etc.

Fortunately, many state legislatures have made great strides in allowing the judicial branch to manage its own internal operations in a progressive and efficient manner. These states are repealing the archaic and repressive statutory controls over internal court

procedures and replacing them with broader statements of policy, leaving the details of implementation to the judiciary.

Whether maintenance of rules governing judicial branch operations is the responsibility of a legislature, supreme court, judicial council, or local court, a great deal of work may be required to ensure that these rules are an asset, rather than a barrier, to implementation of an electronic filing system. Courts across the nation have been experimenting with various types of technology, and these activities often include the implementation of new or modified rules. Appendix B contains a summary of rules related to electronic filing, organized by topical category. Appendix C contains a similar summary organized by state. The purpose of this chapter is to outline some of the areas that have been or should be addressed by court rules, to show the response to this need in different locations, and to recommend action for court leaders. The widely varying environments will dictate different approaches from state to state, but the materials provided here should save a considerable amount of work and reinventing of the wheel.

The most important point made in the sections that follow is to ensure that new legislation, rules, and operating procedures are flexible. It is assumed that the accelerating pace of change will continue to challenge court leaders for many years to come. To replace an archaic rule about minute orders with one that requires the use of a specific word processing package or document format is to guarantee that the issue must be addressed again in the near future. On the other hand, an approach that specifies the content of the document and the order of presentation of materials can survive a transition through several generations of office automation technology.

The remainder of this chapter covers thirty-three topics, listed below. For each area, there will be a description of the issues associated with the topic, approaches used in

some of the states, and recommendations based on a national view of what is working well. The materials for some topic areas are more detailed than for others because of variations of complexity in each. Appendix E contains a complete listing of the statutes, regulations, rules, and operational procedures most often cited below.

The following list represents the topic areas that comprise the rest of this chapter.

1. Requirements to develop a plan and operating procedures
2. Authorization to accept electronically filed documents
3. Specific documents only
4. Technical standards for system use
5. Agreements between courts and filing parties
6. Making electronic filing mandatory
7. Specific data requirements
8. Electronic authentication
9. Digital signature
10. Requirements concerning passwords
11. Provisions concerning paper records
12. Retention schedule for electronic records
13. Exemptions from public disclosure laws
14. Public access to electronic records
15. Sealing and expungement of records
16. Collection of filing fees
17. Fees for electronic filing service
18. Electronic filing system constitutes docket and other records
19. Electronic document is written
20. Electronic document is usually deemed to be an original
21. Electronic document is conditionally deemed to be signed
22. Paper original, or follow up filing, is not required
23. Paper copy of electronic original may be used
24. Procedures for submitting electronic documents
25. Page limits on electronic filings
26. Attachments, appendices, or exhibits in different form
27. Filing time
28. Standards for organizing, identifying, and indexing documents
29. Acknowledgment of receipt
30. Electronic issuance of summons
31. Electronic service
32. Private service providers
33. Assumption of risk for system failure

Requirements to Develop a Plan and Operating Procedures

Statutes and court rules in several states address the need to plan for the implementation of electronic filing systems. Each state takes a different approach to defining how required planning should occur, but there are three main issues that are raised consistently. They are 1) why testing the technology is important, 2) what questions an experimental test of the technology should answer; and 3) how to conduct the test.

Why testing the technology is important

Several states support technology testing to "promote economic development and efficient delivery of government services."[3] There is inherent risk in implementing emerging technologies because so little is known about the benefits, shortcomings, and unanticipated consequences of these tools. Proving the technological concept, educating the court, legislative body, and the general public, and determining if there should be a regulatory role for government are among the reasons for conducting well-planned experiments. One state summarized these issues succinctly in statutory language enabling digital signatures.[4]

> **5-24-3-3 Procedural standards**
> Sec. 3. The state board of accounts shall implement a method of conducting electronic transactions using digital signatures that:
> (1) considers existing and potential technological advances and defects;
> (2) is practical, reliable, and effective; and
> (3) insures the security and integrity of electronic digital signatures.

What questions should be answered?

The planning process should ensure that the pilot test of the electronic filing technology answers several important questions. First, it is important to know if the

technology delivers the benefits that were promised, as well as any that were not expected. Second, what problems were encountered in the implementation and operation of the system? These problems should be compared to the original work plan to see if future implementation plans at other locations should be adjusted. Third, how did the cost of acquisition, implementation, and maintenance compare with original projections? A pilot test should provide more realistic estimates of the true cost of an electronic filing solution—they may be significantly different than expected. Fourth, given the strengths, weaknesses, and costs of the technology being tested, what is the value of electronic filing technology to the court?

The Maryland Rules of Procedure provide an excellent example of required planning for an electronic filing pilot project.

> **RULE 16-307. ELECTRONIC FILING OF PLEADINGS AND PAPERS**
>
> b. Submission of Plan. A County Administrative Judge may submit to the State Court Administrator a detailed plan for a pilot project for the electronic filing of pleadings and papers. After consulting with the County Administrative Judge, the Clerk of the Circuit Court, the vendor identified in the plan, and such other judges, court clerks, members of the bar, vendors of electronic filing systems, and other interested persons as the State Court Administrator shall choose, the State Court Administrator shall review the plan, considering among other things: (1) whether the proposed electronic filing system will be compatible with (A) the data processing and operational systems used or anticipated for use by the Administrative Office of the Courts and by the Circuit Court, and (B) electronic filing systems that may be installed by other circuit courts; (2) whether the installation and use of the proposed system will create any undue financial or operational burdens on the court; (3) whether the proposed system is reasonably available for use by litigants and attorneys at a reasonable cost or whether an efficient and compatible system of manual filing will be maintained; (4) whether the proposed system will be effective, not likely to break down, and secure; (5) whether the proposed system makes appropriate provision for the protection of privacy; and (6) whether the court can discard or replace the system during or at the conclusion of a trial period without undue financial or operational burden. The State Court Administrator shall make a recommendation to the Court of Appeals with respect to the plan.

[3] Code of Georgia, 50-29-12 (a).
[4] Indiana Code, 5-24-3-3.

How to conduct the test

Again, the Maryland rule is instructive with respect to procedures for testing new technology.

> **RULE 16-307. ELECTRONIC FILING OF PLEADINGS AND PAPERS**
>
> c. Approval; Duration. A plan may not be implemented unless approved by administrative order of the Court of Appeals. The plan shall terminate two years after the date of the administrative order approving it unless terminated earlier or extended by a subsequent administrative order.
>
> d. Evaluation. The Chief Judge of the Court of Appeals shall appoint a committee consisting of one or more judges, court clerks, lawyers, legal educators, bar association representatives, and other interested and knowledgeable persons to monitor and evaluate the plan. Prior to the expiration of the two-year period set forth in section c of this Rule, the Court of Appeals, after considering the recommendations of the committee, shall evaluate the operation of the plan.
>
> e. Extension, Modification, or Termination. By administrative order, the Court of Appeals may extend, modify, or terminate a plan at any time.
>
> f. Public Availability of Plan. The State Court Administrator and the Clerk of the Circuit Court shall make available for public inspection a copy of any current plan.

Mississippi adds some specific requirements with respect to electronic filing technology.[5]

> **Section 9-1-57. Plan for electronic storage system.**
>
> A plan for the storage system shall require, but not be limited to, the following:
>
> (a) All original documents shall be recorded and released into the system within a specified minimum time period after presentation to the clerk;
>
> (c) The plan shall include setting standards for organizing, identifying, coding and indexing so that the image produced during the duplicating process can be certified as a true and correct copy of the original and may be retrieved rapidly;
>
> (e) The plan shall provide for retention of the court records consistent with other law and in conformity with rules and regulations prescribed by the Administrative Office of Courts and adopted by the Mississippi Supreme Court and shall provide security provisions to guard against physical loss, alterations and deterioration; and
>
> (f) All transcripts, exemplifications, copies or reproductions on paper or on film of an image or images of any microfilmed or otherwise duplicated record shall be deemed to be certified copies of the original for all purposes.

[5] Mississippi Code 1972, 9-1-57 (a), (c), (e), and (f).

Several states provide additional requirements for testing technology. Delaware[6] and Mississippi[7] discuss promulgation and distribution of rules or operational procedures, Mississippi mentions use of industry standards and parallel paper systems,[8] and Georgia encourages public and private sector partnerships to minimize the use of public funds, implementation of user fees, and a request for proposals acquisition process.[9]

Recommendations

States with centralized technology administration and sufficient research and development funding to pay for pilot projects probably do not need specific rules to authorize pilot testing. Local courts with adequate resources and no requirement to coordinate technology projects with a state administrative office or other courts may be in a similar position. Others may be required or may elect to pursue development of a specific statute or rule to govern pilot testing of electronic filing technology.

With or without a specific policy statement, it is important to incorporate the plan elements discussed in this section that are appropriate for the court's circumstances. Good planning will encourage proper management and thorough evaluation. A well-run pilot project will answer questions about the replication and sustainability of the technology, both key issues in deciding whether to continue or expand use of electronic filing at the conclusion of the testing phase.

[6] Delaware Superior Court Rules of Civil Procedure, Interim Rule 79.1, Complex Litigation Automated Docket.
[7] Mississippi Code 1972 Annotated, 9-21-3 and 9-21-5.
[8] Mississippi Code 1972 Annotated, 9-1-57.
[9] Code of Georgia, 50-29-12 (b).

Authorization to Accept Electronically Filed Documents

Legal authority to accept digital documents is a basic requirement for an electronic filing project. Every state that has implemented or contemplated the development of statutes or rules to allow electronic filing has included some type of statement addressing this issue. Some authorize the program, others allow litigants to file documents electronically, and others enable the court to receive them. Some rules require individuals to accept court documents transmitted electronically, and others authorize a digitally signed acknowledgment of receipt. One state has a statutory provision equating legal issues surrounding electronic filing with the paper filing process.

Oklahoma vests authority for the development of electronic filing in its Supreme Court, and requires the administrative office to develop appropriate rules, as shown below.[10]

> **Section 3004. Electronic filing of documents**
> The Supreme Court is authorized to provide for electronic filing of documents in the Supreme Court and the district courts. The Administrative Office of the Courts shall promulgate rules for the filing of documents transmitted by electronic device. Rules for electronic filing must have the approval of the Supreme Court.

The Los Angeles Superior Court uses a similar, but simpler approach.[11]

> **RULE 18.00 ELECTRONIC FILING AND SERVICE**
> (a) Requirements for Electronically Submitted Documents. A litigant or the litigant's attorney may file an electronic document in a case via an electronic filing service…

Washington state goes a step further, requiring organizations and individuals to accept electronic documents as if they were prepared on paper.[12]

[10] Oklahoma Statutes, Title 20, section 3004.
[11] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.
[12] Revised Code of Washington, 19.34.321.

> **19.34.321. Acceptance of certified court documents in electronic form--Requirements--Rules of court on use in proceedings**
>
> (1) A person may not refuse to honor, accept, or act upon a court order, writ, or warrant upon the basis that it is electronic in form and signed with a digital signature, if the digital signature was certified by a licensed certification authority or otherwise issued under court rule. This section applies to a paper printout of a digitally signed document, if the printout reveals that the digital signature was electronically verified before the printout, and in the absence of a finding that the document has been altered.

An interesting addition to Washington's Electronic Authentication Act explicitly requires that business transacted electronically be treated the same as if conducted with paper, with respect to certain legal issues.[13]

> **19.34.503. Jurisdiction, venue, choice of laws**
>
> Issues regarding jurisdiction, venue, and choice of laws for all actions involving digital signatures must be determined according to the same principles as if all transactions had been performed through paper documents.

Recommendations

Authorization to accept electronic filings, whether implemented by statute or court rule, is a requirement in every state that has contemplated this type of project. Most of the variations are in how those filings will be transmitted or accepted, issues that are discussed in more detail in the remaining sections of this chapter.

Specific Documents Only

Some electronic filing pilot projects have focused on certain types of pleadings or specific types of cases. Nevada has two statutory provisions relating to juvenile and criminal cases.[14] The fifth appellate district of Ohio[15] and the federal district court for the

[13] Revised Code of Washington, 19.34.503.
[14] Nevada Revised Statutes, 62.206 and 432B.515.
[15] Local Rules of the Ohio Fifth Appellate District, Rule 2.

eastern district of Pennsylvania[16] have adopted court rules that also restrict the types of papers that may be transmitted electronically.

62.206 Electronic filing of certain documents.

1. A court clerk may allow any of the following documents to be filed electronically:

(a) A petition prepared and signed by the district attorney pursuant to NRS 62.128 or 62.130;

(b) A document relating to proceedings conducted pursuant to NRS 62.193; or

(c) A study and report prepared pursuant to NRS 62.197.

432B.515 Electronic filing of certain petitions and reports.

1. A court clerk may allow any of the following documents to be filed electronically:

(a) A petition signed by the district attorney pursuant to NRS 432B.510; or

(b) A report prepared pursuant to NRS 432B.540.

RULE 2. CLERKS OF THIS COURT; FILING DOCUMENTS; PROPOSED JUDGMENT ENTRY REQUIRED

(C) Electronic Filing. Only motions to this Court and their responses may be filed with the appropriate Clerk of this Court by facsimile or other electronic transfer. Such motions shall be deemed filed when received and file stamped by the Clerk. No other pleadings, including the notice of appeal or briefs, shall be filed via facsimile or other electronic transfer.

XLI. ELECTRONIC FILING AND RETRIEVAL OF DOCUMENTS

Electronic filing and retrieval of documents is available for certain documents filed in the Eastern District of Pennsylvania. All civil and criminal documents will be accepted for electronic submission, including complaints, notices of removal and notices of appeal.

APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS

Affidavits, Depositions and Other Signed Statements. Affidavits, depositions or any other sworn statement signed by any person other than the attorney making a submission may not be electronically transmitted to the court. Certificates of service that are normally signed by the attorney must be included as part of any electronic submission.

[16] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania, section XLI and Appendix V.

Recommendations

If a court wishes to restrict the types of cases or documents submitted to a court electronically, particularly in a pilot-testing environment, then this information should be made available to all attorneys and parties. It seems unwise to include this type of language in state statutes—the preferable course would be to dictate such requirements in court rules or operating procedures. This would allow expansion of the program or alteration of the test without waiting on a modification process that could take months to complete.

Because of the cost and difficulty of maintaining parallel systems, it would be better for a court to move all the cases in a work area to an electronic format, using an internal scanning unit to convert paper submissions. Trying to process some cases electronically and others on paper creates so much extra work that the productivity gains brought by the technology could be canceled out entirely.

Technical Standards for System Use

Some courts have adopted very specific requirements for the submission of pleadings, including technical detail about document format, system availability and use, etc. These specifications are included in local rules or procedural handbooks. While this exercise may seem overdone to non-technicians, it is essential that the information be provided in one way or another. If it is not published, technical and clerical staff may spend countless hours on the telephone assisting would-be filers. The following examples are

from the bankruptcy court for the southern district of New York[17] and the U.S. District Court for the eastern district of Pennsylvania.[18]

CLAD ADMINISTRATIVE PROCEDURES

IV. Technical Requirements.

A. Document Format.

1. All pleadings and other documents which are filed electronically shall be filed in WordPerfect 5.1 format or in ASCII format. If a pleading or other document is filed in the WordPerfect 5.1 format, it shall be set up with the following initial style set up:

[T/B Mar:1"] [Pg Numbering: Top Right] [Just:Left] [Ln Height:0.167"] [Ln Spacing:2] [L/R Mar:1.25",1.25"] [Hyph Off] [W/O Off] [Font: Courier 10cpi]

After the initial style set up, the document may contain format codes for appropriate presentation (e.g., single space and block indent).

2. DO NOT USE THE AUTOMATIC DATE CODE FEATURE IN ANY WORDPERFECT DOCUMENT FILED ELECTRONICALLY.

3. Documents which are filed in the ASCII format will NOT contain page numbers when viewed electronically on CLAD. In addition, when ASCII documents are printed from a word processing software, the pagination will not be uniform. Therefore, it is recommended that all documents filed electronically be in the WordPerfect 5.1 format.

B. Hardware Requirements. To access CLAD, it is necessary to have a computer (i) operating under a DOS operating system and (ii) equipped with a Hayes compatible modem with a speed up to 14,400 baud. Each attorney having access to the CLAD BBS for the purpose of filing and retrieving pleadings and other documents must have a computer equipped with a hard disk drive.

The legal agency or law firm utilizing electronic filing must first submit an application to the clerk's office which explains the equipment specifications needed to transmit electronically.

B. Equipment. The electronic submission of documents requires the use of a terminal, a 2400 baud modem, and a computer capable of processing ASCII or XMODEM or Word Perfect 5.0. At the present time, these are the only acceptable means to transmit documents electronically to the district court.

APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS

Acceptable Communication Protocols. The electronic filing system will presently accept files that are transmitted via either ascii, xmodem-checksum,

[17] Bankruptcy Rules of the U.S. District Courts for the Southern and Eastern Districts of New York, Appendix G.

[18] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania, section XLI and Appendix V.

xmodem-crc or ymodem. Only one of these communications protocols may be used.

Acceptable Terminal Types. The following terminal types are presently recognizable by the system: vt100, ansi, and dumb. Users should specify the dumb terminal type if they are unsure as to which terminal they have. Only one of the above terminal types will be specified.

Modem Settings. The court dial-in modem is presently set as follows: 2400 baud, 8-bit, 1 stop, no parity. Data can be transmitted at 1200, 2400 or 9600 baud. User dial-out modems should be set appropriately.

Document Formatting. Presently this system will only accept documents containing standard ascii characters or in WordPerfect 5.0 format (See Attachment B to this application for a list of the standard ascii characters). Most word processing packages have an option whereby the user can convert the word processing formatted file to an ascii file. When this option is used, the word processing system will strip out all special formatting characters and retain only the ascii characters. As a matter of practice, the attorney should review any file that is converted to ascii prior to the electronic submission of the ascii file to the court. The symbol "&" must be used in lieu of the section symbol when referring to a title and section of a code. Title 18, Section 495 of the U.S. Code would be typed as 18 USC & 495. Footnotes must either be treated as end notes or manually inserted on each page. Page breaks (CONTROL-L) must be inserted for each page of the document being submitted. Otherwise, the system will automatically insert a page break every 66 lines.

Routine system backups will be accomplished between the hours of 8:30 am and 9:30 am Monday thru Friday. The system will not be available for use during these hours.

Recommendations

The court should publish very detailed instructions and specifications, similar to those shown above. They should not be included in statutes or court rules, but should be controlled by the clerk's office and technologists. The statute or rule, at most, should authorize the clerk or AOC to prepare and maintain the instructions. The best approach is to make them available from the court's World Wide Web site, so changes can be incorporated and distributed immediately. Paper copies should be kept at the clerk's front counter for those who do not have Internet access.

Agreements Between Courts and Filing Parties

Often courts have initiated agreements with parties who participate in electronic filing programs. Some of these courts publish lengthy instructions, forms, and so forth, in procedural manuals.[19] The Los Angeles County Superior Court has a rule that requires a party to execute a contract with the court before filing documents electronically.

> **RULE 18.00 ELECTRONIC FILING AND SERVICE**
> (1) The filing litigant or the litigant's attorney executes a contract with the court in a form approved by the executive officer of the court, which contract shall include a promise not to send harmful or deleterious matter into the court's information system….

Recommendations

If parties are required to pay to use the court's electronic filing service, then a contractual arrangement may be in order. Sometimes this is the only way the court can generate sufficient revenue to cover the cost of constructing and maintaining the capability. It is better to pay for electronic filing infrastructure through appropriated funds or surcharges on filing fees.

Making Electronic Filing Mandatory

Most states make it clear that electronic filing, and the use of digital signatures in conjunction with electronic filing, is only to be done at the option of the parties involved. Even systems used in large-scale litigation have given users the option of submitting paper. Here are samples of statutory language.

> **Section 9-1-53. Authority to electronically file and store court documents.**
> Courts and county offices are hereby authorized but not required to institute procedures for the electronic filing and electronic storage of court documents to further the efficient administration and operation of the courts.[20]

[19] For example, see Bankruptcy Rules of the U.S. District Courts for the Southern and Eastern Districts of New York and the Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.

[20] Mississippi Code 1972, 9-1-53.

Section 14.01. Digital signatures.

(b) The use or acceptance of a digital signature shall be at the option of the parties. Nothing in this Section shall require a State agency to use or permit the use of a digital signature.[21]

Section 59.1-469 State agencies' use of digital signatures.

Every agency, department, board, commission, authority, political subdivision or other instrumentality of the Commonwealth may receive digital signatures in lieu of manual signatures, provided such digital signatures meet the standards established by the Council on Information Management. The use or acceptance of a digital signature shall be at the option of the parties. Nothing in this chapter shall require a public entity to use or permit the use of a digital signature.[22]

Recommendations

During the development of electronic filing technology, the courts must be able to receive both paper and electronic documents. As time goes on, the judiciary must be able to increase the incentive or pressure on lawyers to implement electronic filing. A mixed system may be less efficient than a paper one. Only when the bulk of the materials received by the court are in digital form will the courts realize the full benefits of the technology. Of course, a small portion of the documents submitted to the court may always be on paper; the judiciary must be able to scan or convert these pleadings for those who lack the means to do so themselves.

Specific Data Requirements

Some court rules and administrative procedures require that certain data are included or give specific directions concerning information provided in the electronic filing. An example of each should suffice.

Rule 61. Procedures Following Filing of Citation--Issuance of Summons

(b) Except in cases charging parking violations when the citation is electronically filed, a copy of the citation shall be served with the summons.

[21] Illinois Statutes, 405/14.01.
[22] Code of Virginia, 59.1-469.

(c) In cases charging parking violations when the citation is electronically filed, the summons shall also include:

(1) the date, time, and location of the parking violation;

(2) a description of the vehicle and the license number; and

(3) a description of the parking violation.[23]

CLAD ADMINISTRATIVE PROCEDURES

F. Title of Docket Entries.

1. The person electronically filing a pleading or other document will be responsible for designating that the title of the document falls within one of the categories contained in Schedule D hereto.

2. The title of a pleading or other document filed electronically MUST (i) identify the party filing said pleading or other document and (ii) be of sufficient detail to describe the subject matter of said pleading or other document.

CORRECT: Debtor's motion to sell nonresidential real property located in Block 11, Lot 6 New York City to Buy It, Inc.

INCORRECT: Motion to sell property

3. The title of a docket entry MUST identify all documents being electronically filed together under one docket number.

CORRECT: Debtor's Notice of Motion to Assume XYZ lease with Motion, Affidavit and Memorandum of Law in support thereof.

INCORRECT: Debtor's motion to assume XYZ lease[24]

Recommendations

Administrative procedures created and maintained by the clerk's office or technologists should provide clear, precise instructions concerning any issue that is important in making the electronic filing process function smoothly and correctly. To ensure adequate flexibility, specific information concerning data elements should not be included in statutes or court rules.

Electronic Authentication

A more complete discussion of legal and policy issues concerning authentication is contained in the next chapter. A New Mexico statute provides a general approach to solving the problem.[25]

[23] Pennsylvania Rules of Criminal Procedure, Rule 61.
[24] Administrative Procedures for Electronically Filed Cases, II. F.

> **14-3-15.2 Electronic authentication; substitution for signature.**
> Whenever there is a requirement for a signature on any document, electronic authentication that meets the standards promulgated by the commission may be substituted.

States have adopted or are considering five methods of determining the authenticity of documents, as recorded in statutes, rules, and procedures. These methods are passwords, electronic approval, electronic signatures, signature dynamics, and digital signature. Each is discussed below.

Passwords

The earliest experiments in electronic filing relied on passwords to authenticate submissions. As more secure methods were developed, some argued that password protection was easier and less expensive than the newer technologies. It was also claimed that password protection was far more secure than the systems used for decades in the world of paper.

Delaware provides a simple example of a rule prescribing password authentication.[26]

> **INTERIM RULE 79.1 COMPLEX LITIGATION AUTOMATED DOCKET**
> 9. The utilization of a password for the purposes of filing a pleading shall constitute a signature of the registrant of that password under Superior Court Civil Rule 11.

Electronic approval

Minnesota statutes allude to a process for approving transactions electronically without a signature.[27]

> **16B.05. Delegation by commissioner**
> Subdivision 1. Delegation of duties by commissioner. The commissioner may delegate duties imposed by this chapter to the head of an agency and to any

[25] New Mexico Statutes 1978, 14-3-15.2.
[26] Delaware Superior Court Rules of Civil Procedure, Interim Rule 79.1, Complex Litigation Automated Docket.
[27] Minnesota Statutes, Administration and Finance, 16B.05.

> subordinates of the head. Delegated duties are to be exercised in the name of the commissioner and under the commissioner's supervision and control.
>
> Subd. 2. Facsimile signatures and electronic approvals. When authorized by the commissioner, facsimile signatures, electronic approvals, or digital signatures may be used in accordance with the commissioner's delegated authority and instructions. Copies of the delegated authority and instructions must be filed with the commissioner of finance, state treasurer, and the secretary of state. A facsimile signature, electronic approval, or digital signature, when used in accordance with the commissioner's delegated authority and instructions, is as effective as an original signature.

Electronic approval could be used for supervisory review of purchase orders, personnel transactions, travel vouchers, etc. This approach seems better suited to electronic intergovernmental transactions, or other applications within large organizations, rather than in adversarial court proceedings.

Electronic signatures

Electronic signature refers to the electronic transmission of an image of a signature. A document is signed in the traditional way, then is sent by facsimile to the court. Or, an image of a person's signature is stored as a computer file and affixed to a word processing document that is attached to an electronic mail message. The following statutes from Nevada[28] and Virginia[29] illustrate requirements for electronic signatures.

> **62.206 Electronic filing of certain documents.**
>
> 2. Any document that is filed electronically pursuant to this section must contain an image of the signature of the person who is filing the document.

> **Section 17-83.1:4 (Effective until July 1, 1998) Signature; when effective as originals.**
>
> If the sender of an electronically filed document files an affidavit of authenticity along with the electronic filing and the electronic transmission bears a facsimile or printing of the required signature, any statutory requirement for an original signature shall be deemed to be satisfied. Any reproduction of the electronically filed document must bear a copy of the signature. The electronically reproduced document shall be accepted as the signature document for all court-related purposes unless the original with the original signature affixed is requested

[28] Nevada Revised Statutes, 62.206.
[29] Code of Virginia, 17-83.1:4.

> by motion of one or more parties to a pending action or is otherwise required by law. If the court grants the motion of a party, the order shall provide that the original be filed with the court.

The terms *electronic signature* and *digital signature* are often confused or used vaguely in statutes and court rules, sometimes in the same sentences, so some care must be exercised in the application of these definitions. This example is from the state of Indiana and could apply to any form of electronic authentication technology.[30]

> **5-24-2-2 "Electronic signature"**
> Sec. 2. "Electronic signature" means an electronic identifier, created by computer, executed or adopted by the party using it with the intent to authenticate a writing.

Signature dynamics

The final draft of regulations prepared by the California Secretary of State defines two acceptable forms of digital signature, the first of which, based on asymmetric cryptosystem technology, is used by many other states and is discussed throughout this monograph. The second, which is unique to the California regulations, is signature dynamics. Since the regulations explain the technology in detail, they are included here in their entirety.[31]

> **22003. List of Acceptable Technologies**
> b. The technology known as "Signature Dynamics" is an acceptable technology for use by public entities in California, provided that the signature is created consistent with the provisions in Section 22003(b)(1)-(5).
> 1. Definitions—For the purposes of Section 22003(b), and unless the context expressly indicates otherwise:
> A. "Handwriting Measurements" means the metrics of the shapes, speeds and /or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.
> B. "Signature Digest" is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.

[30] Indiana Code, 5-24-2-2.
[31] Final Draft of Proposed Digital Signature Regulations, California Administrative Code, Title 2, Division 7, Chapter 10, Section 22003, as found at http://www.ss.ca.gov/digsig/finalregs.htm.

C. "Expert" means a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert pursuant to California Evidence Code section 720.

D. "Signature Dynamics" means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

2. California Government Code section 16.5 requires that a digital signature be 'unique to a person using it.' A signature digest produced by Signature Dynamics technology may be considered unique to the person using it, if:

A. the signature digest records the handwriting measurements of the person signing the document using signature dynamics technology, and

B. the signature digest is cryptographically bound to the handwriting measurements, and

C. after the signature digest has been bound to the handwriting measurements, it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.

3. California Government Code section 16.5 requires that a digital signature be capable of verification. A signature digest produced by signature dynamics technology is capable of verification if:

A. the acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison, and

B. if signature verification is a required component of a transaction with a public entity, the handwriting measurements can allow an expert handwriting and document examiner to assess the authenticity of a signature.

4. California Government Code section 16.5 requires that a digital signature remain 'under the sole control of the person using it.' A signature digest is under the sole control of the person using it if:

A. the signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message, and

B. the signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.

5. The signature digest produced by signature dynamics technology must be linked to the message in such a way that if the data in the message are changed, the signature digest is invalidated.

Digital signature

Digital signature combines a hashing function and public key encryption to produce the highest level of assurance that the document was submitted by the party to whom the filing is attributed, and that it has not been changed during transmission from the sender to the court. Lengthy legislative enactments in many states have enabled the use of

digital signature technology. The next subsection of this chapter explores rules concerning digital signatures more completely.

Recommendations

Authentication of electronic documents is an important and serious issue. Like paper submissions, pleadings filed electronically normally will be considered legitimate. If controversy erupts, it is essential that the court be able to verify the origin of documents and to determine if they have been modified since transmission.

Courts should adopt rules that reflect their policy decisions on authentication. References to specific technologies should not be adopted in statutory language since the software and hardware to support these activities change rapidly. Statutes should delineate the principles with which any electronic authentication technology should comply.

Digital Signature

A signature is a distinctive mark, attributable to the signer, that authenticates a writing. On paper, the signature provides evidence that the signer authorized or approved the transaction contained in the signed document. It also provides a measure of certainty that the document has not been altered or falsely submitted.[32]

A digital signature is not an image of a manually signed name; it is a method of digital file encryption that facilitates verification of the integrity and authenticity of an electronic message.[33] A digital signature, properly used, assures the receiver that the

---

[32] Information Security Committee, Section of Science and Technology, American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce* (1996) [hereinafter *Digital Signature Guidelines*]. A copy of the *Digital Signature Guidelines* may be downloaded free from <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

[33] C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure* (33 San Diego Law Review 1143, Summer 1996).

document came from the purported sender and that the document has not been modified in the transmission process. These concepts are known as *data origin authentication* and *message integrity*. In addition, where the procedures practiced by a trusted third-party in binding the public key of a unique key pair to an actual person can be trusted, the signer cannot deny having signed a digitally signed document with a valid digital signature; this is the principle of *non-repudiation*. The same assumptions of approval or authorization that apply to signatures on paper can be extended to electronic documents accompanied by digital signatures.

Digital signatures are created using asymmetric cryptography. Asymmetric cryptography uses a unique pair of very long numbers, called keys, that have a special relationship to one another. The private key is held by the owner and is used to encrypt messages for the purpose of digitally signing, or authenticating, messages as having been originated by the holder of the private key associated with the public key of the key pair. The private key is also used to decrypt incoming confidential messages encrypted with the associated public key of this key pair and intended only for the holder of this private key. The public key is available to anyone and is used to verify digital signatures and to encrypt confidential messages intended only for the holder of the associated private key. Because of the complex mathematical algorithms employed in public key cryptography, only the associated private key of the unique key pair can make sense of messages encrypted with the associated public key. Similarly, only the public key can verify digital signatures made with the associated private key. Therefore, if the holder of the private

key keeps it secure and safe from compromise, and follows the procedure described below, it is computationally infeasible[34] to forge or alter a message without detection.

To create a digital signature, the person sending the document completes several steps. First, a message digest is created. A mathematical formula, known as a hash function, is applied to the binary data that make up the message. The hash value, or message digest, that results is encrypted with the private key. The encrypted message digest is the digital signature. The signer transmits the original message and the digital signature.

Digital signatures are verified using a similar process. The receiver applies the same hash function to the message. Using the public key of the sender, the receiver decrypts the signature and compares it to the message digest just produced. If a single electronic bit of the original message has been altered, the message digests will not match. If both are the same, the receiver can be assured that the document is authentic and was transmitted by the purported sender.

The Information Security Committee of the Section of Science and Technology of the American Bar Association developed guidelines for implementing digital signature programs,[35] though their work was never formally approved by the Council of the Section of Science and Technology, the House of Delegates, or the Board of Governors of the ABA. Many states enacted digital signature legislation based on the work of this committee.

[34] *Digital Signature Guidelines*, 9.
[35] *Digital Signature Guidelines.*

Utah was the first state to pass digital signature legislation.[36] Minnesota[37] and Washington[38] followed with very similar laws. The Los Angeles County Superior Court[39] enacted a related program by local court rule; Florida,[40] Oregon,[41] and Mississippi[42] passed condensed versions of the Utah legislation. Much of the language of these enactments is directed at the creation of an infrastructure to distribute, certify, and manage the public and private keys needed to make digital signatures reliable.

California[43] passed a much more limited law that merely authorizes the use of digital signatures if they meet certain conditions, directs the Secretary of State to develop regulations to govern this process, and ensures that the use of digital signatures shall be at the option of the parties to the transaction. Illinois,[44] Indiana,[45] New Mexico,[46] Texas,[47] and Virginia[48] passed similar laws, and Kansas[49] enacted nearly identical language in its rules of civil procedure.

A complete analysis of the legislation needed to create a digital signature infrastructure is beyond the scope of this document.[50] It is questionable if a court could or should attempt to build this type of infrastructure solely for its electronic filing project. This would be akin to creating a new telephone system, with all the wiring, switches, and

[36] Utah Code Annotated, 46-3-101 to 46-3-504. Utah Digital Signature Act.
[37] Minnesota Statutes Annotated, 325K.01 to 325K.24. Electronic Authentication Act.
[38] Revised Code of Washington Annotated, 19.34.101 to 19.34.503. Washington Electronic Authentication Act.
[39] California Rules of Court, Los Angeles County Superior Court Rule 18.01 to 18.02.
[40] Florida Statutes Annotated, Title XIX 282.72 to 282.745.
[41] 1996 Oregon Revised Statutes, 192.825 through 192.855, Electronic Signatures Act.
[42] Mississippi Code 1972 Annotated, 25-63-1 to 25-63-11. Digital Signature Act.
[43] California Government Code, section 16.5.
[44] Illinois Compiled Statutes Annotated, 405/14.01.
[45] Annotated Indiana Code, 5-24-2-1 to 5-24-2-6. Electronic Digital Signature Act.
[46] New Mexico Statutes 1978, 14-15-1 through 14-15-6, Electronic Authentication Act.
[47] Texas Statutes and Codes Annotated, 10B-2054.060 and 6A-201.931 to 201.933.
[48] Code of Virginia, 59.1-467 to 59.1-469.
[49] Kansas Court Rules and Procedures, 26-60-2616.

telephones just for court-related conversations. To justify the administrative overhead of a digital signature system built just for courts would require a tremendous amount of filing activity. Only if a state has already commenced the process of building this infrastructure, is the court in a good position to use it in a cost-effective way.

Issues that will not be addressed are the definition of all the digital signature technology terms that have been included in the various legislative enactments, the licensing, regulation, and/or accreditation of certification authority organizations, duties and obligations of certification authorities and subscribers, certificate repositories, and reliance on certificates and digital signatures. Issues of allocation of legal liability also will not be covered.

Two issues relating to digital signatures that are appropriate for court adoption will be covered. The first shows two approaches to authorizing the use of digital signatures, one from Kansas[51] and the other from Virginia court rules.[52] The second is a definition of digital signature enacted by local court rule in the Superior Court of Santa Clara County, California.[53]

Section 60-2616. Digital Signature

(a) This act may be cited as the Kansas digital signature act.

(b) As used in this act, "digital signature" means a computer-created electronic identifier that is:

(1) Intended by the person using it to have the force and effect of a signature;

(2) unique to the person using it;

(3) capable of verification;

(4) under the sole control of the person using it; and

(5) linked to data in such a manner that it is invalidated if the data are changed.

[50] But see, http://www.mbc.com/ds_sum.html, a web site hosted by the law firm of McBride Baker & Coles out of Chicago, and dedicated to maintaining a current review of digital signature and electronic commerce legislation in the states and internationally.

[51] Kansas Court Rules and Procedures, 26-60-2616.

[52] Code of Virginia, 59.1-467 to 59.1-469.

[53] Santa Clara County Superior Court Rules, 1.7.1, Definitions.

(c) A digital signature may be accepted as a substitute for, and, if accepted, shall have the same force and effect as any other form of signature.

Section 59.1-469 State agencies' use of digital signatures.

Every agency, department, board, commission, authority, political subdivision or other instrumentality of the Commonwealth may receive digital signatures in lieu of manual signatures, provided such digital signatures meet the standards established by the Council on Information Management. The use or acceptance of a digital signature shall be at the option of the parties. Nothing in this chapter shall require a public entity to use or permit the use of a digital signature.

Section 1.7.1 Definitions

C. Digital Signature. "Digital Signature" means a sequence of bits derived from an electronic document by an algorithm using a digital key assigned to a subscriber by a Certification Authority with the property that the integrity, origin and authenticity of the document to which it is applied can be validated. "Digitally Signed" means the application of a Digital Signature to a document.

Digital signature legislation provides examples of problems that can be encountered in the rulemaking process. The first instance illustrates statutory language that is too complicated to be useful to one who is not familiar with digital signature terminology.[54]

325K.19. Satisfaction of signature requirements

(a) Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature, if:

(1) no party affected by a digital signature objects to the use of digital signatures in lieu of a signature, and the objection may be evidenced by refusal to provide or accept a digital signature;

(2) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(3) that digital signature was affixed by the signer with the intention of signing the message and after the signer has had an opportunity to review items being signed; and

(4) the recipient has no knowledge or notice that the signer either:

(i) breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature.

(b) However, nothing in this chapter precludes a mark from being valid as a signature under other applicable law.

[54] Minnesota Statutes Annotated, 325K.19.

The second example appears to inappropriately assign the risk of reliance on a digital signature to the receiver of the document.[55] This may be inconsistent with current practice for paper pleadings.

> **325K.20. Unreliable digital signatures**
> Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances. If the recipient determines not to rely on a digital signature under this section, the recipient must promptly notify the signer of any determination not to rely on a digital signature and the grounds for that determination. Nothing in this chapter shall be construed to obligate a person to accept a digital signature or to respond to an electronic message containing a digital signature.

This section provides an example of an enactment that may be overly technical.[56] Difficulty of understanding meaning is not the only risk in using this type of language; rapidly changing technology and standards may render these types of statutes inaccurate.

> **19.34.010. Purpose and construction**
> This chapter shall be construed consistently with what is commercially reasonable under the circumstances and to effectuate the following purposes:
> (1) To facilitate commerce by means of reliable electronic messages;
> (2) To minimize the incidence of forged digital signatures and fraud in electronic commerce;
> (3) To implement legally the general import of relevant standards, such as X.509 of the international telecommunication union, formerly known as the international telegraph and telephone consultative committee; and
> (4) To establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.

At the other extreme is language that is too vague.[57]

> **19.34.305. Acceptance of digital signature in reasonable manner**
> Acceptance of a digital signature may be made in any manner reasonable in the circumstances.

[55] Minnesota Statutes Annotated, 325K.20.
[56] Revised Code of Washington Annotated, 19.34.010.
[57] Revised Code of Washington Annotated, 19.34.305.

Recommendations

First, be sure that digital signature is the right authentication approach. Other less costly and complex alternatives are available, though they do not provide the same level of protection and confidence. Like EDI,[58] a digital signature infrastructure that is appropriate for large commercial applications may be overkill for the rest of the world. It may not make sense to invest tens of thousands of dollars in a technology that will save a few hundred dollars in postage stamps. In large, high-volume courts with real security risks, digital signature may be a cost-effective strategy.

Second, participate in broader digital signature efforts rather than undertaking independent action. Digital signature technology will only become part of the technology infrastructure if it is widely used.

Third, keep legislative enactments focused on broad policy issues, like authorization to accept digitally signed pleadings and general requirements of the technology. Specific implementation issues and technology requirements should be established in local rules or operational procedures to ensure flexibility.

Finally, avoid hiding subtle yet significant policy changes in implementing language, unless they are truly necessary for the technology to succeed. This will help ensure the adoption of the new technology and ease the transition from the old. At the same time, beware of unnecessarily vague language that can lead to incompatible approaches to implementation.

[58] Electronic data interchange, a method of electronically exchanging standard business forms.

Requirements Concerning Passwords

Several courts have adopted rules or operating procedures that delineate password requirements. The issues covered include procedures for issuance; fees assessed for passwords; the use of funds collected; differentiation between passwords for bar members, used to file papers, and passwords for the public, used to view records; requirements to protect passwords; and the use of the password as a signature.

The following examples illustrate rules and procedures created by courts.

> **INTERIM RULE 79.1 COMPLEX LITIGATION AUTOMATED DOCKET**[59]
>
> 6. The Prothonotary shall establish a procedure for the distribution of passwords to permit access to CLAD. The passwords shall be issued as follows:
>
> (a) Upon request, any member of the Delaware Bar who enters an appearance on behalf of a party shall be issued a password for that specific case for a registration charge of $20.00;
>
> (b) Upon request, any member of the public shall be issued a general non-case-specific password with a registration charge of $50.00 annually.
>
> 7. The Prothonotary shall expend the funds solely for the purpose of operating and maintaining CLAD.
>
> 8a. No Delaware lawyer shall knowingly permit or cause to permit his/her password to be utilized by anyone other than an employee of his/her law firm.
>
> 8b. No person shall knowingly utilize or cause another person to utilize the password of another (1) without permission of the holder of the password, or (2) in violation of this Rule.
>
> 9. The utilization of a password for the purposes of filing a pleading shall constitute a signature of the registrant of that password under Superior Court Civil Rule 11.

> **RULE 9011-1. SIGNING OF PAPERS**[60]
>
> (c) Any password required for electronic filing shall be used only by the attorney to whom the password is assigned and authorized members and employees of such attorney's firm.

[59] Delaware Superior Court Rules of Civil Procedure, Interim Rule 79.1, Complex Litigation Automated Docket.

[60] Bankruptcy Rules of the U.S. District Courts for the Southern District of New York 9011-1.

CLAD ADMINISTRATIVE PROCEDURES[61]

B. Passwords. Access to the CLAD BBS or the CLAD Private Database requires a password, which may be obtained as follows:

1. Each party entitled to participate in CLAD BBS cases for the electronic retrieval and filing of pleadings and other documents in accordance with an order of the Court shall be entitled to one CLAD BBS password for each attorney in each such case and each adversary proceeding in such case. The CLAD BBS password will permit the attorney to file pleadings and other documents with, and retrieve pleadings and other documents from, the CLAD BBS.

2. Any person or organization, other than those referred to in paragraph I.B.1., above, may apply to the Office of the Clerk, United States Bankruptcy Court for the Southern District of New York for registered access to the CLAD Private Database. Registration under this subparagraph will entitle the registrant to retrieval, but not filing, privileges for CLAD cases subject to the limitations and fees imposed by the vendor.

Recommendations

It is most appropriate for courts to define procedures for issuing, using, protecting, and maintaining passwords by court rule or operational procedure. The language used should be clear and concise, so court employees, system users, and the public can understand their responsibilities. While it is preferable for courts to provide free access to the public records they maintain, circumstances may require the imposition of fees to cover the cost of providing service.

The wide acceptance of the Internet is driving most courts to web-based systems for accepting electronic documents and providing access to court information, in the place of dial-up terminal configurations. Password protection is easy to implement in this environment and most of the headaches associated with supporting users are eliminated, since they use the same hardware and software to access other sites on the World Wide Web. Since much of the incremental cost of providing filing and access services is

[61] Bankruptcy Rules of the U.S. District Courts for the Southern and Eastern Districts of New York, Appendix G.

eliminated, courts that have charged fees in the past may find it possible to provide access as a free public service.

Provisions Concerning Paper Records

One state found it necessary to ensure that legislation enabling electronic filing not invalidate previous statutory language concerning maintenance of paper records in those courts not implementing the technology.[62]

> **Section 9-1-53. Authority to electronically file and store court documents.**
> The provisions of Sections 9-1-51 through 9-1-57 shall not be construed to amend or repeal any other provision of existing state law which requires or provides for the maintenance of official written documents, records, dockets, books, ledgers or proceedings by a court or clerk of court in those courts which do not elect to exercise the discretion granted by this section.

Recommendations

Whether or not a state chooses to include this type of language in statutes authorizing electronic filing depends on the nature of current laws. If the statutes give specific instructions on maintenance of paper records, and if there might be confusion as to which requirements are binding for a particular court, then a section similar to the one above should be enacted. Many states have simply eliminated the detailed instructions to clerical staff from state law and have allowed courts to develop more modern and flexible operational procedures.

Retention Schedule for Electronic Records

The State of Mississippi has the most extensive statutory language adapting rules for paper records to electronic documents. The first deals with records retention.

[62] Mississippi Code 1972 Annotated, 9-1-53.

Section 9-1-57. Plan for electronic storage system.[63]

(e) The plan shall provide for retention of the court records consistent with other law and in conformity with rules and regulations prescribed by the Administrative Office of Courts and adopted by the Mississippi Supreme Court and shall provide security provisions to guard against physical loss, alterations and deterioration; and

Section 9-5-171. Destruction of records[64]

(3) Records may be filed and retained by electronic means as provided in Sections 9-1-51 through 9-1-57, whether the record is to be destroyed or not; provided, however, that destruction of such records shall be carried out in accordance with Sections 25-59-21 and 25-59-27, Mississippi Code of 1972.

(4) Any of the records referred to in this section may be preserved by means of electronic storage as provided in Sections 9-1-51 through 9-1-57, whether the record is to be destroyed or not.

Recommendations

Management of information storage resources is just as important with electronic media as it is with paper. Court leaders often want to keep everything online forever. Only when limitations on disk space start to impede system performance, is the problem usually addressed. Initially, retention schedules that apply to paper can be applied to electronic documents. Experience and evaluation will, at some point, lead to refinement of retention schedules to match court needs and system capabilities.

Exemptions from Public Disclosure Laws

Both Mississippi[65] and Utah have exempted records containing private keys and encryption information from public disclosure laws, using nearly identical language. The example below is from the Utah Digital Signature Act.[66]

46-3-504 Exemptions.

(1) The following governmental entity records are exempt from Title 63, Chapter 2, Government Records Access and Management Act:

[63] Mississippi Code 1972 Annotated, 9-1-57.
[64] Mississippi Code 1972 Annotated, 9-5-171.
[65] Mississippi Code 1972 Annotated, 25-63-11.
[66] Utah Code Annotated, 46-3-504.

(a) records containing information that would disclose, or might lead to the disclosure of private keys, asymmetric cryptosystems, or algorithms; or

(b) records, the disclosure of which might jeopardize the security of an issued certificate or a certificate to be issued.

(2) For purposes of this section, "record" has the meaning described in Section 63-2-103.

Recommendations

For the protection of the private key infrastructure, courts should adopt language protecting any documents relevant to the security of the electronic filing system from public disclosure.

Public Access to Electronic Records

Only three courts have realized the need to ensure continued public access to records when they are moved to an electronic format. Oregon's statute requires the same access to electronic complaints as to their paper equivalent, while the bankruptcy court for the Southern District of New York provides specific information to the public about how to access court information.

153.770. Electronic filing of complaint for offenses subject to citation by uniform citation.[67]

(c) Members of the public can obtain copies of and review complaints that are electronically filed and maintained under this section in the same manner as for complaints filed on paper.

CLAD ADMINISTRATIVE PROCEDURES[68]

VI. Public Access to the CLAD Docket.

A. The public will have electronic access to the documents filed in CLAD and the CLAD docket in the Office of the Clerk during the hours of 10 a.m. to 12 noon and 2 p.m. to 4 p.m., Monday through Thursday.

B. Copies of the documents will be available at the copy service in Room 505, Alexander Hamilton Custom House, One Bowling Green, New York, NY during business hours Monday through Friday. The fee for such copy will be made directly to the copy service.

[67] 1996 Oregon Revised Statutes, 153.770.

[68] Bankruptcy Rules of the United States District Courts for the Southern and Eastern Districts of New York, Appendix G.

The United States District Court for the Northern District of California has directed by local rule that documents in securities fraud litigation be made available to the public at designated sites on the World Wide Web. Portions of their rule are shown below.[69]

> **23-2. Electronic Posting of Certain Documents Filed in Private Securities Actions.**
> (Adopted effective March 25, 1997)
> **(a) Electronic Posting.** All postable documents, as defined in subsection (b) of this rule, required to be filed pursuant to Civil L.R. 5-1 in any private civil action containing a claim governed by the Private Securities Litigation Reform Act of 1995, Pub. L. No. 104-67, 109 Stat. 737 (1995), shall be timely posted at a Designated Internet Site. The party or other person filing such document shall be responsible for timely posting.
>
> **(d) Designated Internet Site.** "Designated Internet Site" for purposes of this rule shall mean an Internet site that:
> **(1)** Is accessible at no cost to all members of the public who are otherwise able to access the Internet through commonly used web browsers;
> **(2)** Charges no fee to any party, intervenor, amicus or other person subject to the provisions of this rule;
> **(3)** Places no restrictions on any person's ability to copy or to download, free of charge, any materials posted on the site pursuant to the requirements of this rule;
> **(4)** Maintains and responsibly operates a notification feature whereby any member of the public can request to receive e-mail notification, at no charge, of any posting of materials to the Designated Internet Site;
> **(5)** Undertakes to post on its site within two days of receipt of the electronic copy described in Civil L.R. 26-2(c)(1) of this rule all filings forwarded to it in compliance with the provisions of Civil L.R. 26-2(a);
> **(6)** Undertakes to provide e-mail notification within one day of receipt of the electronic copy described in Civil L.R. 26-2(c)(1) of this rule to all other Designated Internet Sites informing them of the posting of any materials related to securities class action litigation;
> **(7)** Maintains and publicizes a physical address to which the United States Postal Service or other commonly used delivery services can make physical delivery of documents, and/or diskettes, an Internet address in the form of an operational Uniform Resource Location ("URL"), and an e-mail address to which persons subject to paragraph (a) of this rule can transmit electronic copies of documents subject to the posting requirement of this rule;
> **(8)** Undertakes to disclose prominently the URLs, physical addresses, and facsimile numbers of all other Designated Internet Sites known to it; and
> **(9)** Submits to the Secretary of the Securities and Exchange Commission (the "Secretary") a statement, signed by a member of the bar that: identifies the

[69] Local Rules for the United States District Court for the Northern District of California, at http://ndcal.stanford.edu/docs/rules/Civil_L.R.shtml#23-2/

> Designated Internet Site through its URL; provides the name, address, telephone number, facsimile number and e-mail address of one or more persons responsible for operation of the site; and attests that the site satisfies the requirements of the rule and that it will promptly notify the Secretary should it cease to be a Designated Internet Site.
> **(e) Suspension of Posting Requirements.** Compliance with this rule shall not be required for any document filed at any time during which no Designated Internet Site is operational.

Recommendations

States should adopt statutory language that requires that access to electronic court records be at least as easy and inexpensive as access to paper records, even for those who do not have access to computer systems. Rules and operational procedures should provide details about how public access is to be administered and how individuals can view documents and other court records. Courts just beginning to create electronic filing systems should consider using the Internet as a vehicle for public access to documents.

Sealing and Expungment of Records

Procedures exist to limit access, seal, or expunge court records in most states. As more and more information is stored in electronic form and transmitted between agencies and organizations, enforcement of these orders is becoming more difficult. As documents are filed, accessed, and stored electronically, it will become impossible to identify the location of all the copies. Existing procedures to secure these documents will be rendered completely ineffective. Courts have not yet developed a way to solve this problem.

Recommendations

Courts and legislatures must develop policy in this area and implement it by statute or by rule. There are three options that will be discussed in the next chapter: abandoning attempts to seal or limit access to court records; entering these orders at the beginning of

the case, rather than at the end; or finding a way to track the distribution of documents over the Internet so they can be retrieved or removed.

Collection of Filing Fees

One of the first questions typically raised by courts when the subject of electronic filing is introduced is collection of filing fees. Although this appears to be an important issue, only one state has addressed it. Florida's rules of judicial administration provides for local flexibility by allowing parties and the court clerk to make acceptable arrangements for payment of filing fees.

> **Rule 2.090. Electronic Filing of Matters in all Proceedings within the State Courts System**[70]
>
> (2) All attorneys, parties, or other persons using this rule to file documents are required to make arrangements with the court or clerk of the court for the payment of any charges authorized by general law or the Supreme Court of Florida before filing any document by electronic transmission.
>
> (4) Any court or clerk of the court may extend the hours of access or increase the page limitations set forth in this subdivision.

Recommendations

Payment of filing fees is easily accommodated through establishment of attorney accounts or acceptance of credit cards. Court rules should describe how the system selected by the court is to be used.

Fees for Electronic Filing Service

Often courts have created electronic access or filing systems without sufficient appropriated funds to cover costs. The authorization to provide the service often includes permission to collect fees to be applied to purchase equipment and to cover other operational expenses. These fees are assessed as a subscription (one-time, annual, or per case), connect time, or per page downloading or uploading documents. Rules sometimes

indicate authorized or preferred methods of payment and how fees are to be deposited or used. Shown below are samples of some of the language implemented by statute, court rule, or administrative procedure.

Local Rule 5.7 Electronic Filing—Applicable in the Western District of Kentucky Only When Authorized by the Court[71]

(a) Electronic Filing Permitted. When authorized by the Court, any pleading, motion or other paper permitted or required to be filed by the Federal Rules of Civil Procedure or these rules may be filed electronically.

(b) Procedure for Electronic Filing. To file a pleading, motion or other paper electronically, a person must:

(1) Establish an account for payment of filing and administrative fees under procedures promulgated by the Clerk. This account must be established prior to any electronic transmission;

12-119.02. Electronic filing and access; fee[72]

B. The court may impose a fee of not more than one hundred dollars per year for an annual on-line access subscription plus a fee of not more than two dollars per minute for on-line access to court records.

C. All monies collected pursuant to subsection B of this section shall be transmitted to the state treasurer for deposit in the judicial collection enhancement fund established by s 12-113.

D. All filings made electronically pursuant to this section are subject to the fees established pursuant to s 12-119.01.

INTERIM RULE 79.1 COMPLEX LITIGATION AUTOMATED DOCKET[73]

3. Each party in each of the above cases is directed to pay a one-time assessment in the amount of $200.00 for each of the cases in which that party is named for the purposes of establishing the fund necessary to operate CLAD.

CLAD ADMINISTRATIVE PROCEDURES[74]

D. Fees.

1. Fees Payable to CLAD. A twenty dollar ($20.00) filing fee shall be payable to CLAD for each docket number obtained in connection with an electronic filing on the CLAD BBS. In addition, a twenty cents per page (20 cents/page) fee (the "Downloading Fee") shall be payable to CLAD for each

[70] Florida Statutes Annotated Rules of Judicial Administration, 2.090.
[71] Bankruptcy Rules of the United States District Courts for the Western and Eastern Districts of Kentucky, Rule 5.7.
[72] Arizona Revised Statutes Annotated, 12-119.02.
[73] Delaware Superior Court Rules of Civil Procedure, Interim Rule 79.1, Complex Litigation Automated Docket.
[74] Bankruptcy Rules of the U.S. District Courts for the Southern and Eastern Districts of New York, Appendix G.

> document retrieved from CLAD; provided, however, that the Downloading Fee shall be waived for the first retrieval of a pleading or other document from the CLAD BBS by any party entitled to notice and service of such pleading or other document in accordance with the Federal Rules of Bankruptcy Procedure or as otherwise provided by order of the Court.
>
> 2. Fees Payable to the Clerk. For filings that require a fee to be paid to the Office of the Clerk, authorization for credit card payment may be made with the financial officer of the Office of the Clerk.
>
> **APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS**[75]
>
> User Fees. A fee structure may be implemented in order to recover any increased personnel, equipment and telephone line costs that are incurred by the Court. Users will be advised at least 60 days in advance of the implementation of any fee system. At that point users will have the options of either agreeing to pay the established fees or of having their electronic filing access services discontinued.

Recommendations

Subscriptions are relatively easy to administer, but discourage infrequent or casual users because they must pay the same amount as those who use the system much more. Fees based on connect time, processing time, disk or other resources used, pages downloaded or uploaded, etc., are difficult and costly to administer. Tasks include billing, monitoring usage, and collecting overdue or delinquent accounts. Fees based on service offer the advantage of assessing the highest costs to those who use the system the most. Most preferred is a system that allows free access, one that is funded by appropriation.

Electronic Filing System Constitutes Docket and Other Records

A number of statutes and rules provide for the replacement of traditional books, files, and other records by their electronic equivalent. While each instance will not be listed, here are some samples.

[75] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.

9-1-53. Authority to electronically file and store court documents.[76]

It is hereby declared to be the intent of the Legislature that official written documents, records, dockets, books, ledgers or proceedings may be filed, stored, maintained, reproduced and recorded in the manner authorized by Sections 9-1-51 through 9-1-57 or as otherwise provided by law, in the discretion of the clerk.

9-7-171. General docket.[77]

(2) The general docket required to be kept by this section and all other dockets or records required by law to be kept by the circuit clerk may be kept on computer in lieu of any other physical docket, record or well-bound book if all such dockets and records are kept by computer in accordance with regulations prescribed by the Administrative Office of Courts.

9-5-135. Clerk to attend court and keep minutes.[78]

(2) The clerk, at his option, may elect to keep the minute books by means of electronic filing or storage or both, as provided in Sections 9-1-51 through 9-1-57 in lieu of or in addition to any paper records.

9-7-131. Jury fee book.[79]

The clerk of the circuit court shall keep a book to be called the "jury book," in which he shall enter the time of issuing all certificates to jurors, the amount thereof, and to whom issued. Such book may be kept by means of electronic filing or storage or both as provided in Sections 9-1-51 through 9-1-57, or otherwise, as the clerk may elect.

RULE 9021-1. ENTRY OF ORDERS, JUDGMENTS, AND DECREES[80]

The Clerk shall enter all orders, decrees, and judgments of the Court in the electronic filing system, which shall constitute docketing of the order, decree, or judgment for all purposes. The Clerk's notation in the appropriate docket of an order, judgment, or decree shall constitute the entry of the order, judgment, or decree.

CLAD ADMINISTRATIVE PROCEDURES[81]

7. The electronic filing of a pleading or other document in accordance with CLAD Procedures shall constitute docketing of that pleading or other document.

[76] Mississippi Code 1972 Annotated, 9-1-53.
[77] Mississippi Code 1972 Annotated, 9-7-171.
[78] Mississippi Code 1972 Annotated, 9-5-135.
[79] Mississippi Code 1972 Annotated, 9-7-131.
[80] Bankruptcy Rules of the United States District Courts for the Southern District of New York 9021-1.
[81] Bankruptcy Rules of the United States District Courts for the Southern and Eastern Districts of New York, Appendix G.

Recommendations

It should not be necessary to replace obsolete references to paper records in state statutes with similar entries for electronic systems that also will become obsolete very quickly. Nor should it be necessary to establish an equivalent of each record series and manual function in the computer. Statutes should provide general, policy-level statements about procedures. Court rules and operational procedures should be much more explicit and detailed, but should not be tied to old ways of doing business.

Electronic Document is Written

It is necessary to equate electronic documents to paper-based writings. Indiana[82] begins with a legal definition that requires electronic information be capable of being displayed in a perceivable form.

> **5-24-2-6 "Writing"**
> Section 6. "Writing" means the following:
> (1) Handwriting.
> (2) Printing.
> (3) Typewriting.
> (4) Information that is created or stored in any electronic medium and is retrievable in a perceivable form.
> (5) All other methods and means of forming letters and characters upon paper or other materials.

While no statutes or court rules addressing electronic filing cover the legal definition of writing, several states have nearly identical code sections relating to digital signature.[83] The following sample is from the Minnesota Statutes Annotated.

> **325K.21. Digitally signed document is written**
> (a) A message is as valid, enforceable, and effective as if it had been written on paper, if it:
> (1) bears in its entirety a digital signature; and
> (2) that digital signature is verified by the public key listed in a certificate that:

[82] Indiana Code, 5-24-2-6.
[83] Utah, Minnesota, and Washington.

(i) was issued by a licensed certification authority; and
(ii) was valid at the time the digital signature was created.

(b) Nothing in this chapter shall be construed to eliminate, modify, or condition any other requirements for a contract to be valid, enforceable, and effective. No digital message shall be deemed to be an instrument under the provisions of section 336.3-104 unless all parties to the transaction agree.

Recommendations

Because there are both similarities and differences between paper and electronic documents, courts should include language that defines computerized pleadings as legal writing. In the future, electronic documents will be nonsequential, nonlinear, nonstatic, and nonadjacent, which will greatly complicate traditional terminology and legal concepts.

Electronic Document is Usually Deemed to be an Original

Mississippi defines any paper reproduction of a record to be a certified copy. Other states define electronic reproductions as originals, as shown in the examples that follow.

9-1-57. Plan for electronic storage system.[84]

(f) All transcripts, exemplifications, copies or reproductions on paper or on film of an image or images of any microfilmed or otherwise duplicated record shall be deemed to be certified copies of the original for all purposes.

46-3-404 Digitally signed originals.[85]

A copy of a digitally signed message is as effective, valid, and enforceable as the original of the message, unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, effective, and enforceable message.

Section 1.7.2 Standards[86]

F. Original Document. A Digitally Signed electronically filed document as it resides on the Court's computer, and print-outs of said document, shall be considered originals satisfying the best evidence rule (Cal.Ev.Code s 1500). The Court may require the party to produce the original of an exhibit that has been filed electronically.

[84] Mississippi Code 1972 Annotated, 9-1-57.
[85] Utah Code Annotated, 46-3-404.
[86] Santa Clara County Superior Court Local Rule 1.7.2.

Recommendations

As computer display technology improves, paper will cease to be the primary medium for exchanging information. Our legal system must begin to adapt to this change by granting full legal status to electronic information. Documents created, transmitted, stored, and displayed electronically must be considered to be originals. This will open many other issues, as documents become dynamic more complex, hyperlinked to pages all over the world. Because these links change, it will be necessary to define a document at a particular point in time. Defining an electronic document as an original is only the first of many steps in adapting our legal system to changing technology.

Electronic Document is Conditionally Deemed to be Signed

A signature on a document once carried certain representations to the court under an old version of Rule 11(a) of the federal rules of civil procedure. The federal rule has been changed, but many courts still use it in their state rules. While the need for original signatures on documents has been relaxed somewhat, tradition is not easily abandoned. Early word processing systems could not incorporate signatures, only ASCII text. Courts around the country came up with original and creative ways to reconcile the desire to use new technology with the need to preserve tradition.

Rhode Island's bankruptcy court equates an electronic signature to an original signature on a document.

> **Rule 5081-1. Signatures--Judges**[87]
>
> **Use of Judge's Endorsement Stamp or Electronic Signature.** The Clerk, and/or his/her designees, are authorized to use the Bankruptcy Judge's endorsement stamp, or a computer generated or electronic signature, which shall serve as the original signature of the Court, on orders entered in accordance with the July 12, 1996 Order Delegating Authority to Clerk to Act on Court's Behalf in

[87] Bankruptcy Rules of the United States District Courts for the District of Rhode Island, Rule 5081-1.

Matters Specifically Delineated, or any subsequent amendments/modifications/additions thereto, and as further authorized in R.I. LBR 5075-1.

Ohio's rules assume a signature on an electronic document to be authentic.

Civil Rule 5 Service and Filing of Pleadings and Other Papers Subsequent to the Original Complaint[88]

(E) Filing with the court defined

The filing of pleadings and other papers with the court, as required by these rules, shall be made by filing them with the clerk of court, except that the judge may permit the papers to be filed with the judge, in which event the judge shall note the filing date on the papers and forthwith transmit them to the office of the clerk. Local rules may provide for the filing of pleadings and other papers by electronic means. Any signature on electronically transmitted pleadings or papers shall be considered that of the attorney or party it purports to be for all purposes. If it is established that the pleadings or papers were transmitted without authority, the court shall order the filing stricken.

This Oregon statute simply eliminates the requirement for a signature but indicates that law enforcement officers have the same responsibilities as if they had signed the complaint.

153.770. Electronic filing of complaint for offenses subject to citation by uniform citation.[89]

(1) A law enforcement officer, following procedures established by court rule, may file a complaint with the court by electronic means, without an actual signature of the officer, in lieu of using a written uniform citation. Law enforcement officers who file complaints under this section will be deemed to certify to the complaint and will continue to have the same rights, responsibilities and liabilities in relation to those complaints as to complaints that are certified by an actual signature.

In this instance, attorneys are required to keep a signed copy of the document on file in their offices; ASCII word processing documents indicate who signed the paper version.

[88] Ohio Rules of Civil Procedure, Rule 5.
[89] 1996 Oregon Revised Statutes, 153.770.

CLAD ADMINISTRATIVE PROCEDURES[90]

C. Signatures; Affidavits of Service.

1. Original signatures on pleadings, affidavits, and other documents filed electronically shall not be filed with the Office of the Clerk. Each party electronically filing a pleading or other documents on the CLAD BBS (whether or not in conjunction with a conventional filing of a document related thereto) shall maintain in his or her files the original signature on the original paper copy of said pleading or other document. However, the pleading or other document electronically filed shall indicate a conformed signature, e.g., "s/Jane Doe".

2. Affidavits of service shall no longer be filed with the Office of the Clerk and shall not be filed with the CLAD BBS. Each party electronically filing a pleading or other document on the CLAD BBS (whether or not in conjunction with a conventional filing of a document related thereto) shall maintain such affidavits of service in his or her files.

Delaware allows use of a password to substitute for signing the document.

INTERIM RULE 79.1 COMPLEX LITIGATION AUTOMATED DOCKET[91]

9. The utilization of a password for the purposes of filing a pleading shall constitute a signature of the registrant of that password under Superior Court Civil Rule 11.

In this New York bankruptcy court, the initials of the filing party, with the last four digits of his or her social security number concatenated to it, constitutes the signature on the electronic document. The original signed document must be kept in the attorney's file.

APPENDIX G. IN RE: PILOT PROGRAM FOR COMPLEX LITIGATION AUTOMATED DOCKET, GENERAL ORDER M-134[92]

3. With respect to the electronic filing of pleadings and other documents on CLAD BBS, the filing party shall identify the initials and last four digits of the social security number of the attorney signing such pleading or other document, which shall constitute a signature of the responsible attorney under Rule 9011 of the Federal Rules of Bankruptcy Procedure; and the original signature of the attorney approving said pleading or other document shall be maintained in that attorney's files.

---

[90] Bankruptcy Rules of the United States District Courts for the Southern and Eastern Districts of New York, Appendix G.

[91] Delaware Superior Court Rules of Civil Procedure, Interim Rule 79.1, Complex Litigation Automated Docket.

[92] Bankruptcy Rules of the United States District Courts for the Southern and Eastern Districts of New York.

Nevada law requires the image of a signature on any electronically filed document.

> **62.206 Electronic filing of certain documents.**[93]
> 2. Any document that is filed electronically pursuant to this section must contain an image of the signature of the person who is filing the document.

New Mexico takes a flexible approach, delegating authority to deal with authentication to a commission. Texas uses a similar approach.

> **14-3-15.2 Electronic authentication; substitution for signature.**[94]
> Whenever there is a requirement for a signature on any document, electronic authentication that meets the standards promulgated by the commission may be substituted.

> **403.027. Digital Signatures**[95]
> (a) The comptroller may establish a procedure for a person to provide a digital signature for any document or data submitted to the comptroller if the comptroller determines the procedure will provide a degree of security and authenticity at least equal to that provided by a manual signature.

Several states allow the digital signature to substitute for the manual signature on paper. This example is from Texas.

> **2.108. Digital Signature**[96]
> (a) A written electronic communication sent from within or received in this state in connection with a transaction governed by this chapter is considered signed if a digital signature is transmitted with the communication.
> (b) This section does not preclude any symbol from being valid as a signature under other applicable law, including Section 1.201(39).
> (c) The use of a digital signature under this section is subject to criminal laws pertaining to fraud and computer crimes, including Chapters 32 and 33, Penal Code.
> (d) In this section "digital signature" means an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.

Virginia satisfies the signature requirement by having an attorney submit a facsimile of the signature on a separate document.

---

[93] Nevada Revised Statutes, 62.206.
[94] New Mexico Statutes 1978, 14-3-15.2.
[95] Texas Statutes and Codes Annotated, 4A-403.027.
[96] Texas Statutes and Codes Annotated, 1A-2.108.

17-83.1:4 Signature; when effective as originals.[97]

If the sender of an electronically filed document files an affidavit of authenticity along with the electronic filing and the electronic transmission bears a facsimile or printing of the required signature, any statutory requirement for an original signature shall be deemed to be satisfied. Any reproduction of the electronically filed document must bear a copy of the signature. The electronically reproduced document shall be accepted as the signature document for all court-related purposes unless the original with the original signature affixed is requested by motion of one or more parties to a pending action or is otherwise required by law. If the court grants the motion of a party, the order shall provide that the original be filed with the court.

In what is perhaps the most unusual approach, a Pennsylvania federal court requires each attorney to submit a signature document to the court, then include an authorization statement with any document filed electronically.

XLI. ELECTRONIC FILING AND RETRIEVAL OF DOCUMENTS[98]

A. Signature Documents. Each attorney with an electronic filing account must submit one original signature document to the Clerk of Court to be appended to each electronic submission. Any electronic document that does not have a signature document on file will be returned to the attorney. In addition, the attorney must submit a Signature Document Authorization Statement with each electronic submission.

The Signature Document Authorization Statement will authorize the Clerk to append the signature document. The Authorization Statement should state: I hereby authorize the Clerk of Court to append my signature document, on file in the Clerk's Office, to this electronic submission.

New Hampshire makes an emphatic statement concerning its feelings about electronic documents and electronic signatures.

Local Bankruptcy Rule 9004-1. Papers—Requirements of Form[99]

(h) Electronic Filing. Electronically transmitted facsimiles or other substitute copies of documents shall not be construed to be signed original pleading documents.

Michigan allows the use of an electronic citation, unless someone notices that there is no signature on it.

---

[97] Code of Virginia, 17-83.1:4.
[98] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.
[99] Bankruptcy Rules for United States District Court for the District of New Hampshire, Rule 9004-1.

Rule 6.615 Misdemeanor Traffic Cases[100]

(D) Contested Cases.

(1) A contested case may not be heard until a citation is filed with the court. If the citation is filed electronically, the court may decline to hear the matter until the citation is signed by the officer or official who issued it, and is filed on paper. A citation that is not signed and filed on paper, when required by the court, will be dismissed with prejudice.

Recommendations

The legal definition of a signature and requirements for proving the authenticity of documents will undergo significant changes in coming years as new technologies are introduced. Courts must decide how much they are willing to invest in ensuring the integrity of electronic documents. Any decision that is made today certainly will be remade every few years. For now, find a method that works and be prepared to adopt better approaches as they become available.

Paper Original, or Follow Up Filing, is Not Required

Three interesting facts are noted in statutes, rules, and procedures concerning submission and retention of paper documents in addition to the electronic filing. Montana requires the original paper records to be retained by the court. Florida requires the submission of paper copies of documents filed electronically, with a procedure to discontinue this practice if the Supreme Court is convinced that paper copies are no longer needed. A federal court in Pennsylvania does not allow paper copies to be filed if a pleading is submitted electronically. This is because they print a security copy as soon as they receive the transmission.

3-1-115. Electronic filing and storage of documents -- rules[101]

(4) The procedures for electronic storage of documents may require but are not limited to the following:

[100] Michigan Court Rules of 1985, Criminal Procedure in District Court, Rule 6.600.
[101] Montana Code Annotated, 3-1-115.

(d) retention of the original documents consistent with other law and security provisions to guard against physical loss, alterations, and deterioration.

Rule 2.090. Electronic Filing of Matters in all Proceedings within the State Courts System[102]

(C) the Supreme Court of Florida has entered an order granting permission to the clerk of court to accept documents filed by electronic transmission. Any attorney, party, or other person who file a document by electronic transmission shall immediately thereafter, file the identical document in paper form, with an original signature of the attorney, party, or other person if a signature is otherwise required by these rules (hereinafter called the follow-up filing).

(2) The follow-up filing of any document that has previously been filed by electronic transmission may be discontinued if:

(A) after a 90-day period of accepting electronically filed documents, the clerk of court or the chief judge of the circuit certifies to the Supreme Court of Florida that the electronic filing system is efficient, reliable and meets the demands of all parties;

(B) the clerk of court or the chief judge of the circuit requests permission to discontinue that portion of the rule requiring a follow-up filing of documents in paper form, except as otherwise required by general law, statute, or court rule; and

(C) the Supreme Court of Florida enters an order directing the clerk of court to discontinue accepting the follow-up filing.

XLI. ELECTRONIC FILING AND RETRIEVAL OF DOCUMENTS[103]

The documents electronically transmitted are in lieu of paper submissions. The attorney making the electronic submission should not transmit a document electronically and also submit the same document in paper form.

APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS[104]

Files Lost Due to Hardware Malfunction. It is remotely possible that an electronically submitted document may be lost on rare occasions due to a malfunction of the court computer. This problem is only likely to occur if the hard disk on the computer should sustain some damage during the few seconds between the time that a user confirms acceptance of the document for submission and a security copy of the document is printed out in the court.

Recommendations

Courts are not, and should not be, risk takers when in comes to the preservation of court records. A redundancy requirement is essential during the testing phases of an

[102] Florida Statutes Annotated Rules of Judicial Administration, 2.090.
[103] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.

electronic filing project, but it will be impossible for courts to realize the benefits of the technology as long as parallel paper systems are in use. Rules should define the period of transition and parallel operation during which paper will continue to be used, and the disposition of paper records received from individuals who lack the capability to submit them electronically.

Paper Copy of Electronic Original May be Used

Courts in two states recognize that paper still may be used in proceedings, even after the implementation of electronic filing systems. The Mississippi statute[105] allows the use of paper in court, while the Los Angeles Superior Court[106] gives a detailed rendition of the various perceptible forms information may take.

> **9-1-57. Plan for electronic storage system.**
> (b) Original paper records may be used during the pendency of any legal proceeding;

> **RULE 18.00 ELECTRONIC FILING AND SERVICE**
> (f) Visible Renditions of Electronic Documents. A visible presentation of an electronic document is equivalent to the original of the document according to the following restrictions:
> (1) A screen display of a document transmitted by facsimile transmission is equivalent to a paper print-out of the transmitted document, if the display of the document image is at a degree of resolution equal to the resolution at which the facsimile is stored in the records of the court.
> (2) A screen display or paper print-out of an electronic document in image form is equivalent to the electronic original, if the display or print-out is at a degree of resolution equal to the resolution at which the document is stored in the records of the court.
> (3) A screen display or paper print-out is equivalent to the original of a textual document.

[104] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.
[105] Mississippi Code 1972 Annotated, 9-1-57.
[106] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.

Recommendations

Until the resolution and convenience of computer displays match paper, courts should continue to allow paper to be used when it is needed. Rules should not restrict the ability of the court to use any visible rendition of information it chooses in conducting its business.

Procedures for Submitting Electronic Documents

It is not enough for a court merely to authorize the use of electronic filing; it must work with potential filers to develop comprehensive instructions. Numerous examples of procedures have been given in this chapter, but few courts have developed administrative manuals with sufficient detail.

Recommendations

The judiciary must consider not only the needs and limitations of court resources, but of law firms and others who will file documents electronically. It must make those procedures available to anyone with an interest in using the system, preferably through a web site that allows continual updates and instant distribution.

Page Limits on Electronic Filings

Two interesting issues arise with respect to the size of electronic filings. First, since electronic documents are formatted differently than paper, how are court-imposed restrictions on document size enforced? The second issue relates to the capacity of the court to accept documents electronically. Should there be size limitations?

The Los Angeles Superior Court answered the first question by limiting the amount of text submitted in an electronic pleading as if it were submitted on paper. Of course,

when documents contain links to web-based materials and when footnotes connect to original references, enforcement of these restrictions will be impossible.

> **RULE 18.00 ELECTRONIC FILING AND SERVICE**[107]
>
> (3) The electronic document is received at an address specified. Rules governing the size of paper, margins, and other specifications based on characteristics peculiar to paper, whether in these or other court rules, shall not apply to electronic documents filed pursuant to this rule, except that such documents, when printed in accordance with the rules governing paper documents, may not exceed any limits on the number of pages that may be filed.

Florida implemented restrictions on the number of pages that could be filed electronically.

> **Rule 2.090. Electronic Filing of Matters in all Proceedings within the State Courts System**[108]
>
> (1) Any clerk of the court who, after obtaining Supreme Court of Florida approval, accepts for filing documents that have been electronically transmitted shall:
>
> (A) provide electronic or telephonic access to its equipment during regular business hours; and
>
> (B) accept electronic transmission of documents up to 10 pages in length.

It should be noted that the Florida rules allow the clerk of court to extend the ten-page limit on documents filed electronically.

Recommendations

Limitations on the number of pages submitted to the court will require parallel paper systems, inhibit the use of the technology, and prevent the court from realizing the full benefits of electronic filing. If needed, limitations should be removed as quickly as feasible. Limitations on the amount of material submitted in a single document will be more difficult to address. At present, we are submitting electronic documents that look like the current paper documents, so traditional page counts are acceptable. Courts

[107] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.
[108] Florida Statutes Annotated Rules of Judicial Administration, 2.090.

should prepare to develop new methods of measuring submissions to account for the limitless capacity of Internet-based information as the nature of documents changes.

Attachments, Appendices, or Exhibits in Different Form

One of the most significant problems for electronic filing pilot projects to date has been how to handle attachments, appendices, and exhibits. Early pilots relied on word processing formats that could only use typewriter characters; it was not possible for them to scan pages or pictures or handwriting. As lawyers create documents electronically, it is a simple matter to pass them along to the court. Often the other materials that are necessary to support the pleading are on paper, not in a computer system.

The Santa Clara County Superior Court[109] and the U.S. District Court for the Eastern District of Pennsylvania[110] require all attachments to be included with the electronic document. The Pennsylvania court also requires all materials to be in ASCII format; no graphics of any kind are allowed.

> **Section 1.7.2 Standards**
>
> A. Electronic Filing. A party may file an electronic pleading or other paper with the Court provided it has executed an agreement with a Service Provider and Digitally Signs the documents filed electronically. Any papers filed shall include exhibits attached.

> **APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS**
>
> Attachments, Appendices, Exhibits to Electronic Submissions. Documents with attachments, appendices or exhibits may only be submitted electronically if they may also be included in full as part of the submission document. This means that if a document is transmitted as an ascii file only attachments, appendices or exhibits that consist entirely of ascii text files may be submitted. No document may be electronically submitted that has attachments, appendices or exhibits that consist of graphs, drawings or pictures of any other non-ascii characters.

[109] Santa Clara County Superior Court Local Rule 1.7.2.
[110] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.

Recommendations

Fortunately, technology has advanced to the point that images of paper documents can be processed nearly as quickly, inexpensively, and easily as word processing files. Because there are so many formats available, courts should define specific standards for attachments to pleadings. The lesson to be learned from earlier pilots is that these technologies will change rapidly, so courts should prepare to upgrade their standards periodically. Today HTML[111] may appear to be the format of choice. Within a year or two, XML[112] certainly will replace it. Who knows what will be the best choice in five years?

Filing Time

Electronic filing of documents eliminates barriers of time in accessing the court. No longer are parties and attorneys limited to court staff work schedules in reviewing materials and submitting pleadings. An interesting question is raised concerning deadlines for filing. Several courts have developed similar rules concerning acceptance of documents.

> **RULE 18.00 ELECTRONIC FILING AND SERVICE**[113]
>
> (d) Time of Filing. An electronic document may be electronically submitted to the court at any time of the day, and shall be considered filed on the date and time that it is accepted. Acceptance shall be determined by the clerk, and shall be deemed to occur (i) on the date the filing was submitted if the submission began during normal business hours of the clerk's office, and (ii) on the next day the clerk's office is open for business if submission began after normal business hours of the clerk's office. Notwithstanding the foregoing, the court may authorize the electronic filing service to automatically accept certain electronic documents specified on a list provided by the court and published by the electronic filing service, in which case such filings shall be deemed accepted as of the date and

[111] *Hypertext Markup Language*, the document format of the World Wide Web, based on an earlier publishing standard known as SGML (*Standard Generalized Markup Language*).
[112] *Extensible Markup Language*, a successor to HTML that incorporates many of the features of SGML and adds extensions to link documents with databases.
[113] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.

time the filing was submitted, regardless of whether the office of the clerk is open for business.

Section 1.7.2 Standards[114]

C. Return Notice of Filing. The Court shall return to the sender of an electronic filing a Digitally Signed confirmation of the acceptance or rejection of the filing. The confirmation shall include a notation of the date of filing.

D. Date of Filing. A filing accepted by the Court will be deemed filed on the date of transmission if received during normal business hours of the Court and on the next Court business day otherwise.

Rule 2.090. Electronic Filing of Matters in all Proceedings within the State Courts System[115]

(3) The filing date for an electronically transmitted document shall be the date the last page thereof is received by the court or clerk of the court.

APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS[116]

Effective Filing Date and Time for Electronically Submitted Documents. The date and time that the document is transmitted will be considered as the "Date Filed" for the document. In most cases, documents will be reviewed within a few hours after they are received on the Court machine. The only exceptions will be documents that are electronically submitted after normal office hours (8:30 am to 5:00 pm EST) Monday thru Friday, documents submitted on weekends and documents submitted on holidays. Documents submitted during the exception periods will be promptly reviewed on the next court business day.

One court indicates when documents filed electronically will be available for review by remote users. The delay is based on processing time needed by the court.

CLAD ADMINISTRATIVE PROCEDURES[117]

V. Availability of Documents Electronically Filed.

A. CLAD BBS. Documents filed electronically are immediately available for retrieval on the CLAD BBS.

B. CLAD Private Database. Documents filed electronically are also available for retrieval on the CLAD Private Database as follows:

1. Documents which are electronically filed by 7:30 a.m. will be available for viewing on CLAD by 11:00 a.m.;

2. Documents which are electronically filed by 11:00 a.m. will be available for viewing on CLAD by 3:00 p.m.;

---

[114] Santa Clara County Superior Court Local Rule 1.7.2.
[115] Florida Statutes Annotated Rules of Judicial Administration, 2.090.
[116] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.
[117] Bankruptcy Rules of the United States District Courts for the Southern and Eastern Districts of New York.

> 3. Documents which are electronically filed by 3:00 p.m. will be available for viewing on CLAD by 5:00 p.m.;
> 4. Documents which are electronically filed by 5:00 p.m. will be available for viewing on CLAD by 7:00 p.m.;
> 5. Documents which are filed after 5:00 p.m. will be available for viewing on CLAD by 11:00 a.m. on the next business day.

Recommendations

Because filing deadlines can be a controversial issue, it is important that the court is clear on when a pleading is accepted. If there will be a processing delay for the filed paper, rules should specify when it will be available.

Standards for Organizing, Identifying, and Indexing Documents

One state requires court leaders to develop a plan for managing electronic documents. The Mississippi statute is shown below.

> **9-1-57. Plan for electronic storage system.**
> (c) The plan shall include setting standards for organizing, identifying, coding and indexing so that the image produced during the duplicating process can be certified as a true and correct copy of the original and may be retrieved rapidly…

Recommendations

While this is an important part of system planning and design, it seems odd to include this type of detail in state statutes. The only circumstance where it seems appropriate is if individual courts are developing their own systems independently and the state court administrator is attempting to coordinate and insure the compatibility of these efforts.

Acknowledgment of Receipt

There are several methods of acknowledging receipt of electronically filed documents. In the first example, the court posts messages concerning pleadings that have been submitted and requires the parties to determine if their documents have been accepted.

APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS[118]

Filing Status Messages. Individual attorneys will be expected to access the electronic filing system periodically to check either private or public messages regarding the status of any electronic submissions. Both acceptance and rejection messages relative to an attorney's electronic submissions will appear under private messages. Information relative to submissions by any attorneys that are accepted for filing within the previous few days will appear under public messages.

Courts in Nevada,[119] Los Angeles,[120] Santa Clara,[121] and Virginia[122] have developed a variety of electronic acknowledgment processes.

171.103 Court clerk may accept complaint filed electronically; procedure; service.

2. If a court clerk accepts a complaint that is filed electronically pursuant to subsection 1, the court clerk shall acknowledge receipt of the complaint by an electronic time stamp and shall electronically return the complaint with the electronic time stamp to the prosecuting attorney. A complaint that is filed and time-stamped electronically pursuant to this section may be converted into a printed document and served upon a defendant in the same manner as a complaint that is not filed electronically.

RULE 18.00 ELECTRONIC FILING AND SERVICE

(c) Return Notice of Filing. Upon receiving an acceptable electronic document, the electronic filing system or clerk shall return to the sender a statement confirming acceptance of the filing. The confirmation shall include a notation of the date and time of filing. If an electronic document is received but unacceptable, the electronic filing system or a clerk shall also notify the sender of the document's rejection and the grounds for rejection. A copy of this confirmation or rejection will be retained in the permanent electronic case file maintained by the court.

Section 1.7.2 Standards

C. Return Notice of Filing. The Court shall return to the sender of an electronic filing a Digitally Signed confirmation of the acceptance or rejection of the filing. The confirmation shall include a notation of the date of filing.

17-83.1:3 Completion of electronic filing; transmission and distribution of data.

A. To complete an electronic filing:

---

[118] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.
[119] Nevada Revised Statutes, 171.103.
[120] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.
[121] Santa Clara County Superior Court Local Rule 1.7.2.
[122] Code of Virginia, 17-83.1:3.

1. The person filing an instrument with the circuit court clerk must transmit the instrument electronically;

2. The receiving station must transmit acknowledgment to the sending party by encoding electronic receipt of the transmission;

3. The sending station must encode validation of the encoded receipt as correct; and

4. The receiving station must respond by encoded transcription into the computer system that validation has occurred and that the electronic transmission has been completed.

Recommendations

Courts should provide electronic acknowledgment of filing transactions. Unless there are high-security risks, these procedures should be as simple as possible. A computer-generated electronic mail message with a date and time stamp may be sufficient in most circumstances. Digitally signing the acknowledgment may be overkill, unless all the steps are built in to an electronic mail or similar program.

Electronic Issuance of Summons

Two California courts have planned for the issuance of a summons electronically. Both local rules indicate that the electronic summons shall have the same effect as one issued on paper, but the Los Angeles rule requires that it be printed.

RULE 18.00 ELECTRONIC FILING AND SERVICE[123]

(e) Electronic Issuance of Summons. On request, the electronic filing system may issue a digitally signed summons bearing a graphical image of the seal of the court. A printed version of such summons shall have the same force and effect as a summons issued by the clerk on paper and under the seal of the court.

Section 1.7.2 Standards[124]

E. Electronic Issuance of Summons. A Digitally Signed summons issued via the electronic filing system shall be as valid as a summons issued by the clerk on paper and under the seal of the Court.

[123] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.
[124] Santa Clara County Superior Court Local Rule 1.7.2.

Recommendations

Electronic filing of documents by attorneys is only the first step in the move to conduct court business electronically. As courts are able to create, maintain, and distribute their work products in electronic form, greater benefits of speed, accuracy, efficiency, and effectiveness will be realized. The electronic summons is a good beginning.

Electronic Service

Several different approaches are outlined for electronic service of process. The Pennsylvania[125] federal court requires traditional service of a paper document.

> **APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS**
>
> The attorney making the submission will still be required to serve other counsel in the case with paper copies of any electronically submitted document and take care to ensure that the informational content of the copies served on other counsel is exactly the same as that of the electronic submission.

Nevada[126] requires that the electronic document be printed and served.

> **171.103 Court clerk may accept complaint filed electronically; procedure; service.**
>
> 2. If a court clerk accepts a complaint that is filed electronically pursuant to subsection 1, the court clerk shall acknowledge receipt of the complaint by an electronic time stamp and shall electronically return the complaint with the electronic time stamp to the prosecuting attorney. A complaint that is filed and time-stamped electronically pursuant to this section may be converted into a printed document and served upon a defendant in the same manner as a complaint that is not filed electronically.

Delaware's rules[127] equate electronic filing with service, but require that a notice of service be served by hand or facsimile. The New York bankruptcy court[128] has similar requirements.

---

[125] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.
[126] Nevada Revised Statutes, 171.103.

INTERIM RULE 79.1 COMPLEX LITIGATION AUTOMATED DOCKET

12. The electronic filing of a pleading or paper will be considered service under Superior Court Civil Rule 5. However, counsel shall be required to serve by hand or fax, on all Delaware counsel appearing in that case and file with the Prothonotary, a notice of service under Rule 5 in the following form:

Please take notice that the following pleading has been electronically filed by (name of party) on the Complex Litigation Automated Docket for the Superior Court of the State of Delaware on _____, 1991: (name of pleading).

Signature of Delaware Counsel

Florida's rule[129] simply authorizes electronic service.

Rule 2.090. Electronic Filing of Matters in all Proceedings within the State Courts System

(d) Service.

(1) Electronic transmission may be used by a court for the service of all orders of whatever nature provided the clerk, together with input from the chief judge of the circuit, has obtained approval from the Supreme Court of Florida of the specific procedures and program to be used in transmitting the orders. All other requirements for the service of such an order shall be met.

(2) Any document electronically transmitted to a court or clerk of the court shall also be served on all parties and interested persons in accordance with the applicable rules of court.

The superior court in Santa Clara County, California, authorizes use of a service provider.[130]

Section 1.7.2 Standards

G. Electronic Service. In circumstances where a document may be served by paper mail or fax, a document may be served electronically via a Service Provider. Service is completed at the time of transmission, and service that occurs after 5 p.m. shall be deemed to have occurred on the next Court day.

Finally, Los Angeles[131] authorizes service to an electronic mail address.

RULE 18.00 ELECTRONIC FILING AND SERVICE

(g) Electronically Mailed Service. In circumstances where a document may be served by paper mail or fax on a person who has executed a contract with the court for electronic filings.

---

[127] Delaware Superior Court Rules of Civil Procedure, Interim Rule 79.1, Complex Litigation Automated Docket.

[128] Bankruptcy Rules of the United States District Courts for the Southern and Eastern Districts of New York.

[129] Florida Statutes Annotated Rules of Judicial Administration, 2.090.

[130] Santa Clara County Superior Court Local Rule 1.7.2.

[131] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.

(1) A textual document may be served on such person by electronic mail to the receiver's electronic mail address;

(2) A document in image form may be served on such person by electronic mail to the receiver's electronic mail address with the prior, written consent of the receiver.

An electronic mail address is refutably presumed valid for a particular receiver if the receiver files electronic documents in court from the address, and the sender has no notice that the address is invalid. If served pursuant to this rule, time is calculated as set forth in Code of Civil Procedure section 1013(e).

Recommendations

Court rules should authorize electronic service of process, allowing continued use of traditional methods for those who are not ready or able to use the new technology. The CLAD approach of posting pleadings and notifying parties of their availability for online viewing overcomes many of the problems of compatibility of documents and images, particularly if it is implemented using World Wide Web technology.

Private Service Providers

As electronic commerce becomes more commonplace, private service providers may play a similar role as is played by the post office and telephone companies in moving documents to and from the court. Los Angeles[132] and Santa Clara[133] counties have adopted rules that allow the contractual use of these vendors.

RULE 18.00 ELECTRONIC FILING AND SERVICE

(b) Enhanced Service: Contractual Requirements. Filing documents electronically is an enhanced information service provided by arrangement with one or more private-sector firms under contract with the court. Such a firm may require payment of a fee and/or impose other reasonable requirements by contract with the filing litigant or the litigant's attorney as conditions for processing an electronic filing.

Section 1.7.1 Definitions

A. Service Provider. "Service Provider" means a private sector firm or other business entity authorized by the Court to provide electronic filing services. A Service Provider is contractually obligated to provide specified electronic services

[132] Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service.
[133] Santa Clara County Superior Court Local Rule 1.7.2.

to the Bar, the public and the Court, to transfer filings and messages to and from the Court, and to act as Certification Authority.

In addition, states that have adopted digital signature legislation have provided for independent, private sector certification authorities to ensure the integrity of the private and public key system. Florida's statute[134] is listed below as an example.

282.745. Voluntary licensure

(1) The Secretary of State may adopt, amend, or repeal any rules as necessary, pursuant to chapter 120, to implement, enforce, and interpret the voluntary licensure of private certification authorities. Such rules shall provide, at a minimum, for:

(a) Licensing fees sufficient to support the licensing program.

(b) Standards and requirements for voluntary licensure.

(c) Audit procedures and requirements to assure program compliance.

(d) Insurance reserve or bonding requirements.

(e) Procedures for license revocation and suspension for failure to meet licensure requirements or for misconduct.

(2) No private certification authority shall be required to obtain a license from the Secretary of State pursuant to this section.

(3) The Secretary of State may also enter into reciprocity agreements with other jurisdictions on behalf of this state to allow for the fullest possible recognition of digital signatures executed under Florida law and the fullest possible recognition of certification authorities licensed under this section.

Recommendations

A more detailed discussion of policy issues related to private sector involvement in electronic filing projects is included in the next chapter. Most courts have not addressed the issue of using vendors to assist their efforts to implement electronic filing. If these companies are performing functions that have been or might be done by court staff, then rules governing how they operate seem appropriate.

Santa Clara County's requirement that electronic filing service providers also function as certification authorities seems at odds with attempts by other states to keep

[134] Florida Statutes Annotated, 282.745.

these certification authorities in a more neutral position. Courts should consider the implications of this approach before adopting similar rules.

Assumption of Risk for System Failure

Two courts address the issue of who is responsible for failure of the technology to deliver an electronic document. In the Eastern district of Pennsylvania,[135] users are required to resubmit a document if they do not receive a document review message. Florida rules[136] require the filer to assume all risks associated with interrupted service or system failure.

> **APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS**
>
> Files Lost Due to Hardware Malfunction. It is remotely possible that an electronically submitted document may be lost on rare occasions due to a malfunction of the court computer. This problem is only likely to occur if the hard disk on the computer should sustain some damage during the few seconds between the time that a user confirms acceptance of the document for submission and a security copy of the document is printed out in the court. In these instances, users will not receive a document review message and should contact the Electronic Filing System Administrator by calling 597-5860. Any lost documents will then have to be resubmitted. It must be emphasized that this type of problem is extremely rare and may never occur.

> **Rule 2.090. Electronic Filing of Matters in all Proceedings within the State Courts System**
>
> (e) Transmission Difficulties. Any attorney, party, or other person who elects to file any document by electronic transmission shall be responsible for any delay, disruption, interruption of the electronic signals, and readability of the document, and accepts the full risk that the document may not be properly filed with the clerk as a result.

In addition, many states have adopted extensive legislation concerning liability and assumptions of risk related to the use of digital signature.[137]

---

[135] Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania.
[136] Florida Statutes Annotated Rules of Judicial Administration, 2.090.
[137] See, e.g., Utah Code Annotated, 46-3-402, Revised Code of Washington Annotated, 19.34.310, 19.34.350, and 19.34.410.

Recommendations

Although courts may gain comfort in assigning all of the risks of technology problems to users of the system, more helpful are instructions, adopted in operational procedures, that help litigants and attorneys understand how to know if a document has not been received successfully by the court, and how to remedy the situation.

Chapter 4: Management and Policy Issues

This chapter covers numerous management and policy issues a court faces as it implements electronic filing. The introduction of technology can upset the operation of an entire court system, the people, procedures, papers, equipment, space, funding, and other resources that comprise judicial branch processes. Adjacencies may be altered and the roles of court staff may change significantly. While technology may eliminate or simplify many tasks, it simultaneously introduces new ones that must be assigned and absorbed into existing processes. Many of these non-technical issues may seem insignificant, but they can be critical to the success of the electronic filing project.

It is not appropriate to force technology to fit into an existing environment. Forcing new tools on old structures will not work because technology permits different and more efficient work processes, yet includes the potential for heightened risks that can accompany computerization. Furthermore, court leaders should recognize the opportunity to break with counterproductive traditions by modernizing court processes when introducing significant technological change to the judicial branch.

The reason management and policy issues require such close attention is that electronic court filing is about more than technology. Technologists focus on technology and sometimes fail to recognize management and policy issues. Court leadership must evaluate the potential benefits from changing current processes without being blinded by electronic glitter.

The following list represents management and policy issues that should be considered by court leaders before implementing an electronic filing system. The discussion of each of these topics fills the rest of this chapter.

- Payment of filing fees.
- Network and system capacity.
- Security.
- Authentication.
- Privacy and public access.
- Records retention.
- Service providers.

Payment of Filing Fees

Courts collect filing fees, copy and certification fees and certain fines and collections from their customers. These fees generally are collected pursuant to statutes and rules. The clerks of court are charged statutorily with properly managing this function, and therefore are rightfully careful and cautious about handling money.

Historically, the payment for a filing has accompanied paper brought to the filing counter. As a party delivered a document to the court, fees were assessed and collected by the clerk. When documents arrive at the court electronically, how will filing fees and other charges be paid? Dollars cannot be created and transmitted in the same manner as word processing documents.

Some courts are exploring the area of electronic payment for services. They have developed methods to collect fees for providing access to records electronically, whether on tape/diskette or through computers.

Five payment systems currently are available to courts implementing electronic filing. A court may employ combinations of these methods, as needed. They are electronic funds transfer, escrow accounts, credit and debit cards, direct billing, and digital cash.

Electronic funds transfer

One of the easiest ways to collect filing fees automatically is to set up an electronic funds transfer system. When attorneys register to file documents electronically, whether

with the court or through a private service vendor, they can provide bank account numbers from which filing fees will be drawn. Similarly, vendors can give subscribers the option to have the vendor pay the filing fee electronically, and then bill the attorneys for the fees. The court provides a list of charges to its bank, along with the attorney or vendor account numbers. The bank then transfers the filing fees to the appropriate court revenue account. Attorneys receive notification of all transactions and can correct errors by contacting their service provider or the court.

If there are insufficient funds in the attorney's account to cover a transaction, the court handles the problem the same way it does a bounced check. Of course, attorneys would be required to notify the court of changes in bank account numbers. It should be noted that frequently there are service charges associated with electronic funds transfer – charges that many filers may find prohibitive when added to each and every fee transaction with the court.

An important feature of the electronic funds transfer system is that bank account numbers need not be sent through the Internet. Account numbers can be registered at the court, which can include them with transaction information sent to the bank via a direct dial-up or private network connection.

Electronic funds transfer, once fully implemented, can be an effective method of collecting fees. If courts run their own filing service, however, then establishing and maintaining the account information and reconciliation will require greater court staff resources, and more careful attention, than processing cash or checks.

Escrow accounts

An escrow account can be established for a case. The attorney creates the account by depositing funds with the court or a disinterested third party, depending on judicial

branch procedures. As documents are filed, the court transfers sufficient funds from the escrow account to cover the filing fees. The attorney or firm is notified if the account becomes depleted.

For example, an attorney may deposit $150 into an escrow account when a complaint is filed with the clerk. The clerk deducts the appropriate amount from the escrow account and holds the remainder to be applied to subsequent filings or copying charges. At the end of the case, any unused balance is returned to the attorney.

This approach works equally well in paper or electronic filing systems, but it has some drawbacks. While it would be practical and more efficient to establish one account for the attorney or firm and apply charges for all its cases to that single account, some practitioners require individual accounts for each case. Each attorney account then has a separate court escrow account, doubling the number of accounts attorneys must manage. Also, not all courts have the expertise to provide interest-bearing accounts with end-of-year financial reporting statements, which also may be required by ethics rules. Finally, with hundreds of thousands of attorneys and other filers, the total amount "stored away" could reach tens of millions of dollars at any given point, and may not be the most efficient use of the money.

In an electronic filing system, an escrow account could be maintained by the court, the electronic filing service provider or a bank or other financial institution. The advantage to the court of using a service provider or financial institution is that the funds could be guaranteed contractually by the organization providing the service. Courts receive payment quickly, with little or no costly billing activity.

While this option is convenient, there are costs to court users. Banks charge fees for establishing, accessing and maintaining accounts, and financial resources of parties or attorneys may be tied up for long periods of time.

Credit and debit cards

Attorneys could provide credit or debit card numbers with documents filed electronically, thus charging their filing fees. Courts would receive payment from the credit card company, though a service charge would be deducted from each transaction. These service charges typically are up to several percentage points of the total transaction amount. Many courts have allowed credit card payment of fines for years.

Courts have found that the convenience of credit cards has increased the percentage of cases for which fine payments are made immediately. With fewer accounts unpaid, the court reduces the cost of managing receivables. Courts also receive payment more quickly from the credit card companies and reduce the risk of losses due to bounced checks. Courts are not dependent upon the cardholder for payment, and rarely does the payer challenge the transaction. Most importantly, credit or debit cards offer a convenient alternative for payment; improved service for the public is an important goal of the judiciary.

Some courts are reluctant to accept credit cards because of the service charge (merchant fee) that accompanies each transaction. Credit card companies, as part of their standard contract, do not allow courts to add a separate service charge to compensate for this fee. Some courts have negotiated lower fees with credit card companies, but most accept them and believe the advantages of increased collections way far outweigh the costs.

Another problem is the security risk of providing credit card numbers over the Internet. Two standards have been developed to alleviate this concern. Many Internet browser programs, such as Netscape and Microsoft Explorer, support Secure Sockets Layer (SSL). SSL creates an encrypted or coded communications link between the person using the browser and the server. A credit card number sent over the Internet using SSL cannot be deciphered by any other machine or router between the two corresponding computers. The United States federal courts are using the SSL browser security system in their electronic filing pilot projects.

Visa and MasterCard designed a second method of securing transmissions over the Internet, called Secure Electronic Transaction (SET). It is described on the Visa Internet page as follows:[138]

> "SET SECURE ELECTRONIC TRANSACTION ™ is a specification designed to utilize technology for authenticating the parties involved in payment card purchases on any type of online network, including the Internet. SET ™ was developed by Visa and MasterCard, with participation from leading technology companies…
>
> SET focuses on maintaining confidentiality of information, ensuring message integrity, and authenticating the parties involved in a transaction.
>
> The significance of SET, over existing Internet security protocols, is found in the use of digital certificates. Digital certificates will be used to authenticate all the parties involved in a transaction."

Direct billing

A more traditional method of collecting filing fees is to bill the attorney or party when the court receives the document. This is more difficult for courts because a billing system must be established and maintained, and it is often more difficult to collect the fees once the court has accepted a document. Parties who are unhappy with the outcome

[138] http://www.visa.com/

of their action might refuse to pay altogether, and the collection costs for one case could exceed the revenue collected for many cases.

Digital cash

At some point in the future, digital cash will be transferred over the Internet as easily as the documents it accompanies. In a secure environment, funds will be deducted from a smart card and moved into the court's revenue account. The communications software will perform most of the processing work, so the overhead associated with these financial transactions would be minimal.

Courts will not be required to maintain account information on attorneys and service providers, only to forward the information provided with the transaction to their bank. The electronic filing servers can complete these processes, so little human intervention will be required.

Current drawbacks are the expense to attorneys of the hardware and software and account management to experiment with digital cash. Later on, issues will arise if attorneys need several cards – one for each client.

Nonetheless, as digital cash enters the mainstream of electronic commerce, its benefits likely will be seen in the area of electronic court filing.

Network and System Capacity

Another management item that at first glance appears to be a "pure" technology issue is network and system capacity. Supporting a network, and providing sufficient capacity is what allows many filers to reach a filing system at peak times. Just as courts staff-up for busy periods during the day for paper filing, electronic filing systems must have enough capacity for busy periods.

There are a few important capacity measures: concurrent users – the number of users who can be on a system or server at one time; bandwidth – the speed at which information is passed between users and the system; and processing speed – speed with which the system carries out its processes. Without sufficient capacity, users such as attorneys will get slow response or "denials of service" from the system and those users will switch back to paper filing.

Security

Security is an important issue for law firms and courts attaching their computers to the Internet. Almost everyone is concerned that data may be altered or removed, viruses may be introduced, or sensitive information may be accessed illegally. Attorneys must protect attorney-client privilege and work-product confidentiality when conducting business electronically. When preparing to implement electronic filing systems, courts should plan to protect their servers from Internet-based attacks by installing electronic in-baskets and firewalls, and by developing reliable transaction logging systems.

Server security

In the May 4, 1998 edition of InfoWorld magazine,[139] Stuart McClure identifies four phases of an Internet attack. They are:

Phase one: Gather information.
Phase two: Gain access.
Phase three: Deny service.
Phase four: Evade detection.

For example, a hacker might see that a court's electronic filing web site allows a new user to establish an account with the court online. The hacker may set up a routine to repeatedly establish new accounts until the disk space on the court site is completely

filled, denying potential new users the opportunity to sign up. Denial of service problems could be particularly troublesome in the early stages of implementation, since skeptics in the court may be looking for reasons to rely on traditional paper filing. Courts must acquire the necessary software and hardware, or contract for these services, to protect their electronic filing systems from Internet attacks. Fortunately, Mr. McClure points out that of the many types of Internet attacks, denial of service attacks are "the easiest types of attacks for an administrator to defend."

What kind of hardware and software are needed to defend against Internet attacks? Chapter 6 discusses the concept of an electronic in-box, a computer that is placed between the court's servers and the Internet connection, outside of the security firewall. The electronic in-box accepts documents filed electronically without allowing outside users access to the internal court computer network. Programs running on court servers have security clearance to pass through the "firewall" to retrieve documents from the in-box computer.

PCWebopaedia defines a "firewall" as:[140]

> "A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranet. All messages entering or leaving the Intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria."

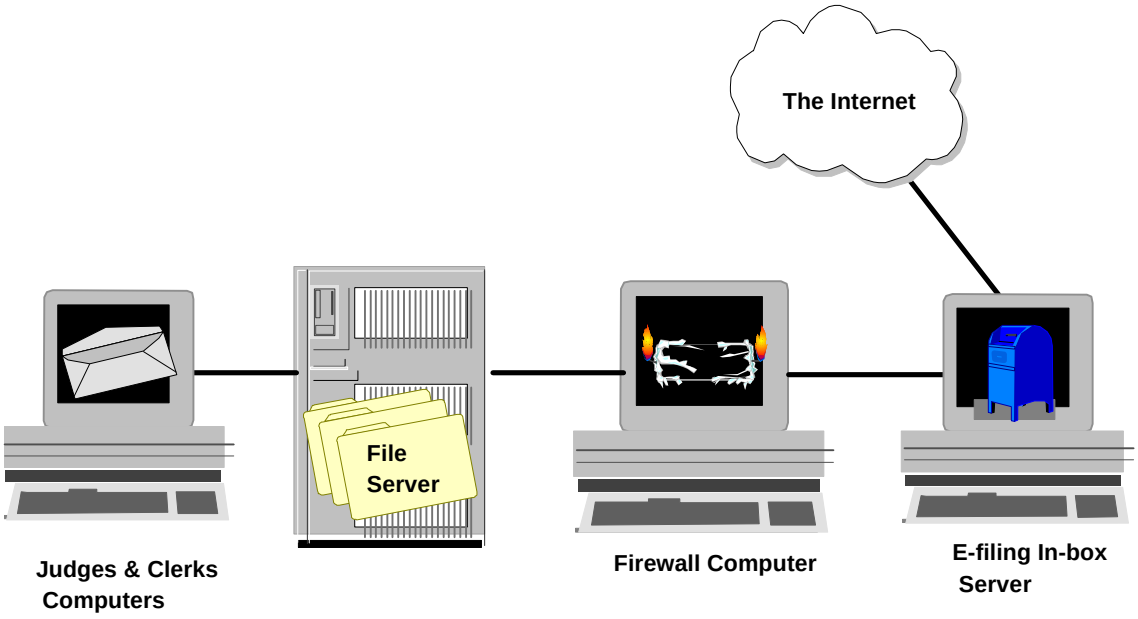
If connected to the Internet, a court should use some type of firewall to protect its internal network. The type of firewall system needed depends upon the type of computer network used and the sensitivity of cases the court hears. There is extensive help

---

[139] Stuart McClure, *InfoWorld Security Suite 16 Debuts*, InfoWorld, May 4, 1998, at http://www.infoworld.com/cgi-bin/displayTC.pl?/980504sb1-iwss16.htm

available from computer security consultants and system vendors who can work with a court or other organization to implement firewall hardware and software systems.

The following diagram shows how the electronic in-box and the firewall are configured to protect the court's information resources.



Notice that the firewall computer stands between the court's file servers and the electronic filing in-box computer. Also, note that both the file server and the firewall are between the judges and clerks using the network and the Internet. This kind of design provides the court's file server and individual computer users with two or three layers of protection, depending on network routing and protocols implemented.

For additional layers of protection, courts can use the secure file encryption software available with all major word processing software packages, and access control. If judges save their documents using a password, those files will be secure from tampering from both internal and external sources. Internal network security can ensure that only

[140] http://www.pcwebopedia.com/firewall.htm/

authorized users can gain access to information and documents stored on certain disk drives and subdirectories.

Transaction logging

Although transaction logging will not prevent attacks on court computer systems, it may help deter them and will help staff analyze and correct security and other technical problems that may damage information resources. Whenever any type of update is made to a database, an exact duplicate of the transaction can be made to a log file, typically kept on a separate computer disk. In the event of a system failure of any type, the backup copy of the database from the previous day can be restored to the disk, and the transactions from the log file can be reapplied, recreating the database as it existed before the problem occurred.

In addition, log files can be examined to determine who made a particular change to the database or accessed the information, if inquiries are logged. These audit trails can be extremely valuable if sensitive information is accessed inappropriately.

Electronic filing systems should log all transactions, at the electronic in-box and on the servers inside the firewall. This logging should:

- Track and store the origin and path of electronic mail coming into the system.
- Track the users attaching to the in-box and their activity, such as submitting a document to the electronic filing system.
- Log the *digital signature* (if used) of any files submitted, to eliminate any question of authenticity or completeness.
- Monitor financial transactions, such as use of credit cards or electronic funds transfer.
- Track the access, copying, and transfer of documents in any part of the electronic filing system.

Transaction log files must be maintained permanently and will be, eventually, printed on paper or transferred to Computer Output Microfilm (COM), CD-ROM, or other type of long-term storage medium.

Authentication

To authenticate a document is to supply evidence to prove the identify its source and to verify the integrity of its content. Historically, signatures have been used for authentication. The court assumes that the document was submitted and its content prepared or authorized by the signer. Signatures are difficult to reproduce, and the process used for detecting impersonators is sufficiently esoteric and well established to discourage forgery. A signature, because it is unique to its owner, can be verified but not stolen. It is also infeasible to reproduce.

Of course, the signature was used for more than authentication of papers. It also expressed the approval or authorization of the signer, the intent that the transaction be legally binding. An old version of federal rule 11, adopted and still in use in some state court rules today (even though it is no longer used in the federal system), listed representations made to the court by a signature. Delaware's Court of Chancery rule is illustrative.[141]

> **Rule 11. Signing of pleadings, motions, and other papers; representations to the Court; sanctions.**
>
> (b) *Representations to the Court.* By presenting to the Court (whether by signing, filing, submitting, or later advocating) a pleading, written motion, or other paper, an attorney or unrepresented party is certifying that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances:
>
> (1) it is not being presented for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation;

[141] Delaware Court of Chancery Rule 11(b).

> (2) the claims, defenses, and other legal contentions therein are warranted by existing law or by a nonfrivolous argument for the extension, modification, or reversal of existing law or the establishment of new law;
>
> (3) the allegations and other factual contentions have evidentiary support or, if specifically so identified, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery; and
>
> (4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on a lack of information or belief.

Other devices, in addition to signatures, have been used to authenticate documents. A notary public is authorized by state or federal government to administer oaths and attest to the authenticity of signatures on papers. Official seals once played an important role in verifying the authenticity of documents. Today, a date and time stamp is used by most courts to show when a pleading was submitted and that it is the same document originally submitted. In some states, staff is not allowed to remove staples from original documents out of fear that the authenticity of the submission might thereby be questioned.

While none of these techniques can guarantee that the purported sender submitted the document and that it has not been modified during or since transmittal to the court, our justice system has functioned effectively with this level of certainty. The introduction of photocopy and word processing technology did not raise serious questions about document authenticity, even though it is possible to attach scanned signature images to papers and make subtle yet significant changes to document contents without detection.

The development of document imaging systems first started court leaders and technologists thinking about document authenticity issues. As some courts started to rely on electronic documents as their primary source of information, holding paper versions as backups, these concerns were magnified. With electronic data interchange and electronic filing of pleadings emerging as viable additions or alternatives to paper systems, guaranteeing document authenticity has become a top priority for many.

Chapter 3 discussed passwords, electronic approval, electronic signature (both facsimile and imaging), signature dynamics, and digital signature technologies. This chapter has covered various security systems, such as access control, transaction logging, and encryption, which also can assist a court in authenticating documents.

Court leaders may argue that because authentication of documents is not a problem in the world of paper, it should not be a significant issue in an electronic environment. All documents are assumed to be authentic when the courts receive them. Because there are techniques for detecting and correcting problems with papers submitted to the court, those same techniques should be applied in the electronic world. Court leaders often are reluctant to consider large expenditures on digital signature or similar technology.

It must be understood that use of electronic commerce greatly increases the opportunities and the methods available to those who would disrupt judicial branch proceedings, while decreasing the likelihood of getting caught. While physical adjacency to paper documents was required in the past, the number of miles between a hacker and a courthouse is irrelevant. Because risk has been magnified, preparations must be strengthened. For example, in the case of some filings, courts need to know who is an attorney and who is not, and in this instance digital certification can help.

Courts must make policy decisions about which of these authentication techniques are appropriate for their environment. Higher levels of security cost more to acquire and operate. Decisions should be based primarily on two factors, strength (or effectiveness) and cost (or efficiency). The chapters that follow will provide insights into the costs of various approaches.

Privacy and Public Access

Technology is changing the nature of court operations. What was once a completely manual, paper system is now becoming high-tech and electronic. Information is now available from multiple sources, paper files and computer databases. Electronic information is much easier to access than that stored on paper. This increased accessibility has raised questions about the appropriateness of traditional practices and rules. Traditional full and unfettered (albeit slow and expensive) access to court data can create significant problems for the judiciary and for those involved in court cases. Once electronic filing becomes a mainstream technology and the focus shifts from limited data about the case to the contents of all the documents in the file, the magnitude of both the benefits and concerns surrounding access issues will increase even more.

This section first will review public access and privacy issues separately, then show the need to balance the two in determining judicial branch policy with respect to information dissemination. Finally, guidelines for the development of policy will be presented. For a more detailed analysis of this subject, see Susan Jennen's work, entitled *Privacy and Public Access to Court Records*.[142]

Public access

Computerization of judicial processes and the general adoption of electronic commerce in many parts of our society have produced increasing pressure on courts to provide information electronically. While the right of the public to know what government is doing and hold officials accountable for their acts is a part of our custom and tradition, much of the interest in judicial branch data is motivated by different

[142] Susan M. Jennen, *Privacy and Public Access to Court Records* (Williamsburg, National Center for State Courts, 1995).

objectives. Many companies have found that providing data to the public is financially rewarding, particularly when they can shift production costs to a public organization. If a company can obtain data at no charge from a court clerk, add value to it to then sell it to the public or to other businesses, it may reap generous profits. Whether it be a lawyer publishing summaries of jury awards, a credit reporting company collecting judgment information for credit histories, a reporter doing an expose on a judge's sentencing practices, or a business compiling the names of recent divorcees for a mailing list, except where the court is paid (a common practice for tape compilations and record access) the public is bearing the expense of a private sector enterprise when the judiciary generates the data for these activities. How far should courts be required to go in providing free and open access to electronic court records?

A one-time request for information in a single case is far different than a requirement for weekly production of a computer tape containing specific data gathered from multiple computer systems. The volume and frequency of requests typically can overwhelm court technical staff, which usually has more to do for court users than it can handle.

Fortunately, data dissemination requirements placed on the courts have not been unlimited. State and federal law never have provided for completely open records. Discussions regarding how an appellate case will be decided, records of many types of juvenile proceedings, adoption case materials, and court personnel files typically have remained confidential.

Though practice varies from state to state, most courts allow full access to most non-confidential records that have been created in the normal course of business. Although some states require courts to format new records to match the specifications of the requestor, most do not.

Privacy

Federal and state laws have established the right of privacy, or the "right to be left alone."[143] While computerization revolutionizes our ability to access information, it creates opportunities for abuse of individual privacy. Electronic searches can extract personal information from databases that would be impractical to assemble in a paper environment. These searches also can produce inaccurate results, such as listing court cases for people with similar names, with no way to distinguish between correct and incorrect information. Without privacy protections, individuals could be denied employment, insurance, scholarships, and other benefits and opportunities without knowing that the reason for denial was incorrect information obtained from a court database. It is ironic that increased demand for access to information has accompanied similar demands for greater privacy protections.

Our legal system allows court records to be sealed, purged, expunged, or to have access limited to specific purposes. As electronic filing system proliferate, documents will be accessed and may be stored in many locations. Just as they are today when paper records are viewed and/or copied, when the court issues orders to remove or limit access to electronic materials, the orders will be impossible to enforce. Court leaders and legislatures should consider modifying these policies to apply them at the beginning of cases, rather than at the end, or traditional privacy protections may be lost.

Balancing privacy and public access interests

Rights of privacy and access overlap, often conflicting with one another. Federal and state policy provides boundaries, but most state courts have a great deal of discretion within those boundaries. Courts must adopt and follow policies that respect both the

right to know what government is doing and the right to be left alone. Of course, there are other issues that will be a part of this determination, such as the need for confidentiality in certain parts of the judicial process, security needs of the courts and the cost of various solutions.

A California case captures the essence of this balancing act.[144]

> "While there is no question that court proceedings should not be conducted in secrecy, the public's right to information of record is not absolute. Where that right conflicts with the right of privacy, the justification supporting the requested disclosure must be balanced against the risk of harm posed by disclosure."

Laws and practice vary widely from state to state. It is impossible to provide precise guidance as to what the policy of any particular jurisdiction ought to be. The following guidelines were developed by the National Center for State Courts to assist with the process of developing policy that considers both rights of access and privacy.[145]

Guidelines for Policy Development

1. Understand federal and state legal requirements regarding public access and privacy rights. Review the following bodies of law:

U. S. & state constitutions	*State common law*
Federal statutes	*State court rules*
State statutes	

2. Identify the degree of discretion that the court or state judiciary can exercise in defining record access rules, policies, and procedures.

3. Consider court operational issues that may affect discretionary decisions.

4. Analyze electronic court information to facilitate decision-making.

5. Actively share resources and ideas with other state and local courts.

---

[143] Griswold v. Connecticut, 281 U. S. 479 (1965).
[144] Westbrook v. Los Angeles County, 32 Cal. Rptr. 2d 382 (Cal. App. 1994).
[145] Susan M. Jennen, *Privacy and Public Access to Court Records* (Williamsburg, National Center for State Courts, 1995), p. 39.

6. Develop public access policy and practices by balancing the relevant factors within the state and state court system; create a "working" document to record and update findings and conclusions.

Courts want to provide information to the public. They also must protect the privacy of individuals. Yet, they desire to promote the use of technology to increase access to the courts for all citizens. Unfortunately, all these objectives cannot be achieved without compromise. This may be one of the most important areas of policy determination for court leaders.

Records Retention

Management of paper files consumes a great deal of court and law office resources. The introduction of computer systems lowered the cost of collecting and storing it, but not the cost of categorizing it. The introduction of electronic filing and document management systems will introduce new records retention issues that must be addressed. If policy is created with the design of the system, it will be much more effective and cost less to administer.

Retention of paper records

Most courts have faced problems with record storage at one time or another. For many large courts, this is an acute problem that must be managed continually. Overflowing records rooms and inefficient procedures developed to deal with the problem are symptoms of inadequate records management.

Some courts instituted microfilming programs to ensure that older files could always be retrieved. This microfilming originally was done at the conclusion of a case, just before a paper file was sent to an archive or destroyed. Later, as paper management problems produced more and more lost files, some courts began microfilming documents

upon receipt. This resulted in delays in acting on a pleading for as long as a week. Because all the materials in the case file were not on the same roll of microfilm, it was still necessary to film the cases again at the end of processing. Although this may seem like a ridiculous solution, it has been practiced by hundreds of courts throughout the United States.

For a variety of reasons, some courts have created multiple files for the same case. Sometimes this is for purposes of protecting confidentiality—sensitive material is excluded from a file used for public access. Some courts create a separate file for the judge's area. Lawyers representing litigants also maintain files of materials and must deal with storage issues.

Some courts, prosecutors and law firms have procedures for purging files for long-term storage. This procedure consists of reviewing every page in a case file, retaining a few specific documents and discarding the rest. This reduces the size of the case file so it consumes less space in the records room, but the amount of time required to purge each file far exceeds the cost of storage space.

When records rooms become full, many courts use off-site archive facilities for older cases. It requires a great deal of effort to keep track of the location of individual cases to ensure they can be retrieved, if necessary.

At some point, most court case files are no longer needed. Some courts are not allowed ever to destroy these public records, but most eventually purge older materials. Traffic tickets, for example, often are destroyed as soon as the conviction disappears from a person's driving record, roughly three to five years after the case disposition. Felony convictions may be retained permanently.

A final issue with paper files is retrieval. Although very few historical records are ever needed again, occasionally one is required. Courts may spend hours trying to locate these old files.

Records retention and computerization

If there is any universal truth in court automation, it is that judicial branch employees want to have all case information available forever. Were it not for the expense and limitations of technology, electronic archiving never would have been developed for case management systems. As the cost and capabilities of computer hardware have improved, technologists have discovered another problem. While it has become possible and affordable to retain case information for decades, it is still not desirable to do so. The reason is performance. Even though a file of docket records can hold millions of entries, the length of time needed to retrieve an individual record increases with the file size. The index records that track individual entries must be read to locate specific information. If a docket entry can be found with a few reads of the index file, then response time is rapid. As the size of the index file increases, the number of reads on the file will grow, and response time deteriorates to an unacceptable level. It is still wise to manage electronic records just as carefully as paper, to avoid these problems.

The second generation of court computerization moved away from large, centralized computer systems to distributed environments. Smaller minicomputers were placed in individual courts and networked together. This reduced the size of the electronic files and provided better performance on cheaper equipment. These systems were more efficient at their most important work, supporting trial court activities. Generation of statewide statistics became more cumbersome, but the tradeoff was more than worthwhile for everyone at that time.

Even with distributed systems, courts found it necessary to keep file sizes as small as possible by purging older records. Because state criminal history repositories maintain files of convictions and sentences, courts found it easy to remove criminal cases shortly after work was completed. But new legislative initiatives, like *three strikes* and the Brady law, created a greater need to be able to review details of older convictions.

An emerging technology relevant to court case information management is data warehousing. A warehouse is a server that stores information. It is still accessible to court users, but is not stored with active case data. Though it takes a little longer to retrieve, it is still on-line information. Using a data warehouse, courts can maintain *legacy data* indefinitely without hampering day-to-day operations. The warehouse also can be used to consolidate cases from multiple servers for inquiry purposes in a distributed environment.

Electronic filing and records retention

The use of document management systems actually will increase the need for active management of court records for two reasons. First, the electronic case file will be the primary source of information about the case and paper documents will be a backup source. With today's computer systems, the roles of these record types are reversed. Second, as courts implement electronic filing fully, the paper case file will cease to exist. Without tight integration to management systems, documents conceivably could be filed with other papers submitted on the same date, not with pleadings for the same case. It still will be possible to reconstruct a file with paper in case of a catastrophic system failure, but this will require considerably more time and effort.

Because electronic documents require much more space than docket entries describing them in a case management system, the storage needs of courts and law firms

will grow significantly. As with data entries, very large document files will at some point begin to impair retrieval time, degrading system performance. Courts always will be required to manage their information storage resources, regardless of whether they are found in the basement of a building or on an optical disk platter.

Retention policies should be adopted as the system is designed, rather than waiting for performance problems to create a crisis. If a court decided, for example, to flag certain document types for deletion two years after case disposition, it would be a simple matter to begin removing these records when storage space became a problem. If a court waited to make this decision until there was a problem, it would have no way to identify these pleadings without individual review of tens of thousands of pages. The development of electronic records retention policies must be an integral part of system design.

Service Providers

When a court owns and operates its own technology system and chooses to incorporate electronic filing into that overall system, it also takes on the burden and responsibility of a service provider. While, in a sense, courts have always provided services to attorneys, those services have been the traditional ones of a clerk's office, most of which commence only after a pleading has crossed the counter on paper. With electronic filing, there is now a technology service component to be delivered as well.

Some courts will decide to avoid the costs, complexities and potential headaches of the service provider role by allowing third-party, commercial firms to handle the electronic filing component. For courts that already are using a commercially developed case processing system and receiving system support from the vendor, this decision is

almost a foregone conclusion. These courts will be concerned mainly with whether their case management system is tightly integrated to the system capabilities. In addition, many courts that have developed and will continue to maintain their own case management systems may elect not to own the front-end technology needed for electronic filing. Just as some judicial technology departments have let third parties connect electronic public access systems to the court's databases, many courts will turn to outside service providers for electronic filing. When a court decides, for whatever reason, not to take over the traditional private function of courier and messenger, then the choice of a service provider, cost factors and the need to ensure the quality of the service that is delivered become critical issues.

Role of service providers

Service providers may have a varying role in the overall technology and operation of a court, depending upon the characteristics of each court. In some courts, the vendor will assume the maximum role of providing the entire technology infrastructure to support the court. A maximum role would involve providing several components:

- Case management system.
- Electronic public access system.
- Electronic filing interface, consisting of:
  - Interface with court database and case management functions.
  - User interface (client software resident on the attorney's PC).
  - Electronic filing functions, including:
    - Electronic packaging of attorney's documents.
    - Authentication and security.
    - Transmission to court.
    - Time stamp and acknowledgement.
    - Fee processing.
    - Workflow routing for review and approval.
    - Updating of case management system database.
    - Noticing (electronic or hybrid).
- Customer service.
- Installation support.
- Training on-site.

Marketing/promotion.
Upgrades and ongoing enhancements.
Integrated benefits to other systems.
Support for new operating systems, browsers and other filer technology.

A minimal role, on the other hand, could involve providing only a single component, such as a secure dial-up connection for the attorney. In fact, during the early stages of an electronic filing implementation, it may be necessary to provide conversion services to law firms that do not meet the requisite level of computerization to file directly. The Republic of Singapore, for example, which initiated an electronic filing project for civil litigation in 1997, addressed this problem through the use of private "law bureaus." These service firms operate as an intermediary, accepting paper pleadings from law firms and submitting them electronically to the courts.

Just as courier services now exist in most U.S. cities to handle the transportation and physical submission of paper pleadings, there may be an interim role for an "electronic courier" service as courts begin to convert to electronic documents. Such services could be furnished by the vendor that provides the electronic filing system or by independent businesses that are themselves end users of the electronic filing system.

For a given court and legal community, the range of potential functions and services would be delivered through some combination of shared responsibilities among court staff, one or more vendors and law firm staff.

Major issues

When considering the role and responsibilities of an electronic filing service provider, courts must address a number of sensitive issues that have not been of concern in a paper environment. Although there is much overlap, these can be grouped into three categories: policy issues, management and procedural issues and technical issues.

Policy issues:
Allowing a filer to update court database without court supervision.
"Partnership" roles and responsibilities (court—service provider—attorney).
Exclusive *versus* open service provider agreements.
Fee structure and revenue sharing.
Authentication and security standards.
Liability for system "down-time" and transmission failures.

Management and procedural issues:
Financial accounting and billing.
Training of users.
Time stamp (e.g., if an attorney files at 4:59 or 11:59 p.m., how to ensure that the court receives it at the same effective time).
Assurance of noticing.
Future modifications to case management system and database (how to ensure that electronic filing interface will be kept compatible without delays).

Technical issues:
Ease of use.
Method of transmission (e.g., direct dial-up or Internet).
Uptime approaching 24 hours a day.
Sufficient capacity to handle peak volumes.
Speed of total transaction.
Providing secure transactions (attorney to provider, provider to court).

Ensuring satisfactory service providers

Courts have much at stake when they take the significant step forward into electronic filing. While electronic public access systems raise important policy issues as we have discussed, they serve primarily an inquiry function with minimal danger of adversely affecting court records. On the other hand, electronic filing, by design, most definitely affects the content of court records, just as pleadings filed on paper do. Clerks of court should expect to review filing submissions in electronic forms much as they do paper submissions today delivered by lawyers, couriers, messengers and the public. In addition to facing a variety of legal, procedural and technical hurdles, courts must overcome the inertia of tradition and address the doubts and concerns among both court officials and the bar. Consequently, they must exercise great care in selecting the service providers

they rely on for this critical function and ensure that proper safeguards are in place to protect the judicial processes.

Chapter 5: Court Workflow

This chapter documents differences and similarities between workflow in courts that use paper and electronic filing, including the effects of the development of case management technology on paper flow. It also addresses how paper filing will continue in an electronic filing system–the inevitable need to scan paper for parties who lack the means or capability to interact with the courts electronically.

The usual approach to describing workflow is to follow a single piece of paper sequentially through processing steps. While this method provides a good general view of paper flow, it does not reflect the way courts actually work. The division of labor in a clerk's office places related functions together and processes many documents in batches. In other words, a more accurate view of court workflow is gained by examining functions performed by people in the office, not by determining the path a piece of paper has followed. For that reason, this chapter compares differences and similarities between manual and electronic filing systems based on workflow functions. It also examines the use of paper in a fully electronic system.

Differences and Similarities Between Paper and Electronic Workflow Processes

Work necessary to process information is not the same as work required to process paper, the current medium of exchange of information. The implementation of electronic filing introduces a new medium of exchange, but not necessarily new information. Paper processing steps are replaced by more efficient procedures for processing electronic documents, although the information being moved can be the same. It is important to distinguish between *what* is being moved and *how* it is being moved.

This discussion of workflow is organized into four subsections: information processing, paper processing, information processing in a mixed paper and computer world, and electronic document processing. The reason for examining the mixed environment is because the case management system replaces many of the indexing and reporting portions of the paper systems, while leaving case filing systems intact.

Information processing

Information processing is very similar in paper and electronic court environments. A judge, for example, reviews the content of a document and decides whether to grant or to deny a motion. The vehicle used for presenting the information to the judge, be it ink on paper or electronic pixels on a monitor, makes little difference in what is done with the information. Information processing is, then, largely unaffected by the introduction of electronic filing.

On the other hand, electronic information in a court document can be linked directly to other information, making access much easier and quicker. A footnote in a court opinion may refer to a statute or another case. In a paper environment, it may be necessary to retrieve another book (that may or may not be available) to check the reference. In an electronic world, a simple mouse click will make the case or statute appear. Lawyers and judges may have more information available to them with electronic filing, since the barrier of access time has all but been eliminated.

Electronic filing also may affect information quality. When people complete paper forms, they may leave out information or make mistakes that go undetected. When people enter the same information into a computer screen, they may receive immediate feedback if there is an error, allowing them to correct it. In the same way, a document

filing system can provide a lawyer with nearly instant feedback if certain types of problems exist, which should result in higher quality filings.

In addition, documents submitted electronically can provide data to a case management system automatically. This reduces data entry, another potential source of error. It also lowers operational costs significantly.

Information processing in the legal system, then, is enhanced, even if document content does not change. Electronic text and data are available sooner, usually are more complete, and often are more accurate.

Paper processing

> "All records go through the same four-stage cycle: creation or receipt; maintenance; retrieval, use, and distribution; and disposition.[146]"

All of these steps have costs. The medium, paper, has huge costs. Nicholas Negroponte, in his book *Being Digital*,[147] discusses the costs and benefits of converting the atoms of paper and commerce to the bits of the digital world. He starts by discussing the cost and effort of moving "Evian" water (atoms) from France to a meeting in California. He remarks:

> "In the case of Evian water, we were shipping a large, heavy, and inert mass, slowly, painfully, and expensively, across thousands of miles, over a period of many days. When you go though customs you declare your atoms, not your bits."

The current paper-based filing system must be analyzed and dissected to better understand the benefits of electronic filing and storage processes, and working with bits instead of atoms.

---

[146] Skupsky, Martin, Grumer, and Wolfe, *Comparative Record Management Systems and the Courts: Manual and Automated Alternatives*, NCSC publication number R0044, p. 8 (Williamsburg, National Center for State Courts, 1980).

[147] Nicholas Negroponte, *Being Digital* (London, Hodder & Stoughton, 1995).

Creation or receipt

Documents generally are created by attorneys and others outside the court. A Prince George's County, Maryland project estimated the cost of document preparation at approximately $25. This included printing, copying, envelope preparation, and postage. This cost did not include fast delivery services, such as walking the document to the court, courier service or overnight express delivery.

Attorneys increasingly recognize the cost of document preparation and use document production software based on word processing programs. For example, one company offers a complete set of bankruptcy forms in electronic form to speed document creation. These forms step the attorney through the process to ensure accuracy. Since the forms are also templates, just as with paper forms, the attorney does not have to create the entire document, thus saving time and money. This provides a competitive advantage to more efficient attorneys.

Paper-based court information systems can be divided into two categories, information tracking and file maintenance. Courts record documents, the history of the case, in registries, dockets, calendars, name indexes, and financial records. This category of court record was designed to improve information retrieval, create summaries of actions and, most important, provide process control. This was needed because the court case file, as it moved from office to office, served as the workflow control for the case decision process. If the file couldn't be found, the registry or docket could provide information about the status of the case and who might have the file.

Receipt and initiation of a new case is a particularly work-intensive task in court clerk's offices. This is because both the processing tracking system and the file maintenance system must be set up for the case. In some courts, specialized files have

been pre-printed with a form on the file jacket to assist in organizing the information. The files also may have color-coded numbers on the tab. Both of these methods are an attempt to make the file folder a useful work tool in order to summarize information and prevent misfiling.

Maintenance

The second general record area is the court file, which contains detailed information regarding the case, including signed documents and orders. The maintenance of the file is of paramount importance since this record contains the information needed by the judge to make decisions. Paper files are expensive and difficult to handle, organize, move, and find. Case files often contain hundreds, if not thousands, of pages of documents. These documents are usually punched with holes and fastened to the case file so that they do not fall out. Once more than a few pages are attached to the folder, it becomes unwieldy to navigate through the documents.

A National Center for State Courts report pointed out other problems with paper records management.[148] These include:

- Court personnel use longhand or dictation to a stenographer to originate text for typing, at a cost that can be four to six times that of machine dictation.
- Courts use manual and electric typewriters to type repetitively the same information.
- Courts fail to control the use of copier equipment, resulting in unnecessary copies and a progressive degradation of copy quality.
- Courts record the same information in multiple court records.
- Courts lack basic information regarding their record systems, such as volume of records, access to records, efficiency of equipment, and supplies used.
- Courts use outdated and inefficient filing equipment and fail to match supplies properly with the installed equipment.

[148] Skupsky, Martin, Grumer, and Wolfe, *Comparative Record Management Systems and the Courts: Manual and Automated Alternatives*, NCSC publication number R0044 (Williamsburg, National Center for State Courts, 1980).

- Courts store and protect closed records improperly, utilize storage space poorly, and often store records with potentially destructive water pipes and water sprinklers overhead and fire hazards nearby.
- Courts resist change to new technology that will improve the productivity and effectiveness of the courts with no net increase in cost over a period of years.
- Courts retain voluminous records much longer than the interest of justice requires.

Although progress has been made, these comments are often as true in 1998 as they were in 1980.

Retrieval, use and distribution

Not only does the court have to distribute information within the courthouse; it must communicate with the attorneys, law enforcement, jails, corrections, probation and other participants in the legal system. The Maricopa County, Arizona clerk's office had a postage budget of approximately $400,000 in FY 1997-98. While a significant portion of these expenses was for child support checks, the court was sending a lot of other mail as well.

As noted in *Records Management,*[149] working with case files within the courthouse has particular challenges. Courtroom uses, inquiry response and daily updating of case files are common reasons for accessing records. If record retrieval time is high due to untrained personnel, improperly located file stations, a deficient numbering system, or misfiling, needless personnel time is wasted and records management costs increase. Standard procedures for filing and transporting case files to and from courtrooms can help avoid these problems. Lost files create delays in case processing and impair the administration of justice.

[149] Ernest H. Short and Charles Doolittle, *Records Management*, p.13 (Washington, US Department of Justice Law Enforcement Assistance Administration, 1979).

In *The Promise of Electronic Filing*, presented at the 1996 ABA TechShow in Chicago, Illinois, Judge Arthur M. Monty Ahalt[150] reported that in the Prince George's County Circuit Court:

> "Each file is moved to a Judge at least five times before it is closed. Thus, the 40,000 cases filed each year must move at least 200,000 times. A study conducted during the Court's building program revealed that those 200,000 moves costs $880,000 each year in personnel and other operational costs. Of course, when the case load grows to 65,000 cases in the year 2000, there will be 325,000 moves which will cost in the excess of $1 million." (p.3)

Thus the bill for paper filing continues to mount.

Disposition

The "tomb" of records is the archive. States, counties and localities all have significant physical plant and financial resources tied up in storing and archiving case files. A study of the Iowa courts by the National Center for State Courts found that 79% of older inactive case files are stored within the courthouse.[151]

Courthouses, whether new or historic, are very expensive warehouses. In 1998, a new courthouse cost an average of $200 per square foot to build, based on construction costs for both urban and rural areas. Since courts housing the larger collections of records are located predominantly in urban areas with substantially higher construction costs, there is little doubt that this is very expensive real estate to be consumed by files. Because the majority of these files are accessed infrequently (if at all), this expense becomes even more significant. In *A Guide to Court Records Management*,[152] the author cites a typical record inventory for a court. In that inventory he found that 1,988 square

---

[150] AMAHALT@virtualcourthouse.com.
[151] Thomas G. Dibble, Michele Panker-Beresh, James R. James, *Iowa Court Records Management Project Final Report* (Williamsburg, National Center for State Courts, 1990).
[152] Thomas G. Dibble, *A Guide to Court Records Management*, p. 31 (Williamsburg, National Center for State Courts, 1986).

feet of floor space was consumed by inactive case records, compared to only 301 square feet for active records. If the court had to pay even a low commercial real-estate price of $14 per square foot annually, it would cost taxpayers more than $32,000 per year just for the space to store records for this court.

Microfilm and microfiche have been the answer to many archival problems of the courts. However, as Mr. Dibble states in *A Guide to Court Records Management*:

> "Micrographics should be approached with the same care and consideration as the development and installation of a computer system. These technologies are cost-effective in the appropriate applications but can consume large amounts of money and resources with little benefit when inappropriately applied.[153]"

It should be noted that microfilm does not release the court from the need for a good records retention policy. Mr. Dibble goes on to state that,

> "It should not be assumed that every document in the case file must be filmed; a purging list can often reduce the sheer bulk of case files by 50 percent to 75 percent."

Just as with physical records, microfilm and electronic files must be evaluated for their value as historical or long-term records. It was noted in the Iowa study that "judgments and decrees" are the most often sought historical documents.[154] If this is so, then abstracters are the primary clients for this information and the court should plan for appropriate access.

[153] Thomas G. Dibble, *A Guide to Court Records Management*, p. 50 (Williamsburg, National Center for State Courts, 1986).
[154] Thomas G. Dibble, Michele Panker-Beresh, James R. James, *Iowa Court Records Management Project Final Report*, p. 11 (Williamsburg, National Center for State Courts, 1990).

Document System Evaluation

The *Comparative Record Management Systems and the Courts: Manual and Automated Alternatives*[155] contains an excellent checklist for evaluating a court document management system. This checklist is as valuable for courts planning for electronic filing as for those who wish to improve their manual systems.

> **Gathering Information**
>
> Once the general objectives have been defined, the systems analyst must gather all relevant information. This is accomplished through interviewing court personnel, funding agencies, and archivists; inspecting records and facilities; and monitoring workflow and operations. Statutes and court rules must be examined to determine legal requirements relating to records. Some of the questions that should be considered include the following:
>
> - What records are created?
> - What records are received?
> - What is the legal basis for each type of record?
> - What is the legal, administrative, fiscal, and historical value of the individual records?
> - How often are the records updated?
> - How frequently are the records needed?
> - How are the records used? For what purpose?
> - What is the sequence and indexing scheme of the files?
> - Are facilities, equipment, and space available for records storage?
> - What is the total volume of records in filing inches?
> - What is the total anticipated annual volume of records in coming years?

The Trial Court Performance Standards[156] add some reasons for good records management policies and procedures:

> **Standard 3.6 Production and Preservation of Records**
>
> Records of all relevant court decisions and actions are accurate and properly preserved.

---

[155] Skupsky, Martin, Grumer, and Wolfe, *Comparative Record Management Systems and the Courts: Manual and Automated Alternatives*, NCSC publication number R0044, p. 10 (Williamsburg, National Center for State Courts, 1980).

[156] Bureau of Justice Assistance. *Trial Court Performance Standards with Commentary* (Washington: U.S. Department of Justice, 1997).

Commentary

FAIRNESS, EQUALITY, AND INTEGRITY depend in substantial measure upon the accuracy, availability, and accessibility of records. Standard 3.6 requires that trial courts preserve an accurate record of their, proceedings, decisions, orders, and judgments. Relevant court records include indexes, dockets, and various registers of court actions maintained for the purposes of inquiry into the existence, nature, and history of actions at law. Also included are the documents associated with particular cases that make up official case files as well as the verbatim records of proceedings.

Preservation of the case record entails the full range of responsible records management practices. Because records may affect the rights and duties of individuals for generations, their protection and preservation over time are vital. Record systems must ensure that the location of case records is always known, whether the case is active and in frequent circulation, inactive, or in archive status. Inaccuracy, obscurity, loss of court records, or untimely availability of such records seriously compromises the court's integrity and subverts the judicial process.

Information processing in a mixed environment

Fortunately, it is not necessary to make the transition from a paper-based system to a completely electronic one in a single leap. For more than two decades, courts gradually have increased their reliance on an intermediate technology, the case management system. Electronic filing and document management systems will not replace today's data systems, but will change their role to one of an index to electronic documents, much like the old docket books and index cards served the paper files.

An automated case management system can assist in this purging of documents by marking the events recorded in the case with an archive or purge default flag in the associated document or case management database. The purge flag would assist greatly in the maintenance; archiving and purging of the case file and the purge could be overridden, if desired by the court.

One point to consider is the constant rate of technological change. In 1998, the change from CD-ROM technology to DVD or some derivative that has greater storage

capacity is beginning. Optical media that can store information at 100 megabytes per square inch of surface are reportedly being developed. It is safe to say that storage media capacity will continue to expand in the future.

It also is necessary to recognize that the operating system programs that organize the bits and bytes on the storage media will change and expand in the future along with the data formats and application software. All of these changes mean one thing: it may not be practical to commit long-term and “permanent" archives to digital media.

But what is the alternative? One possibility is computer output micrographics, known as *COM* in the records management world. Recognizing that court cases are rarely retrieved from archives, the lowest cost, lowest technology solution seems to be the best alternative at this time. COM is produced in a manner similar to a laser printer. Instead of printing to paper, the system displays the print image on a high-resolution device and captures it on the microfilm or microfiche. While COM output is not as space efficient as CD-ROM or similar digital media, with proper storage the information will be available a century from now.

Simply put, a COM image can be viewed through magnification. Electronic or laser images require the correct hardware and software to be available. Think of the computers of only 20years ago, such as the Apple II and dedicated word processors, and you will understand this point.

What about converting the data as the systems and software change? It would require extreme vigilance, rigidly enforced procedures, and a commitment of financial and systems resources to ensure consistent conversion of the ever-growing library of information. Over time courts make significant changes to the types of information captured in their databases and to the organization of the databases. Such changes add

complexity to the process of converting existing records to a new retrieval system. Each time conversion occurs, all records, including those dating back to the earliest digital archive, would have to be converted. Over the years a given record may be read, converted, and rewritten many times, even if no one ever needed to see it. The COM approach, on the other hand, would not require old archives to be converted.

Perhaps in the future, digital capacity will grow beyond what currently is possible so that all the information is stored in on-going, upgraded systems. Under such an approach, nothing would be "thrown away" or archived from the active information system or network, even though data organization would be managed to optimize retrieval time for more active files. Until that time comes, solid alternatives must be selected to address archiving needs.

Case management systems

The recording and scheduling functions of the court often are referred to as case management. Paper-based case management systems often consist of a docket book or register to record the documents and events that have been held in a particular case. This register is usually supplemented with index cards that record information related to the parties. The court would create an index card for "Jane Doe" that lists the cases that she is involved in and, often, financial records and obligations owed. The other major piece of case management systems is the case file where documents are stored. In some courts the case files are pre-printed with a form to list contents and indicate case status and workflow. Automated case management and its relation to electronic filing are discussed below. At this point, it is sufficient to say that the computer is a much more flexible tool than the paper and pen systems that courts are abandoning.

First-generation case management systems

Courts that implemented a case management system in the 1970s or ’80s may have difficulty tying these legacy systems to an electronic filing system. There are several reasons for these problems.

First, COBOL and other older computer languages and systems required that the entire court's workflow be defined step-by-step. This was done so that the data and workflow could be programmed into the computer system. The major problem with COBOL and other languages was that it took considerable time to create this programming. Ann even bigger problem arose when the process changed. These older computer languages often require that the entire program be changed to reflect the new process, which is both time-consuming and expensive.

As a result, two strategies emerged in writing these older court case management systems. First, the software was written in a general way to capture key information and to generate required reports. This approach meant that the court's staff would work around the limitations of the computer system with paper files and notes. The second strategy was to have a computer programming staff available to modify and enhance the system as needed. Both approaches necessitated significant additional personnel resources and related costs.

Second, older case management systems often suffered from the lack of a relational database system in which to store data. Data was stored in “flat files” that can be thought of as long sentences without punctuation. Information is readable, but not easily readable. Therefore, translators, which we call programs, would add, insert and retrieve data from these "sentences.” The most significant problem is that it is difficult to connect different pieces of data with this kind of program storage system. Why is this important?

Courts relate many pieces of information together to reflect the complexity of a case. Further, courts relate different persons to all the cases in which they are involved. Practicing attorneys are excellent examples, because they are related to several different cases in different ways. In addition, the hierarchical nature of these archaic data structures required a significant amount of redundant data entry.

If a court uses an older case management system in which data is stored in "flat" or indexed-sequential files, then it will not be easy to use the case management system as a document indexing system. It is a difficult task to link advanced technologies to these obsolete systems. Courts should consider replacing them before pursuing any type of document management solution.

New case management systems

New case management systems use a table-driven approach to perform functions such as workflow. Tables also are used to validate data entered in the case management system. Tables can be thought of as containers of similar information. For example, case type designations, such as civil, criminal, domestic relations, family, probate, and chancery, can be coded and stored in the case type table. There can be hundreds of tables in a modern case management system. The good news regarding this trend is that court managers easily can modify the tables to reflect changes in the workflow of the court. The challenge is that someone must understand the interrelationships between data, tables and workflow.

The most important aspect of these new designs is that the tables define events. Events can include filing or issuing documents, scheduling hearings or trials, and recording financial information or transactions. When events reflect documents, the case

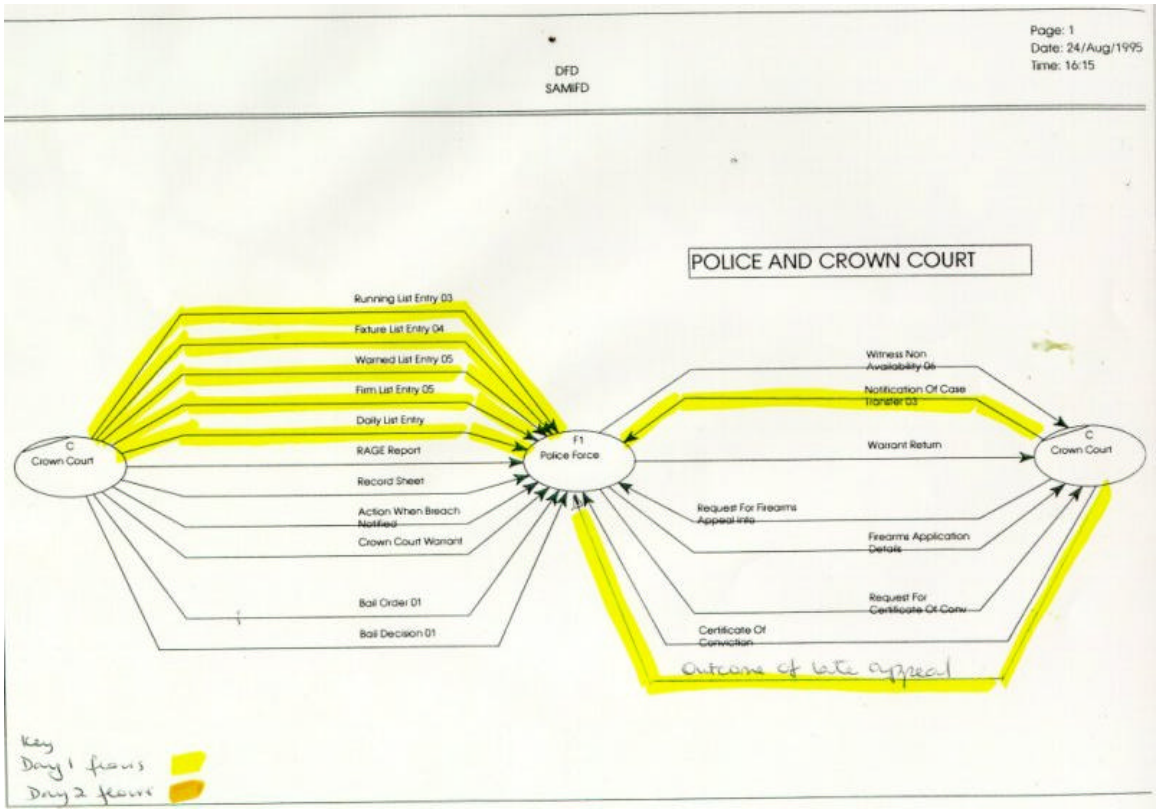
management system contains the description of the documents. More importantly, the tables can define what to do with those documents.

Tables also can define workflow by identifying the next event to be scheduled and documents to be produced. For example, when a document is received, the court records this event in the case management system. The type of document determines subsequent actions the court will take. Perhaps a filing fee is assessed, a hearing is scheduled, and notices are produced. Thus, the tables make workflow flexible and controllable within the court. Court managers will be able to manage both the court organization and automated systems. In the near future, we also will see sophisticated multi-branching workflow capabilities being designed into case management systems.

Note that in addition to automating workflow within the court, it is just as important to automate workflow between the court and the outside entities with which it transacts business. These include government agencies such as law enforcement, prosecutors, public defenders, corrections, probation, social services, and education systems, in addition to private attorneys and citizens. The court, being at the hub of scheduling and decision making has the opportunity to develop and coordinate workflow and information exchange standards though court rule for the entire justice system.

It is important for the court to understand the paper flow and workflow between organizations. A good example of a simple but effective representation of workflow was completed by England's Home Office in their CCCJS project. A copy of one flow set between the police and crown court is shown below.[157]

[157] See Appendix A for an article about the Hampshire pilot project.



Form and format of information

It is also important to note that courts traditionally have governed the form and format of information presented. A simple example is the traditional case "header" format shown below:

The Court of Somewhere
Division 1

In the matter of:

J. Q. Citizen	)	
	)	
Vs.	)	Case Number: 99-1234
	)	
I. M. Respondent	)	
	)	

_____

Courts have designated this format to convey information in an orderly manner. In keeping with this tradition, courts can and should continue this practice with electronic filing and communication systems.

One example of courts controlling the format of documents is a project in Ontario, Canada. This project uses word processing forms and document templates to present information to the courts. The court provides the forms and templates to attorneys at no cost. These forms and templates provide an organized foundation for documents to be submitted to the court, conforming to the court's rules. This court has gone one step further by providing the first step in an electronic format, in this case a word processing document. There are several advantages to courts providing this guidance:

1. The courts control the organization of the information.
2. The courts control the "look" of the document.
3. The courts can mark data fields within the documents that can assist in data entry.

The single biggest drawback to this approach is that by basing the system upon a couple of versions of word processing software, it will be difficult to change and upgrade the forms and templates in the future. This is due to incompatibilities of the upgraded word-processing software over time. Another drawback is the courts only endorse one or two private, commercial word-processing programs. Restraint of trade is a concern.

Whatever the format selected for electronic documents, courts or their service providers must be responsible for making those documents retrievable through the current access technology in use by their clients.

Electronic document processing

A fully electronic system will offer tremendous advantages to the court. This subsection describes how the paper and paper/case management system approaches of the past will yield to dramatically more efficient, effective processes.

When proper re-engineering is incorporated, the processing of electronic documents will be very different than the processing of paper documents. The most commonly used data fields in case management systems likely will be automatically fed by the electronic filing system once an electronic document has been validated and accepted. Typically, either the filing party will provide that information as part of the filing process (perhaps through a step-by-step data entry procedure using a "wizard" software utility) or the data within the document will be marked or "tagged" so that the computer can find it.

The clerk's office also will no longer move paper from the file room to chambers or the courtroom. Instead, they will manage the flow of information either through the electronic filing system, electronic mail or the case management software.

It also is likely that court staff will be involved with "linking" documents and information within documents to a case. Instead of linking information only by the case number, documents will be linked to persons, families, companies, and other identifiers. Some linking will be done automatically by computer, while court staff will accomplish other linking.

Why would a court want to establish such links? It is becoming increasingly important, in order for justice to be achieved, to understand the bigger picture involving a particular person. For example, one individual may have been involved in traffic, civil, domestic relations, and criminal court. Without understanding the person's history and

obligations, ineffective decisions could be made. This is the beginning of what is termed "decision support," which organizes information for the decision-maker, the judge.

Courts can realize significant gains in efficiency through electronic filing, with resulting savings in operational costs. In 1997, the Shawnee County, Kansas court[158] compared manual versus electronic workflow. A summary of their findings for processing documents received by the court is shown in the table below:

Time and Estimated Savings per 100 Documents Processed

Process	Manual processing time in hours	Electronic filing	Staff time savings in hours	Staff savings @ $30,000 salary plus 30% benefits
Case Filed and fees collected	1.00	5.5 minutes	0.93	$21.14
Petition checked for completeness	0.75	included above	0.75	$17.05
Data entry	3.25	3.3 minutes	3.20	$72.73
Summons issued	1.00	included above	1.00	$22.73
Summons signed	1.25	included above	1.25	$28.41
Docket fees rung by cashier	1.00	automatic	1.00	$22.73
Receipt mailed by attorney	0.25	automatic	0.25	$5.68
Documents filed	1.00	automatic	1.00	$22.73
Summons carried to sheriff	0.25	automatic	0.25	$5.68
Total	9.75 hours	8.8 minutes	9.63 hours	$218.86

Staff savings estimated by this report were based on the salary and benefits shown above. It is important to note that the estimated savings reported by the Shawnee County court is for 100 ***documents***, not cases.

[158] http://www.shawneecourt.org.

A number of years ago, a study of the Maricopa County, Arizona Superior Court file system was made by the NCSC. It revealed that an average of a little more than 19 documents were filed per case. According to the *Arizona Courts Data Report 1996*, Maricopa County received 95,619 cases. If 19 documents are received per case then more than 1.8 million documents were received that year. If the savings from Shawnee County were applied to this equation, the potential savings would be more than $3.9 million for this one court. Furthermore, this does not begin to consider the maintenance costs of the files in the courts or the re-engineering benefits of the electronic filing system.

How Paper Will Be Handled in an Electronic System

Despite the best efforts of courts to conduct business with law firms and individuals electronically, paper will continue to be used in judicial processes for the foreseeable future. Pro se (or pro per) litigants constitute a growing proportion of court users, particularly when the cost of representation exceeds the amount in controversy in a civil action or the potential fine in a criminal or traffic case. Many of these litigants who represent themselves cannot afford, or lack the ability, to use computer systems. These individuals have the same right to access court services as those represented by technologically sophisticated law firms, so courts must continue to accept handwritten, paper pleadings.

In the beginning, courts will maintain paper files along with electronic case files residing in document management systems. Over time, more and more cases will be filed electronically, and work on those originally filed on paper will be completed, producing an increasing inventory of electronic cases. At some point, it will be cost-effective for

the court to convert its paper case files to an electronic form and abandon the parallel systems.

As part of this process, courts can begin to convert paper to an electronic form upon receipt, using scanners, optical character recognition software, and handwriting recognition systems.

Even after courts are conducting their business electronically, paper will still be necessary. Those pro se litigants who cannot provide electronic documents to the court also cannot receive electronic service or view case information resources, so courts must continue to generate paper for these individuals.

Summary

Electronic filing promises speed, efficiency, productivity, and effectiveness. Unfortunately, a paperless system is beyond our grasp for the foreseeable future. Nonetheless, courts and law firms must prepare for a gradual transition that could take many years.

Chapter 6: Technology Infrastructure

Experience has shown that success with electronic filing requires the proper infrastructure. This includes the computing environment, networks, Internet connections, case management systems, and document management systems. This section outlines various system configuration options and describes what is needed by a court to make the transition from paper to electronic filing. Specific implementation details will be covered in Chapter 8. Emphasis here is on open systems that are compatible with other pieces of the e-filing puzzle.

Much has been written about "open systems." Unfortunately an open system rarely exists. Instead, many databases and applications support multiple operating systems. Courts must evaluate computer hardware, operating systems, database, and applications software to determine the best combination of components to meet their needs while understanding market forces. One strategy is to buy products that dominate their category or at least have a very significant market share. Then, if that company runs into financial difficulty, the product likely will be acquired by another company. While not an operating system, WordPerfect is a good example of this transition from a private company through a second company, Novell, and finally to its new home with Corel. WordPerfect had too many users to terminate its existence.

Before we discuss computer hardware, software and communications environments required to support e-filing, we must briefly consider a basic question: What is a document? To a court it is anything that is submitted. This can range from a simple piece of paper to large models or physical objects. What is normally kept in the court file is paper or pictures of an object. The evidence room generally contains the physical evidence in the case.

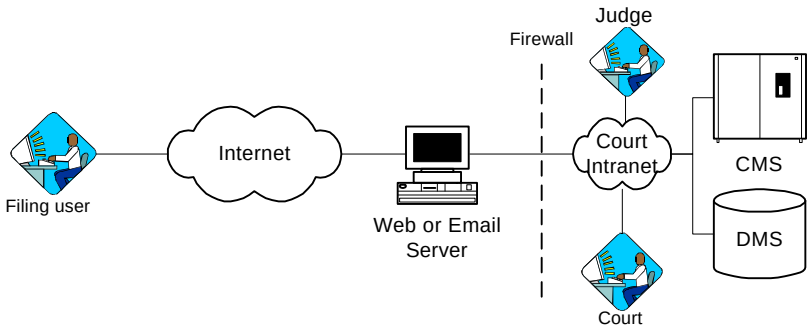
Therefore, this chapter concentrates on the requirements needed to replace the traditional court file—not the evidence room.

Electronic Filing Architecture

The following section describes the primary architecture options to implement electronic filing. These architectures serve as a reference to the hardware and software requirements included in the following sections. Each court should evaluate its needs based on factors such as feature set, number of filings, costs, and support structure. This will help determine which architecture model best fits that court's specific requirements. These options generally outline the systems, connectivity and integration required and are not provided as an exhaustive list. Variations or phased implementation using a combination of these options also should be considered.

Court Management System (CMS) vendor or Court provided e-filing

This system model suggests tight integration with the specific CMS currently used within the court. This may require the CMS vendor to enhance the software if electronic filing is not already supported. These enhancements should include software and hardware system upgrades to address the new security, functionality and connectivity features that e-filing introduces.

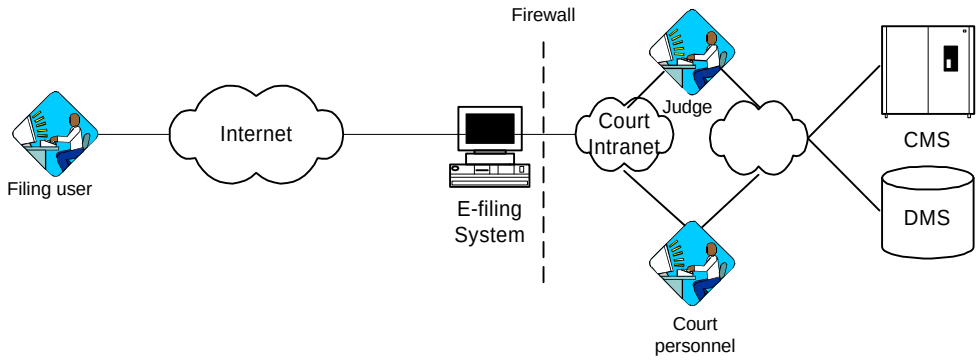


CMS or Court provides e-filing Figure 1

This model also suggests that the court or CMS vendor address the needs of the filers, mainly attorneys who are new users. Support services should include sales, marketing and customer service support for the e-filing process and communications. User requirements and enhancements, such as forms integration, and consistency across courts should be evaluated and efforts prioritized. Providing the latest technologies, security features and integration with attorneys' existing work flow will be critical if the court hopes to receive broad acceptance of the new filing paradigm, which offers productivity benefits and cost savings.

Standalone e-filing system

This option–a "one step at a time" approach—already is in use by some commercial electronic filing service providers. In most cases the courts are not prepared to integrate electronic filing into their CMS systems that are planned for the future. This model includes a stand-alone e-filing service separate from the court's internal systems. Since it is not integrated into the court's CMS, most of the court's productivity and cost savings are lost. However, this architecture can be implemented quickly because it doesn't have to be integrated into other existing systems. This model also maintains the court's traditional separation of CMS and case file maintenance operations. However, additional software and hardware may be required and must be introduced into the existing workflow processes.

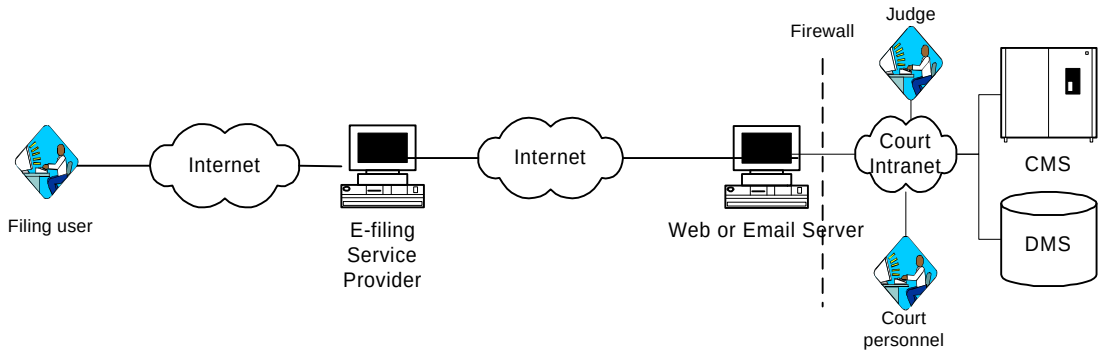


Standalone E-filing service Figure 2

As with the previous scenario, this model suggests that the e-filing service vendor provide the necessary sales, marketing and customer service support needed for e-filing process and communications. Meeting the court's needs and the electronic filers' needs is critical to the success of this approach.

Open e-filing service integrated into court's systems and workflow

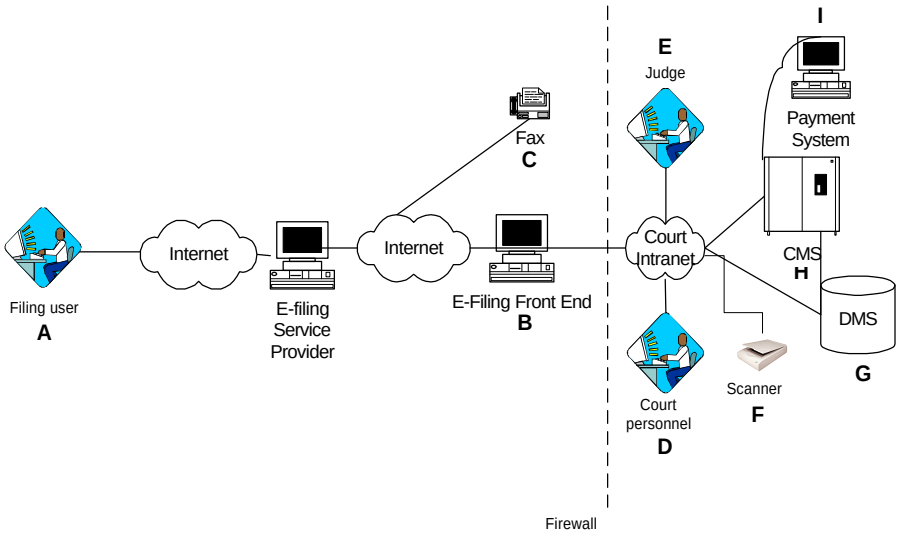
This architecture combines the benefits and functionality of the previous two models. An e-filing service vendor provides the integration into the court's case management system using open, published e-filing protocols. In supporting these open interfaces, the CMS vendors reduce development costs and improve the available alternatives for future expansion. The e-filing service provider also provides the filer (attorney) with sales, marketing, customer support and enhanced functionality. This architecture also can reduce filing and retrieval traffic in the court system and provide around-the-clock availability into the e-filing service. An example to illustrate this architecture is the ATM (Automated Teller Machine) model. ATMs provide a consistent interface whereby customers can deposit or withdraw money whether the bank is open or not. This has been very successful for the banking industry, which has successfully eliminated availability and security concerns of customers. This architecture meets the varying needs of both the filers and courts.



Open E-filing Service integrated into Court CMS Figure 3

When considering which architecture best fits the needs of a specific court, the following key factors should be analyzed. Early consideration of hardware, software, connectivity, communications, security, integration into existing systems or processes, user and systems support, performance, reliability, and scalability will ensure that the e-filing system will be efficient, manageable and user friendly.

The remainder of this section will review infrastructure requirements and available options that take into consideration the key factors listed above.



E-Filing Infrastructure Components Figure 4

E-filing Architecture Components

The diagram above (Figure 4) shows the components required for e-filing considering the previously described models. The following sections discuss each of the components identified in Figure 4.

Figure 4 A. Filing User

Clients that use the e-filing system include judges, court personnel and attorneys who file documents. The advent of the personal computer in the late 1970s changed the way information systems worked. The computer interacted with other computers rather than working in isolation. Now computers are classified as clients, often a personal computer, or servers. Servers are computers that store and share information, and they can be large or small depending upon the task required. For example, a stock exchange may have many large server computers linked together to handle volume and communications for millions

of transactions per minute. Conversely, a small rural municipal court may have a PC set aside as a server.

With the advent of the Internet browser, the “universal” terminal was created. The browser interface allows a centralized computer to control the look and content of what is sent to the client. The flexible nature of the HTML combined with graphics allows the user to view more content in an interactive rich format.

In addition to software that allows clients to retrieve and submit filings, the user may need to proprietary software to access the CMS. This software would allow court personnel to change a name or address, or flag a document after it is officially docketed. This software may or may not be needed depending upon the architecture of the e-filing status.

How clients interact with the server is a determining factor for system requirements and performance, because different clients need varying levels of support. Typically, a personal computer needs more support than a "dumb" terminal. However, the additional cost of support for a personal computer can often be justified because of the flexibility of the software, the server and the peripheral equipment that can be attached.

Figure 4 B. E-Filing Front End

All courts should establish an electronic front end that is outside of the court or government's firewall. All electronic files should be submitted to that computer. This rule should also pertain to government agency Intranet document filings. Why should a court do this? Because the court needs to establish a single point of presence wherein Internet security and virus checking can reside.

The court should assume this computer can be destroyed just as your home mailbox can be vandalized at night, and develop a base set of software to facilitate both e-filing and fax filing. Once the basic software is created, a backup image is made on a tape or CD. If the machine is "hacked," gets a computer virus or is somehow destroyed, the court can easily rebuild the machine with the backup. The machine would not store any permanent data, but function solely as a communications receiver and virus checker. This separates the court from the Internet and provides a degree of separation needed as part of a good security plan. Courts working with an e-filing service provider must address some basic issues. How often to back up data? What happens to lost filings when a restore is done? When does the filing document become the court's responsibility? How will the filer be notified of successful filing or loss of filing?

Allowing e-filing via e-mail includes simply attaching the filing document to an e-mail message. This attached document would be in a file format supported by the court. Once the e-mail is received, the document would be manually reviewed and stored in the document management system. The e-mail solution for e-filing is limiting, however, because it does not allow for many of the features that would make it a full-service filing. If electronic filing was primarily e-mail based, information would have to be transferred from the e-mail server to a database, and a user interface would be required for users to view the documents that have been filed at the court. The e-mail solution would not allow retrieval of cases. It could not be integrated with the billing and payment system, and usability would be sacrificed.

The Internet has become the common model for new software. Using a web browser provides an easy and consistent way to access services. Current estimates are that more than 90% of all lawyers have Internet access and use it everyday for e-mail and web browsing.

Since most courts can add Internet access relatively easily and inexpensively, this technology is a natural fit for electronic filing. A web server is required for connectivity to the Internet through a browser interface.

Current approaches to e-filing via web browser include providing on-line dynamic forms so the user can complete necessary filing information and attach the filing document. This attached document must be in a file format that is supported by the court. Web-based communication with the court or e-filing service provider enables the court's CMS to be automatically updated and the electronic documents to be stored in the DMS.

The hardware and software options for a web server or e-mail server will vary depending on the court's filing capacity, availability and scalability needs. The operating system will be chosen with these criteria in mind.

To learn about factors a court should consider when installing an Internet connection, please refer to the NCSC Publication, *Information Superhighway Implementation Guidelines,* which can be found on the Internet.[159]

Because of the growth of the Internet and myriad legal services being developed, it is recommended that courts connect to the Internet for e-filing. This connection can be made directly by the court or through a general government connection, college, university or commercial Internet service provider. The speed and type of connection will depend on the volume of documents that the court will be receiving and providing to the public.

Security

As mentioned earlier, security is an integral part of electronic filing. Security options include digital signature and public and private encryption. A digital signature proves who the sender of the document is. This would allow the court to identify specifically who sent

the document. Encryption scrambles the document so it cannot be read or altered en route to the court. When the document is encrypted (coded), two "keys" are assigned to allow it to be unlocked and read. The "private key," used by the sender, is different than the "public key" used by the court where the document is submitted. The public key is made available on the Internet or via e-mail by the court to the filing attorney. Using the court's public key to encrypt the document, the attorney is assured that only the court is able to decrypt and read the document. Depending on court rules this security component may vary from court to court.

Integration

If electronic filing is integrated with the Document Management System, the e-filing system can guarantee that the filing is complete prior to the actual *filing*. Programmatically, the electronic filing system can validate that the required data fields are complete and that the document is in the correct word processing format. In addition, if electronic filing is integrated with the DMS, court personnel will not have to physically file the document and risk misplacing or misfiling the document.

Performance

In order to integrate fully with electronic filing, the court must have a robust and scalable web server that can satisfy all of the requests it receives. In addition, the court must have enough network bandwidth connecting to the court's systems to support all of the users accessing the system.[160]

[159] http://www.ncsc.dni.us/NCSC/ISIG/Guide.htm
[160] More information on bandwidth can be found at http://www.ncsc.dni.us/ncsc/isig/guide.htm.

Reliability

It is imperative that the electronic filing system is always available to the users. Having the server go down would be the same as locking the front doors on the courthouse. One server failure could ruin the credibility of electronic filing. If users experience unreliability, they will not use the service and the courts will not benefit from the cost and productivity savings.

Scalability

Scalability issues vary from court to court. One court may receive 3,000 filings a day, while another might handle only 50 on a busy day. The electronic filing system needs to be scalable to handle the court's varying needs, without performance being affected. Selecting software and hardware that can grow with the court's needs is critical.

Figure 4 C. Fax

A fax modem dial-up phone line connection should be included in all court e-filing systems. As discussed in the imaging section of the report, fax is an efficient way for a court to receive images. The fax modem is directly attached to the e-filing front end. Since this connection should be set to only receive facsimiles, there is less chance for a "hacker" to invade this part of the system. If the court is working with an e-filing service provider, they most likely will support the fax functionality instead of having the court provide it.

Figure 4 D. Court Personnel

One of the benefits of e-filing is that it reduces the workload for court personnel. They will no longer need to enter the information manually into the CMS, freeing more of their time for other critical tasks. However the court personnel may need to update or

change information in the CMS, depending upon the level of integration with the e-filing system.

Figure 4 E. Judges

Judges will benefit greatly from the e-filing service, because they can retrieve all of the filings pertaining to a case almost instantly from their desktop. Furthermore, judges will be able to "print-on-demand" any or all of the case file and not worry about misplacing items since the "original" is safely stored and backed-up by the computer system.

Figure 4 F. Scanner

A scanner is necessary to import paper documents into the system. This also will allow non-electronically filed documents to be viewed by the e-filing service users. The scanner is explained in more detail in the Paper-to-Data Conversion portion of this chapter.

Figure 4 G. Document Management System

In addition to the current CMS system, workflow software and database and file sharing systems, electronic filing requires a Document Management System (DMS) to store and manage the electronic documents. The DMS replaces the filing cabinets that store the paper filings. Some courts already may have a DMS integrated into their CMS, or their CMS may support a preferred list of DMS vendors.

Often the first question from information systems professionals is, "How big should the DMS be in order to handle e-filing?" The answer depends on the volume and type of cases, as well as the number and kinds of electronic documents that must be accommodated. The best approach is to use conservative projections as is done below. The advantage of this

approach is that within one year to 18 months, improvements in computer storage technology will greatly increase storage capacities.

Server Processor & Memory

Nearly any computer CPU installed in a new commercial grade computer server should have the speed and capacity needed to handle the file requests for an e-filing system. E-filing systems likely will not be "processor bound." Rather they will be I/O bound. This is because the file server is simply storing and retrieving files, which is a quick and simple process. However, it may be necessary to provide ample RAM in order to cache requested documents and images for quick display. This is because modern database and file access programs attempt to guess which documents you will want to read. Thus, when a document is requested, the server's software will also read and "cache" or store into fast chip RAM memory other documents.

Server Storage

The good news is that technology has reduced significantly the cost of computer disk storage. This cost is now low enough that courts no longer need only to consider "optical" media as the sole solution for storing large amounts of documents. In mid-1998, an eight-gigabyte hard disk cost less than $400, and prices are continuing to drop radically. This drive can store approximately 200,000 pages of image files or more than 3.2 million word processing text pages. All this is stored in a 1 inch by 5 inch by 6 inch area. A paper file would require more than 40 linear feet of space for the same 200,000 pages. If possible, a court should first estimate the number of pages received per year using the following scale:

File drawer - vertical - 4,000 pages per drawer.
File drawer - horizontal - 5,000 pages per drawer.
Stacked paper - 200 pages per inch.

Secondly, a court should determine the types of documents it receives. Determine the percentage generated by the legal profession and court reporters, which could be directly e-filed. Then determine what percentage originates from pro se filings or from attorneys not equipped for electronic filing. Next assess the volume of original documents that are evidentiary because of signature, handwritten notes, or other special circumstances. Finally, it may not be necessary to enter certain documents, such as transcripts and depositions, into the system until they actually are needed. This process, called just-in-time submission, could reduce the size of the electronic case file.

A court should then take the number of documents by type and estimate the amount of electronic storage needed using the following table to estimated file sizes. Some assumptions concerning the type of electronic documents the court will wish to receive must be made. However, this table can be used in a spreadsheet portion of a "what-if" analysis for any plan.

Document Format	**Approximate file size per page**
Word Processing document without graphics	3,000 bytes per page (3 K)
Word Processing document with graphics	20,000 bytes per page (20 K)
Internet type file (HTML/XML) without graphics	2,500 bytes per page (2.5 K)
PDF (Acrobat) file without graphics	5,000 bytes per page (5 K)
Image file	40,000 bytes per page (40 K)
Facsimile image file	40,000 bytes per page (40 K)

As you can see in the table above, the most efficient file types are Internet HTML/XML and standard word-processing formats. However, if numerous graphics are included, then these files can be as large as the imaging or fax files.

The various hardware and software options for a DMS will vary depending on the court's filing capacity, availability and scalability needs. An operating system should be chosen with these criteria in mind.

Security within the DMS is critical because it insures that documents are not accessible by the wrong parties. Access control can be implemented in many ways within varying levels. This can be based on court requirements, rules and type of cases, and in most situations it will be implemented by the CMS.

Performance, reliability and scalability also should be based on the courts and the filers' user requirements, the number of filing transactions per day and integration with existing systems. Performance and scalability can be addressed in many ways, including hardware configuration, operating system and additional software. Reliability can be addressed in the following ways.

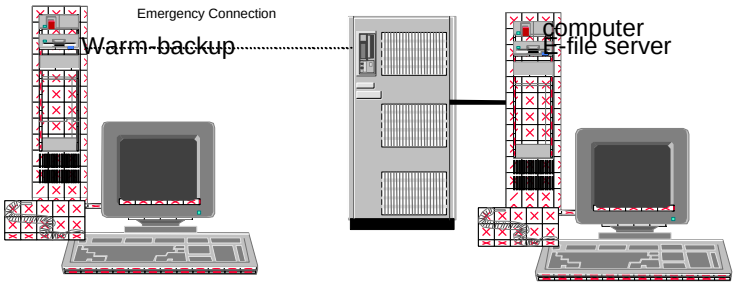
Server Fault-tolerance

Banks, hospitals, 911 centers and others have a critical need to keep their computer systems running without failure. Other types of organizations want to reduce the chance that server hardware failure will interrupt services. Therefore both fully and partially fault-tolerant computer systems have been developed. Fully fault-tolerant systems are similar to those used on the space shuttle. Shuttle launches have been delayed because the multiple computers don't agree with each other. In that system, fault tolerance is imperative. However, courts likely will not have the need to spend the extra money to buy a fully fault-tolerant system. Instead, courts should take advantage of several lower cost fault-tolerant strategies. Three items to consider are RAID (redundant array of inexpensive disks), dual network interface cards and a "warm" backup computer.

RAID level 5 combines multiple disk drives (at least three) to provide automatic backup of data. If one disk drive fails, the disk drive can be replaced and the data is automatically rebuilt from the other disk drives. It is recommended that all electronic filing servers have RAID level 5 or equivalent capabilities.

Most networks installed today are based on the TCP/IP networking standard. If a court's network uses TCP/IP, it is recommended that the server be installed with two network cards and be assigned two IP addresses. While network interface cards rarely fail, this provides inexpensive fault tolerance for this component.

A "warm" backup computer is essentially a clone of the e-file server. In the example shown below, the court bought a separate disk subsystem. When the e-file server fails, the warm-backup computer can be connected to the disk subsystem and service is quickly restored.



Backup System Figure 5

Backup

In order to have reliability a system backup of the e-filing server is imperative. Rotating tapes, archive tape sets, on- and off-site storage are all parts of an effective backup system. In addition, it is imperative that the data on the tapes be validated. Many courts have gone to their backup tapes only to find that there was no data recorded on them. Courts may wish to develop a relationship with another data processing operation so that they can check each other's backup tapes on a regular basis.

Figure 4 H. Court Management System (CMS)

This CMS manages many of the day-to-day activities in the court such as filings, documents, records, calendar, etc. Many courts already have this component in place,

and an open protocol will allow the CMS vendors to hook into the e-filing service providers.

Figure 4 I. Billing/Payment Services

When e-filing is implemented, some electronic process must be established to replace the manual process of the court clerk taking the court filing payment. If the electronic filing system can be integrated into the court's billing system, court personnel would not bill the users of the system. Incorporating the billing component guarantees that the payment is complete before the documents are filed because the charges will be handled by a credit or debit card, escrow account, digital cash or electronic funds transfer. When establishing an on-line billing system, the following items must be considered: hardware, software, connectivity, security, integration, support, performance, reliability and scalability.

Other Issues to Consider

Data Distribution

Making sure that the data is in the right place at the right time is another consideration. Copies of filings should be duplicated automatically for the filing party, the court and the served parties. Sometime individuals receiving the information need all the information, while others simply and sometimes need a notification. Therefore, three technologies: replication, e-mail and push can all be used to fulfill the needs in an e-filing system.

Replication: This technology is used to automatically distribute documents as in Lotus/IBM Notes databases or data in relational databases such as Oracle or Informix. Basically, replication makes copies of information from one computer to another based on a set of rules. Replication software also makes sure that the data or documents are

synchronized between the different computers. Since replication is built into these and many other products, courts should evaluate how this technology can be used to their best advantage. For example, a state administrative office may control the court forms. Using replication technology the state could replicate all the forms to each of the court's individual e-filing servers throughout these state with a single command. Thus all local courts would receive the update simultaneously. And, if there were problems, the state office would be automatically notified. Replication also would allow a court to synchronize its information with another court.

E-mail: E-mail is one of the most widely used applications on the Internet. It can be useful for notification, as well as the submission of filings and service. Although there is no universal limitation to the size of an e-mail message, the e-mail provider may impose a limit, often between two and nine megabytes. E-mail software packages have different ways of handling file attachments such as word processing documents and this can cause difficulties. Unfortunately it is unlikely that standards will appear and the problems will dissipate.

Push: PC Webobaedia[161] defines push when in a client/server application data is sent to a client without the client requesting it. This idea has been used by at least two commercial e-filing systems to notify parties that pleadings had been filed in a case. However, the push technology was not limited to an Internet browser or e-mail, it also included fax and even mail notification. This might be a service that is provided by the e-filing service provider. Since fax and e-mail can be automatically generated, adding these "push" features caused no great burden on the system. Therefore, it is recommended that all e-filing systems have an

[161] http://www.pcwebopedia.com/push.htm

ability to "push" information out in multiple formats as a standard part of their data distribution systems for notification and distribution.

Scalability

An important overall issue is scalability. The court must plan for increasing use of its electronic filing system in hardware and software, and even more so when it comes to communications. A scalable system is one that can grow to larger storage and faster processing speeds. The court also must plan to increase the size of its communications infrastructure, and the budget for communications lines into the court. The choice of operating systems, network protocols and communications providers also is important. If the court uses a private company to provide these services, it is important to scrutinize the vendor's current capabilities and future plans. The bottom line is to avoid bottlenecks that could diminish the speed and usefulness of the system and in turn it's acceptance to the public and legal community.

Paper-to-Data Conversion

At least for the short-term (the next decade or two) courts will be forced to contend with paper. Since the 1970s computers have had the capability of scanning and reading paper text. Unfortunately, the computers have never been 100% accurate. In many environments this is not a problem. In the legal environment, where one word may be critical to an argument, this is unacceptable.

Courts can find uses for OCR/ICR technology as part of their e-filing solution if the limitations are recognized and error correction is planned. For example, documents can be OCRed and the "rough" copy used by text search software to find information. Programs have been developed that allow for errors in the rough copy. Thus the search can easily

locate the requested text. But instead of viewing the rough copy, the judge or attorney will see the document's image, which will be error free.

A second method using OCR/ICR technology takes advantage of more powerful computers to scan and convert handwriting. We have all filled in paper forms with blue boxes to "delimit" each character that we write. Insurance and other financial companies use the combination of OCR/ICR technology and databases to improve the data entry process. For example, a traffic citation most often contains a name and a driver's license number. The computer database of the same name and number combinations is stored at the state's motor vehicle registry. By using that database, either directly or as a downloaded subset, a court could develop a system to OCR/ICR traffic citations and validate the information against the database. The OCR/ICR doesn't have to be perfect. It can be used to affix the citation to the proper defendant. This technology also could be used for child support and other cases where information has been previously stored.

Types of data and documents

Data and document formats are important to courts because the information must be easily read and stored. Paper documents have a common format called paper and ink. How the basic standard of paper and ink is created by all the different technologies such as handwriting, printing press, typewriter, mimeograph, xerographic copy, and laser printing need be of no concern to the court. The court needs to focus on the fundamental elements of readability, portability (communications) and long-term readability.

Currently, there are three basic document types: images, limited and tagged. Each is discussed below.

> **Images** are what we use on paper. This is information that can usually (see discussion above regarding OCR/ICR) only be accurately read and worked on by

people. Other than retrieval and display, computers have difficulty working with image documents.

Limited documents are those which by design have limitations placed upon them for a variety of reasons. Some are the result of proprietary codes, which allow the programs to display and print data in a special way. Word processing programs and the documents that they produce fall into this category. In addition, special document formats, such as Adobe Acrobat PDF or Folio, are designed to control how documents are retrieved, viewed or printed. There are advantages to limited documents. Word processing documents have many capabilities, including the ability to embed field data information, create automatic hyperlinks and macros to automate tasks. Acrobat PDF files can accurately display or print documents while maintaining the format. Several courts are accepting documents in Acrobat format as part of their e-filing systems. The downside for courts is whether or not these formats can be read and used by computers in the future without expensive conversions.

Tagged documents currently are best seen on the Internet. Anyone viewing an HTML (HyperText Markup Language) Internet page is familiar with a tagged document. With an Internet browser, the "view source" feature shows how information is tagged in an Internet page. For example, a simple tag for the title of the document looks like this:

<title>The text of the title of the document**</title>**
Tagged documents have advantages of being written in standard ASCII so computers can read them in the future. Further, HTML is being enhanced with a new version called XML or eXtensible Markup Language, which will allow data to be identified within documents. The federal courts currently are looking into future use of XML documents.

It is likely that all of these document types will be used in a court's e-filing solution. Courts should plan to use the various document types where they work best without prejudice to a single solution.

Summary

E-filing requires a paradigm shift for the attorney, the courts, the judges and the court personnel. It is obvious that all parties will benefit, but each court must evaluate what solution provides them with the most efficient and robust system. To effectively implement e-filing, the court must consider: usability, hardware, software, connectivity,

communications, security, and integration into existing systems or processes, user and systems support, performance, reliability, and scalability.

Chapter 7: Budget Planning

Courts usually must perform at least some preliminary budget analysis as a part of investigating the feasibility of implementing electronic filing. Once the decision has been made to pursue this application of technology, the real budget planning begins. The complexity of the budget planning process depends upon many factors, including:

- The size of the court.
- The extent, quality and capacity of the current technology infrastructure.
- The scope of application for electronic filing across different divisions and case types.
- The capabilities and adaptability of the current automated case management system.
- The balance between technology services delivered directly by the court and services outsourced to a third party.

The purpose of this chapter is to help court managers identify the components necessary to include in the budget planning process and provide a budget-planning tool, in the form of an electronic spreadsheet, to assist them. The discussion assumes that the court already has a functioning case management system, as this is a precursor to any consideration of electronic filing. In addition, workstations, printers, network cabling and other components exist and are adequate to handle the case management system, office automation or desktop productivity applications, and other technology applications installed in the court. In other words, this chapter focuses on the budget planning process necessary to address the addition of electronic filing technology to an existing base of hardware and software.

The existence of a case management system and an appropriate technology infrastructure to support it, however, does not mean the court's technology is adequate to permit simply plugging in an electronic filing component. Case management software

will require upgrading, for example, to link tightly with a document management system and the electronic filing system that delivers documents to it. Additional workstations and upgraded processors also may be necessary. The local-area network probably will require upgrading as well to handle the increased traffic and volume of data passing through it. Consequently, this chapter does address those prerequisite and concurrent improvements that court managers must take into consideration in conjunction with an electronic filing project.

Budget Planning Worksheet

There are numerous ways to organize the cost categories in planning for a technology project. The worksheet that forms the core of this discussion is structured around three broad categories: organizational readiness, upgrade of the existing technology infrastructure as needed to support electronic filing, and implementation of the fundamental electronic filing component or "front end" of the court's technology system. Each of these broad categories is subdivided into two types of costs. Equipment, software, materials, services, utilities, and facilities are one type of expense. The other reflects the time and effort required for planning and implementation. It is referred to in the worksheet as "human resources" and includes salary, fringe benefits and other expenses associated with all court staff involved in the project.

Furthermore, within the category of upgrading the existing technology, separate sets of costs are identified for major components that must be upgraded or added: the case management system, a document management system, the general network infrastructure, and the court's Internet capabilities. Finally, the worksheet provides for estimating the costs for each of the first three years. Subtotals are accumulated for the two types of

costs (human resources and all costs that are not human resources costs) for each year, and then the total cost for each is shown on an annual basis.

The worksheet is designed as a flexible tool that can help court and technology managers think through the budgeting process. It is not intended to be inclusive of all cost factors or ideally suited for any particular situation. Every court has a different set of circumstances to consider in planning for electronic filing. There is tremendous variation from court to court in the type of computer hardware and software installed, the age and capabilities of the systems, the number of users, the approach to buying or building new applications, the source of funding and procedures that must be followed, and the organization and capabilities of the technical staff. Consequently, some of the budget items may not be needed, while others may need to be added.

The worksheet also is one-sided; that is, it encompasses costs only. As discussed throughout the monograph, when courts implement electronic filing, they can anticipate some costs savings or cost avoidance to help offset the one-time and ongoing expenses. Although the worksheet is concerned only with the expenses for which funding must be allocated, courts should identify potential savings as part of their long-range planning and, if necessary, to justify the expense of implementation.

Potential cost savings span a range of categories, many of which are applicable to the majority of courts. As discussed in Chapter 5, for example, reducing the necessity for physical handling of paper files eliminates many labor-intensive steps in processing cases, freeing up staff time for other duties. While such technology projects seldom result in laying off workers (and may even require the temporary addition of staff), they can reduce sharply the need for future staffing increases commensurate with rising workloads. A second area of savings is the reduction in storage space needed to house

physical files. Even with additional hardware requirements, electronic files consume only a fraction of the expensive square footage needed for paper records. A third area of savings is the simple result of purchasing less paper and fewer file folders, shelves and file cabinets. Paper documents generate more paper because of the need to make copies for each person who needs access, while electronic documents can deliver simultaneous access to everyone. Furthermore, paper costs increase steadily over time, whereas computer storage costs decrease constantly, often at an astonishing rate. When electronic filing is fully implemented and integrated with case management software, additional savings result from eliminating some of the manual data entry now necessary to update the court's database as new documents are filed.

Readers are encouraged to view the worksheet as a starting point from which to develop one or more budgeting tools more specifically suited to the needs of their own courts and the approach to electronic filing they choose. Budget planners may wish to add cost savings categories or create worksheets specifically for cost savings. Alternatively, they may decide to incorporate projected savings in the amounts they enter in the cost categories already appearing on the worksheet.

A printed version of the worksheet appears below. The remainder of the chapter is devoted to a brief explanation of each cost component or line item on the worksheet, with respect to its implications for the budget. The items are discussed in the order in which they appear on the worksheet. Chapter 6 describes the technology components in more detail, and Chapter 8 covers the major items included in the worksheet in terms of how they fit into the overall implementation process.

Electronic Filing Budget Planning Worksheet

	Year 1 Costs	Year 2 Costs	Year 3 Costs
Organizational Readiness			
Educational materials, services, conference fees, travel, etc.			
Consulting fees			
Other expenses			
Human Resources			
Preliminary education and training			
Initial planning activities			
Develop conceptual design and implementation plan			
Other activities			
Upgrade of Existing Technology			
Case Management System			
Application software replacement or upgrade			
Server hardware upgrades			
Client/PC upgrades			
Contractor services			
Hardware maintenance			
Other expenses			
Human Resources			
Develop and implement additional functions			
Perform or manage hardware upgrades			
Prepare and deliver training, documentation, user support			
Court staff time for training			
Other activities			
Document Management System			
Document management software purchase			
Document server hardware			
Client/PC hardware upgrade or purchase			
Peripheral hardware/software (e.g., scanners, monitors)			
Contractor services			
Hardware maintenance			
Other expenses			
Human Resources			
Staff time for acquisition and integration			
Perform or manage hardware upgrades or installations			
Prepare and deliver training, documentation, user support			
Court staff time for training and parallel testing			
Other activities			
General Network Infrastructure			
Upgrade cabling, hubs, routers, etc. for increased traffic			
Upgrade server processor, memory, disk capacity			
Upgrade network OS, monitoring, and security software			
Upgrade modems and phone lines for local dial-up			
Implement or upgrade network fax capability			
Implement or upgrade e-mail and office productivity software			
Upgrade system backup capabilities			
Uninterruptible power supplies (UPS)			
Upgrade PCs and monitors (if not already covered above)			

Additional public terminals for case information access			
Additional conditioned space for components or staff			
Hardware maintenance			
Other expenses			
Human Resources			
Planning, analysis, and management of network upgrades			
Technical staff time to accomplish network upgrades			
Other activities			
Internet Capabilities			
Servers (Web, e-mail, proxy, etc.)			
Additional communications hardware and software			
Server software and Web development tools			
Browser software and other end-user tools			
High-speed phone lines (ISDN, T1, etc.)			
Security(firewall hardware/software, etc.)			
Internet service provider fees			
Hardware maintenance			
Consulting fees			
Other expenses			
Human Resources			
Planning and mgmt of Internet implementation/upgrade			
Staff time to implement or upgrade Internet components			
Staff for webmaster and Internet technician positions			
Prepare and deliver training, documentation, user support			
Court staff time for training			
Other activities			
Implementation of E-Filing Component			
Separate e-filing server with fault-tolerance or redundancy			
Uninterruptible power supplies (UPS)			
Backup capabilities for E-filing transactions			
E-filing application software or interface with service provider			
User billing and accounting software, if separate			
Consulting fees			
Other expenses			
Human Resources			
"Marketing" and education for legal community			
Detailed planning and development of court procedures			
Planning, analysis, and management of implementation			
Technical staff time for installation and testing of components			
Training and support of court staff and attorney users			
Court staff time for training			
Court and technical staff time for parallel testing			
Billing and accounting (if additional procedures)			
Other activities			
TOTALS			
Equipment, Software, Services, and Other Costs	0	0	0
Human Resources Costs	0	0	0
Grand Total Costs	$0	$0	$0

Description of Worksheet Fields

Organizational Readiness

Educational materials, services, conference fees, travel, etc.

This entry covers a range of hard costs associated with preparing court officials and staff to move forward with electronic filing. Judges or managers may wish to visit other jurisdictions that have implemented electronic filing, attend seminars and educational conferences, or obtain books, videos or other information to use within the court.

Consulting fees

Consultants may be engaged to help with initial planning activities, conduct a needs assessment, or to provide education about electronic filing.

Other expenses

Any other non-personnel costs associated with preparing the organization should be recorded here.

Human Resources—the following items are personnel-related costs resulting from staff time expended on organizational readiness activities.

Preliminary education and training

This entry covers costs for staff time spent in preparing, conducting or attending educational and training activities.

Initial planning activities

Costs for time spent on planning tasks, including meetings and deskwork, should be recorded.

Develop conceptual design and implementation plan

This item shows costs for staff time involved in either performing or managing the development of analyses, designs, implementation plans, etc.

Other activities

Personnel costs for all other activities associated with organizational readiness should be entered here.

Upgrade of Existing Technology

Case Management System

Application software replacement or upgrade

This entry relates to the non-personnel costs associated with upgrading the case management system software to integrate it with an electronic filing front end. If

extensive changes will be needed to a very old system, this may present the opportunity to replace the software with a new system.

Server hardware upgrades

This category can be adapted as needed for the computer platform used to support the case management system in each court. For example a series of network server PCs may be used in one court, while the database and programs may reside on a midrange computer in another court.

Client/PC upgrades

Individual workstations may need upgrading to handle new or improved case management software as well as to support electronic documents more effectively. Additional units may also be needed as fewer operations rely on paper.

Contractor services

Consultants, contract programmers, or software vendor services may be required to accomplish the upgrades to the case management system.

Hardware maintenance

The estimated cost for hardware maintenance contracts, average equipment service costs or the cost of additional hardware held in reserve for replacement purposes should be entered here.

Other expenses

Any other non-personnel costs associated with upgrading the case management system can be recorded here.

Human Resources—the following items are personnel-related costs resulting from staff time expended on upgrading the case management system.

Develop and implement additional functions

This entry covers the time spent by technical staff and other court employees to manage or perform various tasks needed to upgrade the case management software.

Perform or manage hardware upgrades

Staff time associated with planning, acquiring, installing, and testing hardware upgrades for the case management system can be entered in this item.

Prepare and deliver training, documentation, user support

Staff time expended for up-front preparation or acquisition of training materials and programs, conducting training of court staff, and preparing user documentation should be estimated here. The estimate should include staff costs for help desk operation and other ongoing user support to the extent that these costs can be attributed to the software upgrades.

Court staff time for training

In addition to the time expended by the technical staff or others responsible for providing the training, the cost of the time required for the users to receive training should be accounted for. Also, if technical staff must be trained on new software tools or maintenance of new system functions, their time should be reflected here.

Other activities

Personnel costs for all other activities associated with upgrading the case management system should be estimated here.

Document Management System

Document management software purchase

Most courts elect to purchase, rather than build, the document management software needed to complement traditional case management functions. All software-related costs for this component should be estimated here.

Document server hardware

A separate document server is usually installed during this upgrade process, or dedicated disk drives may be added to a mid-range or mainframe environment to handle the document management system. All such costs should be recorded here.

Client/PC hardware upgrade or purchase

PC workstations should be assessed to determine if they have adequate processor power, local hard disk capacity and adequate video graphics performance suitable for document management use. Costs for upgrades and replacements should be estimated here.

Peripheral hardware/software (e.g., scanners, monitors)

This entry can be used to capture the cost of high-resolution monitors, scanners, optical storage, or other types of peripheral equipment needed for the document management system.

Contractor services

Consultants, contract programmers, or software vendor services may be required to implement the document management system.

Hardware maintenance

The estimated costs for hardware maintenance contracts, average equipment service costs, or the cost of additional hardware held in reserve for replacement purposes--to the extent that those costs stem from the document management system--should be entered here.

Other expenses

Any other non-personnel costs associated with implementing the document management system can be recorded here.

Human Resources—the following items are personnel-related costs resulting from staff time expended on implementing or upgrading the document management system.

Staff time for acquisition and integration

This entry covers the time spent by technical staff and other court employees to manage or perform the various tasks needed to implement the document management software.

Perform or manage hardware upgrades or installations

Staff time associated with planning, acquiring, installing, and testing hardware upgrades or additions needed for the document management system can be entered in this item.

Prepare and deliver training, documentation, user support

Staff time expended for up-front preparation or acquisition of training materials and programs, conducting training of court staff, and preparing user documentation should be estimated here. Also included should be staff costs for help desk operation and other ongoing user support, to the extent that these costs can be attributed to the document management system.

Court staff time for training and parallel testing

In addition to the time expended by the technical staff or others responsible for providing the training, the cost of the time required for the users to receive training should be accounted for. Also, if technical staff must be trained on new software tools or maintenance of new system functions, their time should be reflected here. Finally, initial implementation likely will require maintaining parallel paper-based procedures. The cost of this temporary additional effort should be estimated and entered here.

Other activities

Personnel costs for all other activities associated with implementing the document management system should be estimated here.

General Network Infrastructure

Upgrade cabling, hubs, routers, etc. for increased traffic

This item reflects the cost of upgrading the network topology and associated hardware components. With the shift to document management functions and subsequent electronic filing, the network must be capable of supporting peak traffic loads without substantially degrading performance and user response.

Upgrade server processor, memory, disk capacity

New high-performance network servers may have to be purchased, or existing servers may require upgrading to handle the increased workload and provide more reliability.

Upgrade network OS, monitoring and security software

Along with hardware components, network software should be added or updated to achieve the required level of performance, reliability and security. Monitoring the status of network performance and maintaining network security, which become critical with primary reliance on electronic data and communication, requires specialized software tools.

Upgrade modems and phone lines for local dial-up

As court officials and staff move into the electronic world, it is important to support e-mail and access to court information through adequate local connectivity. A sufficient bank of high-speed modems will ensure that staff can connect from off site. If dial-up access is provided to the bar or other outside users, the communications interface should be adequate to meet the total demand.

Implement or upgrade network fax capability

The network should be equipped to permit efficient fax transmission directly from electronic versions of documents and other information sources. Similarly, the network should be capable of receiving incoming fax transmission for routing or storage as an imaged document. The cost of fax hardware and software components should be estimated here.

Implement or upgrade e-mail and office productivity software

If courts hope to move into a comprehensive electronic environment, they must equip the staff with a current set of productivity tools. Costs should be developed for network versions of powerful office suite products that provide word processing, spreadsheet, database, calendar, e-mail, and other functions.

Upgrade system backup capabilities

Integrity and availability of electronic documents and databases must be insured through the use of dependable and efficient backup capabilities. Network downtime should be minimized, and recovery of deleted or damaged data should be as simple and reliable as possible. The estimated costs for hardware and software needed to provide the desired level of backup capabilities should be entered here.

Uninterruptible power supplies (UPS)

Servers and other critical network components should be protected from power outages, unacceptable voltage drops and surges through the installation of individual UPS units for each device or attaching them to circuits connected to a large-scale UPS. The cost for the UPS hardware, along with the accompanying software needed to perform an orderly automatic shutdown process, should be estimated here.

Upgrade PCs and monitors (if not already covered above)

All user workstations and monitors should be brought up to the standard required to ensure that staff can work effectively with all applications. Any associated costs not already attributed to case management or document management system requirements should be entered here.

Additional public terminals for case information access

As the court moves from paper to electronic operation, managers must ensure that adequate numbers of workstations are provided for public use. Because many of these workstations will be used by most people only for occasional inquiries, there may be an opportunity to employ some workstations that have trickled down from staff being equipped with newer hardware. Estimates should be developed for any new equipment, upgrades to existing equipment, and additional cabling or other components that will be needed to provide public access in the courthouse.

Additional conditioned space for components or staff

Gearing up the technology infrastructure may involve additional servers, scanners, printers, and, possibly, technical staff. New equipment and staff may require additional space and environmental controls, along with mounting racks and office furnishings. This line item can be used to enter any quantifiable facilities costs resulting from the technology upgrades.

Hardware maintenance

The estimated costs for hardware maintenance contracts, average equipment service costs, or the cost of additional hardware held in reserve for replacement purposes should be entered here if attributable to the general network upgrades.

Other expenses

Any other non-personnel costs associated with upgrading the general network infrastructure can be recorded here.

Human Resources—the following items are personnel-related costs resulting from staff time expended on implementing or upgrading the general network.

Planning, analysis and management of network upgrades

This item is for the cost of staff time expended managing the overall process of upgrading the network infrastructure, as well as conducting the planning and analysis necessary to determine what must be done.

Technical staff time to accomplish network upgrades

In contrast to the above item, this line reflects the cost of staff time spent on installing, configuring and testing new components.

Other activities

Personnel costs attributable to all other activities associated with upgrading the general network infrastructure should be estimated here.

Internet Capabilities

Servers (Web, e-mail, proxy, etc.)

This line item captures the cost of Internet server hardware. The extent of hardware required will be determined by a number of factors, such as how many users need to be

supported, how the different functions (e.g., Web, FTP, listservs, general e-mail, and security) are to be distributed, and what type of Internet service provider is being used.

Additional communications hardware and software

In addition to the servers, costs must be figured for any communications hardware and software needed for the Internet capabilities.

Server software and Web development tools

This line is for the cost of the software that runs on the different types of servers, as well as software tools needed to develop and manage a Web site.

Browser software and other end-user tools

In addition to the software described above, all users must have Web browser software installed on their PCs if they are to access the World-Wide Web. Some non-technical court staff also may be assigned responsibility to provide Web content. These individuals will need appropriate software tools (e.g., Microsoft FrontPage) or extensions to office productivity tools that permit conversion of documents and other files to HTML pages. While some browser software is free or built into the operating system, estimates should be developed for the cost of other tools needed to meet the uses planned for the Internet capabilities.

High-speed phone lines (ISDN, T1, etc.)

Installation costs, fixed monthly fees and anticipated usage charges for upgraded communications lines should be entered here. It is imperative to provide sufficient bandwidth to meet the expected demand for Internet traffic.

Security (firewall hardware/software, etc.)

Establishing a secure Internet capability should be a top priority for courts preparing for electronic filing. This involves installing a robust firewall between the court's computer system and the Internet connection. Costs for all security components, both hardware and software, should be added here.

Internet service provider fees

Many different arrangements are possible for connecting the court to the Internet backbone, depending upon the size of the court, the technical capabilities, local phone service characteristics, and providers in the area. Startup costs and monthly fees should be estimated and entered on this line.

Hardware maintenance

The estimated costs for hardware maintenance contracts, average equipment service costs or the cost of additional hardware held in reserve for replacement purposes should be entered here if attributable to the Internet technology.

Consulting fees

The court may need the services of a consultant to determine the best implementation strategy or to advise court staff on components or configurations. Fees for all such services should be entered here.

Other expenses

Any other non-personnel costs associated with implementing or upgrading the Internet capabilities can be recorded here.

Human Resources—the following items are personnel-related costs resulting from staff time expended on implementing or upgrading the Internet technology.

Planning and management of Internet implementation/upgrade

This line is for the cost of staff time to plan and manage the implementation or upgrade of the court's Internet capabilities. Activities such as meetings with court managers and staff to determine how the Internet should fit into the court's technology strategy, working with vendors to obtain costs for hardware, software, and services, designing security strategies, exploring other Web sites for ideas, and orchestrating the work of technical staff and consultants throughout the implementation or upgrade process should be included.

Staff time to implement or upgrade Internet components

This line should cover time spent by technical staff to install, configure and test components.

Staff for webmaster and Internet technician positions

This item can be used to enter costs associated with additional positions required for the Internet. If a portion of existing staff's time is allocated to these new tasks, those proportionate costs should be entered here.

Prepare and deliver training, documentation user support

In many courts, implementation of new or upgraded Internet technology may require additional training of end users and technical staff as well. The cost of employee time to provide such training should be entered here.

Court staff time for training

To the extent that time spent receiving training or acquiring self-training through documentation, tutorials or experimentation can be measured or estimated, the associated costs should be entered here.

Other activities

Personnel costs attributable to all other activities associated with implementing or upgrading the Internet capabilities should be estimated here.

Implementation of E-Filing Component

Separate e-filing server with fault-tolerance or redundancy

Hardware costs for a dedicated e-filing server should be calculated and entered on this line. It is essential to provide a secure, reliable connection for electronic filing users that is always available. Documents submitted electronically must be protected from

damage or loss, as well as being available without delay for processing by court staff or automated procedures. For these reasons e-filing servers may have built-in fault-tolerant technology or some redundancy of components that makes them more costly than ordinary servers.

Uninterruptible power supplies (UPS)

E-filing servers and other components should be protected by UPS units to ensure that they are not knocked out of service by power problems. The cost of these devices should be entered here.

Backup capabilities for E-filing transactions

Enter the cost of any backup devices dedicated to the e-filing system components storing incoming electronic documents and transactions.

E-filing application software or interface with service provider

The purchase cost of e-filing software or any software required to connect with e-filing service providers should be entered here. If the court develops its own software, those costs should be recorded below as human resources costs.

User billing and accounting software, if separate

If the court handles the billing and accounting functions associated with e-filing, additional software may have to be purchased to perform these functions. If existing case management accounting software can be used to handle these functions, then there may be no separate costs. Financial software developed in house for this purpose should be recorded as a human resources expense.

Consulting fees

The court may wish to hire a consultant to help with planning and implementing electronic filing. Fees for such services should be entered on this line.

Other expenses

Any other non-personnel expenses associated with implementing the e-filing system should be entered here.

Human Resources—the following items are personnel-related costs resulting from staff time expended on activities related to implementation of electronic filing.

"Marketing" and education for legal community

Active participation by the local bar is essential from the beginning of any e-filing project. Court staff will need to spend adequate time promoting the project, educating the legal community about it, and securing their involvement in planning and implementation tasks.

Detailed planning and development of court procedures

Beyond the preliminary planning phase, court staff must plan, develop and document the detailed procedures whereby the electronic filing technology is to be used. This line should reflect the cost of those activities.

Planning, analysis and management of implementation

This line should capture the cost of the time expended by court and technology managers and analysts in directing the implementation of the e-filing technology, determining the components to be used and designing the functions and interfaces.

Technical staff time for installation and testing of components

Costs for staff to install, test and put into operation all of the hardware and software components for the e-filing front end should be entered here.

Training and support of court staff and attorney users

This item shows the personnel costs associated with developing and delivering training for court staff and the attorney users, as well as providing ongoing support to all users.

Court staff time for training

The estimated cost for the time court staff spends to receive training should be entered here.

Court and technical staff time for parallel testing

As part of the initial implementation of e-filing, most courts will conduct tests of the new procedures and operate in parallel with the paper system for some period of time. The extra time spend on these activities should be estimated and the corresponding human resources costs entered here.

Billing and accounting (if additional procedures)

To the extent that additional effort is expended on billing and accounting for the e-filing users, those costs should be shown here.

Other activities

Personnel costs attributable to all other activities associated with implementing the e-filing capabilities should be estimated here. An example of a possible additional cost is the cost of converting existing documents to some form of electronic document. When a court switches over to electronic filing, it may decide that all active cases should be converted to avoid a dual medium for documents in a single case. Staff time spent retrieving, preparing, scanning, verifying, and indexing those documents must be included as a human resource cost.

TOTALS

Equipment, Software, Services, and Other Costs

This line is the total of all costs other than human resources. It reflects the sum of all line items for hardware, software, consulting fees, travel, training materials, conference fees, phone lines, and other services.

Human Resources Costs

This line is the total cost of human resources across all categories. It is the sum of each line item shown under the Human Resources subheadings.

Grand Total Costs

This line reflects the total estimated cost of the project for each year. It is the sum of the above two subtotals.

Chapter 8: Implementation

Thousands of details attend the implementation of electronic filing or any major new technology. If a project is not well planned, many of these details may not be apparent until they bring activity to a halt. Although it is not possible to outline all of the implementation steps for every conceivable electronic filing project, what follows is an attempt to cover elements that may appear in most.

The discussion of technology deployment is divided into three sections: initiation, planning and implementation. Implementation issues relating to automation in general are covered in *Automating Court Systems*[162] and are not repeated here.

Project Initiation

Project initiation is the activity that occurs from the first indication that a problem exists or may arise through the creation of a project management structure and process. It includes recognizing the need for electronic filing, setting goals and objectives, obtaining a commitment from the court to solve the problem, recruiting progressive law firms to participate, acquiring planning resources, and establishing a project management system. Thorough attention to each step of this process is necessary to establish realistic expectations for electronic filing.

Recognition of need

Electronic filing technology can benefit courts and law firms in many ways, but it is not a magic solution to all problems. A requisite first step in project initiation is to understand the problems that exist in the justice system and find appropriate solutions. An electronic filing system will do little to improve poor calendar management, for

example. The following are examples of problems that may be corrected by electronic filing.

- **Customer service:** Inability to answer routine questions from the case management information system without tracking down the paper file.
- **Redundant work:** Dual entry of data from documents to computer systems adds to the work of overburdened staff, producing higher error rates and case processing delays.
- **Workflow problems:** Inability to define unique paper processing procedures for specific types of documents, resulting in bureaucratic and inefficient paper flow.
- **Staff performance:** Inability to monitor and manage the productivity of staff engaged in paper processing work.
- **Redundant record systems:** Law firms are required to duplicate court record systems because of the inability to access judicial case files quickly and inexpensively.
- **Lengthy delays attributable to file management:** Pulling case file jackets, inserting documents and re-filing delay action in cases.
- **Inadequate storage space:** The growing numbers and size of case files strain space available for storage.
- **Security:** Microfilming of documents as they are filed (in addition to microfilming at the conclusion of the case) is necessary to assure the court's ability to reconstruct lost files.
- **Damaged records:** Wear and tear on papers and folders threaten the integrity of case files.

Too often organizations acquire a technology solution, then look for a problem to fix with it. Computerization is far more effective when designed to address the specific a court is facing. The same is true with electronic filing. Courts and law firms should

[162] Lawrence P. Webster, *Automating Court Systems* (Williamsburg, National Center for State Courts, 1996).

evaluate their problems and needs carefully before deciding if electronic filing will be beneficial.

Goals and objectives

Once the challenges a legal system faces are documented and understood, leaders will be in a much better position to move forward. The next step in the process is to set goals for solving the problems that have been identified. This may not entail the immediate implementation of electronic filing. For example, improvements to the court case management system may resolve a portion of the difficulties, while at the same time emphasizing the benefits to be gained by electronic filing.

The process of setting goals and objectives is beneficial because it gets everyone involved to agree on what will be done, as well as what will not be done, before resources are inefficiently expended. It begins a practical and political process of introducing change into the system. Change redistributes power and other resources in an organization or system, and could, for example, upset the competitiveness of law firms in the area.

Goals should define the ultimate outcome expected of the project. Objectives subdivide each goal into narrower and shorter-term pieces. Both goals and objectives should be:

- Specific.
- Measurable.
- Realistic.
- Attainable.
- Clearly articulated.
- Established by consensus.
- Broadly communicated throughout the organization.
- Generally accepted by everyone involved.

Most goals are established at the policy, legal and operational levels. Courts and law firms also should address technical goals for system performance. These goals and objectives should cover system:

- Availability.
- Maintainability.
- Interconnectivity.
- Security.
- Reliability.
- Portability.
- Scalability.
- Simplicity.
- Usability.

The following are a few examples of goals that could be established for an electronic filing project. While the list is not exhaustive, it provides samples from a broad range of possibilities.

1. **Electronic case file.** The court will create an electronic case file that will replace the paper folder as the primary source of information about the case. It will contain all the documents, attachments, photographs, and other materials traditionally found in the case jacket.

2. **Access.** The court will provide free public access through the Internet to the electronic case file within the bounds of existing statutes and court rules governing the security and confidentiality of paper records.

3. **Access to other resources.** The court will provide access to dockets, calendars and other resources contained in the case management system in the same format as it provides access to the electronic case file. The docket will serve as a register or index to all actions, events and documents in the case.

4. **Electronic filing.** The court will allow any interested law firm that uses equipment and software that meets system standards to file all papers electronically.

5. **Filing and access times.** The electronic filing system, electronic case file and case management system will be available to the public and law firms 24 hours a day, seven days a week, except for scheduled, routine system maintenance. System availability during normal business hours will exceed 99 percent, and will exceed 95 percent during times the court is not open.

6. **Cost savings.** Processing of electronic documents will increase the productivity of court staff and reduce operational cost by eliminating much paper processing tasks, redundant data entry, etc.

Court commitment

The next step in the project initiation phase is obtaining commitment from court leaders to proceed with the electronic filing project. Chapter 2 covers this topic thoroughly, and includes three elements of the business case: benefits of electronic filing, assessment of the technology options and lifecycle costs. It is essential that court and law firm leaders work together from the beginning of the project, or it will fail.

Lawyer support

Even though a few technology-adept lawyers may take a leading role in convincing courts to develop electronic filing, often they do not control the resources within their firms and cannot decide to participate in the venture without convincing others within the office. Marketing to decision-makers in law firms is also an important step, as was shown in Chapter 2. Consultants, vendors or other service providers with experience in working with attorneys can assist in this activity.

A surprising number of courts have built electronic filing systems without adequate consultation with the lawyers who would use it, thinking they could dictate internal business decisions and procedures within the law offices. Policy, management and technology leaders from both sides must develop a flexible solution that matches the capabilities and resources that are available. The system also must be flexible, so it can be adapted to future changes in the legal environment. This can only be accomplished with a great deal of communication and cooperation.

Acquire planning resources

The second phase of the project will require significantly more resources than the first. During the planning phase, a needs assessment, conceptual design and implementation plan will be developed. In addition, system standards will be determined. These activities may require workers and skills not available to the courts or the law offices. Experienced consultants could be invaluable if current staff is too overburdened to complete the project. It would not be unusual to require two or three individuals for a period of three to six months to complete the planning phase of the project. Larger or more complex operations may require significantly more help.

In addition to staff or consultants assigned to work on planning, other employees of the court and law office also must participate. The planning team must meet with individuals in many parts of the organization to learn how it works and help gather necessary information. This will temporarily reduce the availability of staff as they participate in the needs assessment and related activities.

Leaders of the court and law firms should determine who will be responsible for completing each task and then pursue the acquisition of funding from management or funding bodies to complete the work. This step also may include the hiring of consultants.

Establish project management structure and process

Every endeavor requires the coordination of the work of many individuals. Court and law firm leaders must establish structures and procedures for making decisions and assignments, for solving problems that will crop up from time to time, and for keeping commitment high within all of the organizations that are involved in the electronic filing

project. Trying to decide who is responsible for making a decision while in the middle of trying to make one is a recipe for disaster.

A typical approach is to create a steering or advisory committee that is representative of all the organizations. It should include policy leaders and workers who are familiar with internal operations and the implications of decisions. Some committees include technologists, while others have them serve in an advisory capacity.

Once the structure is in place, it is essential to have the individuals meet, receive instruction in their duties and work out the ground rules for committee operation. Technology staff can help organize this meeting. It is not uncommon for these groups to have only limited decision-making authority, though they tend to work better when every decision is not reviewed at a higher level. In other words, they should have sufficient authority to keep the project moving forward, but also should be required to obtain approval for decisions that commit significant resources of their organizations.

Project Planning

This is the phase of the project at which most of the important decisions are made after an intensive study of work processes and available options. The implementation plan, which is the final product of this stage, outlines what work must be done, who will do it, when it must be completed, and how much it will cost.

The planning phase of the project consists of seven steps: evaluation of need, analysis of current system, review of options, conceptual design, development of standards, creation of an implementation plan, and acquisition of resources to complete the project. Each is discussed below.

Evaluation of need

The evaluation of need for an electronic filing project consists of two parts, an evaluation of workflow, as would be done for a case management system project, and a review of the technology infrastructure of the court and law firms. The project team interviews and observes people doing their day-to-day work, documenting processes carefully. Another helpful technique is to review case files. This will help provide realistic data about the volume and type of documents filed with the system.

The product of the needs assessment is a formal document that describes how work moves through court processes, including estimates of transaction volume. It also includes a listing and analysis of the system components of any personal computer networks, case management system, document management system, and communications networks that are already in place.

Analysis of current system

The evaluation of need is a description of workflow and system components.[163] It is also necessary to conduct an analysis of problem areas, and processes and equipment that likely will require modification or replacement as electronic filing is implemented. For this reason, it is important that staff analyzing needs assessment data be familiar with electronic filing technology and its potential for changing work patterns.

A good example is the personal computer network that may be in use. While some older PC models may be adequate for word processing functions, they may not have the power or display resolution to show document images clearly. These personal computers must be upgraded or replaced before electronic filing technology is deployed.

[163] Chapter 2 of *Automating Court Systems* contains a detailed review of tools and processes for conducting the needs assessment.

In addition to reviewing workflow and equipment needs, staff conducting the analysis must look at higher-level issues, including organization and staffing, court rules and operational procedures, potential legal obstacles (as outlined in Chapter 3), and other policy issues (found in Chapter 4). A mistake repeated many times in early experiments with case management systems was to overlay technology on manual processes with minimal change to those work patterns. This produced inefficient systems that often failed to benefit from the new tools that were installed. Today, most organizations appreciate the value of reengineering to productivity and success with technology.

Review of options

Electronic filing technology cannot be purchased in a shrink-wrapped package. No vendor offers a product that can be installed in a few days, at least not yet. But even though electronic filing is still an emerging technology, it is not necessary to build it from scratch. Many components of such a system are mature and stable products. It is important to understand the difference to assess risk successfully. The challenge is to select and meld appropriate components so they work effectively and efficiently, engineered so they can handle peak loads when the system is fully operational. This is no simple task.

Other options exist, such as using service providers for certain parts of the process. Most courts are leery of outsourcing important functions, but must remember that they now rely on many outside service providers in moving documents from place to place. For example, the post office, delivery services, couriers, telephone companies, credit card companies, and banks all are part of the current legal system infrastructure. In a similar way, electronic commerce will rely on outside service providers. Until electronic

commerce is fully established, courts must decide how extensively to rely on the private sector to complete judicial business.

What choices exist for courts and law firms building an electronic filing system? The use of telephone companies and Internet service providers may be obvious. If digital signature technology is used for authentication and encryption, a number of other service providers may be available, such as certification authorities, public key repositories, etc.

It is certain that vendors will provide bundled electronic filing services for courts and law firms that will eliminate the need to perform many of the functions defined in previous chapters. For example, companies may receive and authenticate documents submitted by law firms, add date and time stamps, and pass them along to the court, eliminating many of the security issues and other procedural requirements from the court's implementation plan. They may provide other services, such as linking documents to statutes and case law, and posting selected documents to public repositories, like Stanford's securities litigation site.[164] Additional features will be developed as electronic filing technology matures. The added value of these features will furnish additional incentive to law firms and courts to use private sector service providers.

Case management systems will offer a challenge to court leaders who want to move ahead with electronic filing, only to discover that their existing computer system is inadequate or will require extensive modification. Because the case management system must serve as the index to the document management system, it must be stable and capable of meeting most of the data needs of the court. It is also a good idea not to implement electronic filing with a case management system that, even if meeting the

needs of the court, is nearing obsolescence. Any case management system will require modification to work with electronic filing; courts should be aware of the time and cost of making these changes and compare them to the expense of acquiring a new system. Some vendors are developing integrated case and document management systems, including electronic filing.

While this discussion has centered on the court case management system, it is important to note that many law firms also have comparable systems to manage their workloads. It is assumed that they will undergo the same process of integrating their case and document management systems.

The document management system is usually a new component for courts and law firms. These systems have not proven practical without electronic filing where they have been tried, because of the high cost of converting paper to an image format.

Document management technology is not as mature as case management systems, but will improve with time. The court must select a package that is capable of storing and displaying text, popular word processing formats, print formats like PDF, and images. A problem with some of the first electronic filing systems was the inability to accept images of pages that were not created on the attorney's word processor. Attachments will continue to be submitted to the court and must be included in any successful system. It is also essential to provide flexibility, especially the ability to add new formats as they become popular. Some electronic filing systems still rely on WordPerfect 5.1, and cannot accept documents created in Windows-based formats.

In building the document management system, designers must allow for the conversion of documents stored in older formats, and must be aware of records retention

[164] See http://securities.stanford.edu/index.html

issues. While most court personnel would like to have every document ever filed on the system, in reality, performance issues will require older closed cases to be warehoused on another server—still accessible, but not interfering with system operation.

The choices for communications are limited. Some courts instituted dial-up systems to accept documents, and others more recently have built private networks. The Internet has emerged as the only realistic option for courts and law firms just beginning the process. While existing networks may be adequate for data systems, electronic filing technology will require greater bandwidth to handle much larger transactions.

The options available for the electronic filing components of the system are tied to the scale of the system and the level of security desired. At the low end, courts could allow lawyers to access the document management server directly. At the high end, multiple servers could fill a variety of purposes, such as firewalls, electronic in-boxes, public access, and document storage. Chapter 6 provides a more detailed explanation of these options.

Conceptual design

The conceptual design will have two parts, document and workflow, and technology components. The first part describes how electronic pleadings will be created in a law office, transmitted to the court and served on other parties. It details what happens to the document when it arrives at the court, including indexing entries in the case management system. It explains the various paths the paper may follow as court staff processes it.

The second part of the conceptual design covers the technology that must be developed for the system to work properly. At a high level, it shows each piece of hardware and software, and how it contributes to electronic document processing. It shows the interfaces that must be developed and how they will work.

The conceptual design provides the vision of how the court and law firms will operate in the electronic world. It serves as a reference manual for the technologists building the system and for administrators reengineering the working environment. It is also a valuable tool for maintaining enthusiasm and commitment within the organizations that may be struggling with the added work the analysis and design processes have created.

Development of standards

At a minimum, standards must be created in three areas: documents, data and communications. Document standards should exist at two levels, content standards and technical standards. Content standards refer to the electronic equivalent of formatting: page limits, font and margin sizes and so forth. Most courts impose requirements on the legal community; standards that must be modified to accommodate electronic filing. For example, it may not make sense to establish page limits on documents that may never be printed on paper. In the electronic world, courts may require paragraph or line numbering, rather than page numbering. Instead of page limits, there may be restrictions on the number of characters submitted, or the number of hypertext links to external sources.

Technical standards for documents refer to format of the electronic file in which they are stored. Dozens of text, word processing, printer, and image formats exist, and the court must decide which ones it will accept or exclude. The capabilities of the document management software, and the personal computers in the court network, will dictate which options are best for the system.

Data standards also are important. Many courts require cover sheets with documents. These cover sheets are simply a way to pull information from the document so a clerk can enter it into the case management system without reading the document and guessing

about the meaning of terms. With electronic filing, there is an even greater need for formatted data, because the system can place it directly into the case management database to serve as an index to the pleading. In other words, if the information is formatted, data entry is eliminated. Data standards ensure that information provided by the lawyer will pass edits and will be accepted by the case management software. The standards should list the data elements required and acceptable codes, ranges and other edits that will apply.

Communications standards define the capabilities of equipment that will connect to the network. In a dial-up environment or private network, this includes communications protocols with a lot of technical jargon. For the Internet, it may be as simple as a list of browser plug-in packages that are required to view all of the materials stored in the system.

As has been mentioned, it will be necessary for the court and participating law firms to maintain the standards as they are developed. As new software, formats and protocols are established, they should be quickly incorporated. Older standards should be dropped as soon as all of the organizations are ready and when conversion of documents to a newer format is completed.

Creation of an implementation plan

An implementation plan will encourage the courts and legal community to walk through the implementation process in great detail. It will ensure that realistic time and expense estimates are prepared, and generate consensus about the work that needs to be done, who will do it, when it will be completed, and how much it will cost. The implementation plan will aid leaders with project management for the remainder of the deployment effort.

The plan should contain five components: tasks, schedules, assignments, budgets, and deliverables. Chapter 1 of *Automating Court Systems* describes some of the tools used in project planning and management, like the Work Breakdown Structure, Gantt Chart, PERT chart, Network Diagram, Critical Path Method, etc.[165]

Identification of the tasks that must be completed is the first step. Each task should be broken down into its sub-components until it is possible to estimate the amount of time necessary to complete it. The task list conceivably may include hundreds of items.

Many tasks can be finished concurrently, but some cannot begin until others are completed. Once these dependencies are identified and mapped out, it will be possible to schedule the work. The schedule will be modified as staff is assigned to each task. Since some tasks will be completed by court personnel while others are done by law office employees, it is important to separate this work into categories so each organization can identify its responsibilities and resource requirements. Since there are limits on the amount of hours a person can work, an overbooked staff member can delay project completion. Shifting assignments to others or adding staff can shorten the time needed for completion.

Once assignments and schedules are prepared, budgets can be generated. The cost of equipment, software, space, and other expenses are added to personnel costs. The final step is to define the deliverables for the project. These are milestones that measure progress. The payment of contractors and vendors should be tied to acceptance of these deliverables.

[165] Lawrence P. Webster, *Automating Court Systems* (Williamsburg, National Center for State Courts, 1996).

Acquisition of resources

With the implementation plan in hand, project leaders can request funding. This is an opportunity to reinforce work done initially to sell the plan to the organizations, restating the benefits and cost savings, and expense. Since most of the decisions have been made, it will be possible to be much more specific about the cost of the electronic filing system.

Project Implementation

The implementation plan covers all of the work described in this section. The group responsible for creating the plan should provide oversight to the implementation process, with the project manager responsible for day-to-day activity. During the implementation phase of the project, the oversight group must complete a transition of its role from project management to system management. This means that the same group that supervises the development and installation of the electronic filing system will continue to provide oversight once it is operational. They will be responsible for creating policies and procedures, introducing improvements to the system and solving high-level problems.

As new hardware is installed and new procedures implemented, it is important to make appropriate preparations to the facilities so the equipment and users can function properly and efficiently. Chapter 5 of *Automating Court Systems* contains a great deal of advice on this subject.[166] Other work also must be done, such as acquisition or development of the various components of the electronic filing system, which are detailed in the next five sections of this chapter. Work also is required to train staff,

[166] Lawrence P. Webster, *Automating Court Systems* (Williamsburg, National Center for State Courts, 1996).

prepare for startup and begin operation of the new system. These topics are covered in the sections that follow.

Case management system preparation

The case management system used by the court must be adapted to perform many new functions. New fields must be added to hold record keys to pleadings stored in the document management system. Some data fields may be deleted from the case management system, such as one that gives a summary of the contents of a document. Since the entire document is available and searchable, the summary has much less value.

Computer programs may be required to call document management system routines from the docket and other access points in the case management system. A user, for example, may want to view a particular paper listed on the docket screen of a case. With a mouse click or press of a key, the document should appear. In a similar manner, a user of the document management system may be reviewing a scheduling order in the electronic case file, and may want to see what other cases are on the calendar for the same judge that day. The case management system must be able to respond to calls from the document management system to provide this type of service.

The electronic filing modules may pass formatted data for entry in the case management system. The case management system must be capable of accepting and processing this information (perhaps after quick review by a clerk). It also may be required to respond to the filer with a docket number assigned to the new case, a scheduled date and time for the hearing requested, or with other similar information. The quality of the interface between the case management system and the electronic filing components is key to realizing increased staff productivity from the new technology.

Personal computer and network preparation

Several issues with existing personal computers and networks must be addressed before the implementation of electronic filing. The use of electronic documents will increase network traffic significantly, so upgrades may be required to supply sufficient bandwidth for smooth operation. Individual personal computers must be evaluated to see if they are adequate for the new working environment. The primary issue is the size and resolution of the display monitor, but processor speed, memory size and disk capacity also are factors to be considered. Some courts have found success with large monochrome monitors, which are much less expensive than their color counterparts.

Another important consideration is the availability of public access workstations. Since the court will reach the point where no paper files are available for some cases, making PCs accessible to the public becomes a much higher priority.

Law firms also must review the quality and capacity of their personal computers and networks. Appropriate communications capabilities, as well as the ability to view images, may be necessary.

Communications preparation

As with the court's internal networks, the level of traffic on external networks also will rise significantly. Whether the court chooses dial-up modems, network modems, bulletin board servers, or the Internet, increased capacity may be required.

For these networks it is important to look at the current strategy for providing service, such as the use of communications firewalls, routers, hubs, and switches, the use of proxy and mail servers, the capacity of telephone lines, the capability of Internet service providers currently used, and so forth. Perhaps the network and communications software may require an upgrade, or the court may have to switch from ISDN to T1 lines.

Identification of bottlenecks in the system will be important. Significant upgrades in one area may have no effect on response time if a bottleneck exists somewhere else. What appears to be a communications problem actually may be an inadequate server or slow disk access.

Finally, it is important to consider how to monitor system usage, particularly if users are billed based on connect time, transactions or some other similar measure. Some type of billing and collection system, integrated with usage monitoring, may be required.

Document management system preparation

The document management system likely will be a new component for the court. This is software that can organize and retrieve documents in a variety of formats: text, word processing, printer file, and image. The document management system should have a user interface that makes it difficult or impossible to tell the difference between file types; everything looks like a printed page on the screen. It also must be able to handle documents generated by the case management system.

As has been mentioned, it will be necessary for the case and document management systems to communicate with each other and function as an integrated, single product. If not, redundant data entry, lack of synchronization and other problems may result. The document management system also should be able to keep a log of transactions for security purposes.

The document management system probably will reside on a server that is dedicated for this purpose. The equipment and software must be installed and tested to ensure they are working properly before tests on the interface with the case management system and other components begin.

Electronic filing components preparation

The number and type of components in this area will vary greatly, depending on the size of the court and legal community, the volume of cases that will be processed, and the strategy chosen by court and law firm leaders. A variety of functions may be performed in most implementations, though they may reside on separate servers in some areas, and may be consolidated on fewer machines in others.

The first function is interaction with the user. As attorneys file papers with the court, they will be required to interact with the system through the World Wide Web, a private network, or dial-up system. As they pass documents and data, the system must inspect them and provide immediate feedback if there are errors. It should provide confirmation of successful filings, as well. The system should log all transactions for purposes of security and document authentication. Routines also will be required to allow lawyers and the public to view documents filed electronically.

The electronic filing system may perform document authentication functions, such as verifying the digital signature affixed to the filing. It also may complete service of process (or notification of service) on the other parties in the case.

Other routines may detect new filings on an in-box server and pull the documents and data through the firewall for processing by the case and document management systems. Again, how a court (or service provider) chooses to perform this function could take many forms.

Testing

After individual components of the electronic filing system are installed and tested, it is important to conduct thorough end-to-end tests that will identify problems between

components, and help determine if system performance will be adequate to provide acceptable response times for users.

Training

The success of any automation endeavor depends on individuals with the lowest pay and least respect of any employees of the organization, those doing data entry. It makes little sense to invest thousands or millions of dollars in new systems and fail to provide adequate instruction to baseline system users.

Electronic filing training for court staff should be an extension of case management system training. Separate programs must be developed for law office employees who perform much different functions within the system. Training must recognize the new operational procedures that are being implemented along with the technology. In-depth training must be provided for supervisors and those responsible for maintenance of hardware and software systems.

Most reference and training documentation is now provided on-line. This is a good strategy to use with new electronic filing systems. These materials must be prepared before training begins and must be used in training classes. Again, different materials probably will be required for court and law office staff.

In any automated process, quality control also must be an issue. The court should extend audit functions for financial and case management activities to cover document management systems, as well. This auditing will help identify needs and weaknesses in the system and in the training program.

Startup

As with case management systems, courts must deal with many problems while in transition from one system to another. They must prepare for concurrent implementation

of new technology and procedural changes. Normally, a period of parallel operation is required with new technology, which can double the workload of staff. There is the problem of receiving documents electronically for cases already containing paper pleadings. There are parallel paper and electronic paths that will make locating information slower. There are the frustrations of a learning curve that may make the new technology seem overwhelming to some users at first. There also may be issues of data conversion in the case management system.

There are ways to solve all of these problems. It is important that these plans be made months, rather than days, before system implementation.

A final issue related to startup is system evaluation. From the first day of operation, it is necessary to assess response time and other system performance issues. Problems should be noted, and plans made in advance for correcting them. As time goes on, project staff should look back to the original goals and objectives for the system and determine how much progress has been made.

Operation

New work is generated whenever technology is implemented. Production activities that may accompany electronic filing include running activity reports against transaction logs to profile system use and manage billing processes. Other production activities could include procedures relating to electronic service of process, verifying data supplied to the case management system, etc.

Problem management is another operations activity that requires attention. If a successful help desk has been established to support the case management system, then additional training for staff and the development of procedures for troubleshooting

problems may be all that is required. Users will require immediate assistance when they encounter problems.

System backup of the document database, transaction logs and other records also must be performed. File and disk reorganization and defragmentation, all of which must be done on a regular basis and require a block of time, must be completed, as well. These procedures should be nearly identical to those developed for case management database resources.

It is important to monitor system performance, particularly as the volume of documents on file increases and as the number of users grows. System monitoring software tools can help identify potential bottlenecks in sufficient time to prevent them from becoming noticeable to users.

A final operational area that requires attention is system security. Transaction logs should be reviewed and operational procedures enforced to prevent unauthorized access and other security breaches. Again, it is essential to develop and implement these procedures before problems occur, not after.

Summary

While implementation of an electronic filing system is not beyond the capability of most courts, it is a complex activity. If court leaders plan carefully, most of the bumps in the road should be relatively small and manageable.

Chapter 9: Summary

Electronic filing is a revolutionary approach to conducting court business that will significantly change the way courts work. Electronic filing combines existing and new technology to bring cost savings and efficiency to many court processes. When all case information is available as searchable text, it will be possible to integrate it with databases of legal precedent, courtroom testimony and evidence in its electronic form. This will allow the creation of sophisticated decision support systems that will help courts administer swifter and more effective justice.

Documents, once read from beginning to end, will be prepared in layers accessible through hypertext links. Readers will *drill down* to view greater detail if they desire. Footnotes will link World Wide Web documents stored all over the world. Electronic filing will allow court leaders to revolutionize the way documents are processed in the court.

Computerization of court information began this revolution, which was followed by the introduction of the personal computer. The PC did two things: it extended the use of this tool to areas not previously considered for automation, and it allowed the separate areas of court technology development—case data, office automation, records, legal information, evidence, and testimony—to begin to merge. Of the three stages of evolution of technology, the use of electronic documents might prove the most significant.

In the short term, there are many benefits gained with electronic filing. Most costs associated with paper handling and storage are eliminated in addition to redundant data entry at the courts. Case materials are readily accessible and protected from loss and

destruction. Court employees who work with records will be more productive as paper handling is eliminated, and they will be able to redirect their efforts to other court administration functions. Attorneys will save time and money transporting materials to the courthouse. In addition, they will have greater access to court materials stored in electronic format. Finally, document processing will be easier to manage than today's paper system, providing greater productivity and effectiveness in the court's work.

As this guidebook explains, there are many important factors and issues that must be considered and understood in order to successfully implement electronic filing in the courts. Court administrators must understand the many implications of changing existing court processes. Throughout the process of gaining funding and political support, adopting new court rules, installing new technology, and redesigning the everyday workflow of the courts, those involved in the implementation of electronic filing must be dedicated to the electronic filing revolution.

By way of advice to court leaders, don't be overwhelmed or discouraged by potential challenges related to modernizing today's courts. These first steps will provide tremendous benefits that in turn will create momentum for future progress. It is possible to learn from early pioneers with electricity. They did not foresee the development of the computer as a consequence of their work. In the same way, the effect of electronic document processing on the nature of future decision support systems and court case processing techniques is unclear. We do not know what shape progress will take, but we know it will occur.

Just because progress is inevitable, it doesn't mean it will be easy or that we won't make mistakes. Instead, we will learn more about our destination as we approach it. Good luck on the journey.

Appendices

Appendix A: Article on Hampshire E-Mail Project

SCL Electronic Magazine
Oct/Nov 96 Volume 7 Issue 4

Hampshire E-Mail Project

BY DAVID GODSON

David Godson is Chief Information and Research Officer with Hampshire Probation Service and Chair of the project's Local Management Group.

The complexity and diversity of paper-based transactions involving memorandums, letters, various forms and documents within the individual organisations which comprise the criminal justice system is all too apparent to anyone working in these organisations. Partly a matter of statutory requirements and national standards, what can be seen is also very much the result of custom and practice developed over many years. It is not surprising therefore that different agencies often approach similar administrative tasks in widely different ways. A good example is the codification of offence categories which can be seen to differ widely across the agencies involved. As this project has shown, these differences are placed in sharp focus where agencies are required to conduct computerised transactions in a way that will allow the 'seamless' exchange of information. I believe the project can teach us many valuable lessons and point to a future in which criminal justice agencies are able to work more closely together.

The increasing use of an 'open systems' approach to the information technology used by criminal justice agencies will undoubtedly facilitate easier computerised communications as systems develop. However, ensuring that the different administrative procedures are able to work more easily in harness now is a task not to be underestimated and certainly one requiring more focused consideration. My experience as chair of the Local Management Group steering the Hampshire e-mail project is that, while the challenge is clearly a formidable one, the benefits both in increased efficiency and effectiveness and a greater mutual understanding of how the different agencies operate are there for all to see.

The Pilot Phase

The Hampshire project follows on from a successful pilot involving all criminal justice agencies in Southampton undertaken during the latter part of 1995 and early 1996. A parallel pilot was also set up in Suffolk at the same time. The objective of both pilots was a relatively modest one - seeking to replace some existing paper-based transactions between the agencies with electronic exchanges using e-mail in order to demonstrate that new technology could make a significant contribution to the efficient and effective flow of information.

In many respects much of the work needed to establish the project's viability was achieved during the pilot phase. This included finding the relevant technical solutions, establishing how the project would be

managed and putting appropriate procedures in place to support its continued operation. The time and effort put in by the staff and consultants attached to the Home Office CCCJS Unit at this pilot stage combined well alongside the essential contribution made by the staff in the local agencies. That's not to say this partnership did not have its occasional disagreements along the way, suffice to say at the completion of the pilot phase we have now achieved a successful transition to the local management of the project in a way that ensures its continued success. While the criminal justice agencies in Hampshire had already started exploring the possible benefits of inter-agency co-operation in the use of technology, the decision to choose Southampton as a pilot site for the national e-mail element of the CCCJS project meant significant progress was possible in a timescale that would not otherwise have been achievable.

Organisational Structure

Under the overall management of the Home Office CCCJS Unit, the agencies involved in the initial pilot were the police, the CPS, the probation service, magistrates' courts, Crown Courts and the prison service. More recently we have seen the welcome addition of solicitors and barristers. From the outset it was important to establish well defined working groups with appropriate representation from each of the participating agencies both locally an centrally, including the Home Office. First it was essential to ensure that the computer systems were linked in a way that was reliable, secure and able to deliver measurable improvements over existing paper-based methods. The task of establishing a solid technical infrastructure as the platform from which this could be achieved was undertaken by a local Technical Group supported by Home Office consultants. Using X400 'gateway' technology a 'network' was quickly established and successfully tested.

In many ways the engine room of the project continues to be the local User Group delegated with the task of identifying suitable information flows; it is here that a shared understanding of each others' business processes is explored and analysed. To ensure that each agency exchanges information to an agreed set of procedures, so-called 'interchange' agreements have been established covering each flow. These agreements specify how the flows are to be established and maintained, down to such details as times for the transmission of information. As a result of these agreements, each signed by the relevant authorised person responsible, any difficulties related to individual flows can be quickly resolved. The potential benefits from computerisation of each flow are assessed by using the technique of 'before and after' studies. These were concerned not simply with a 'time and motion' evaluation of the flows, but of the views of those staff required to operate the new procedures. The involvement of front-line staff in the development of the flows has been crucial to the successes achieved. Where it has not proved possible to establish particular flows, their contribution has been essential to understanding why.

Benefits Arising

Turning to the benefits that have been achieved, a good example involving my own agency is the use of e-mail at the arrest stage where a person might be charged and held overnight to appear in court the next day. If the duty solicitor is unsuccessful in obtaining bail, resulting in a remand in custody to the local prison, the use of e-mail by the prison and probation services prior to a second appearance illustrates the gains possible.

First the court-based bail information officer will e-mail all the relevant information concerning the police cell interview prior to the remand in custody to the prison direct from the court building. Interviews will take place in the prison to establish whether fresh information relevant to the possible granting of bail can be identified. Using standard pro-formas this information will be simultaneously transmitted to both the court bail information officer and the CPS. Where practices are part of the project this information can also be sent direct to the relevant solicitor. In a process that is required to be completed as speedily as possible, the extra time gained can be focused on completing a thorough investigation of the defendant's situation and providing a better service to all concerned, including the courts.

A similar example can be seen in relation to the transmission of pre-sentence reports to the Crown Court. Pressures to produce reports within tight timescales have been eased, with the allied advantage of being able to put reports before judges quicker than would normally be the case. Again where agreed these reports can be made available to the defense that much sooner.

These are only two examples involving the probation service, prisons, CPS, Crown Court and solicitors and barristers and illustrate what has been achieved in a very short space of time. There are numerous other examples involving flows between the various agencies as wide ranging as charge sheets sent from police to magistrates' courts; lists of committals from magistrates' courts to Crown Courts and probation; proposed discontinuance from CPS to police; leave to appeal date from Crown Court to magistrates' court, police and participating solicitors and barristers. The list is indeed a formidable one and growing all the time, amply illustrating the confidence that all the participating agencies have in the project. Importantly the project is beginning to identify a range of flows that solicitors and barristers are able to take part in, bringing them much closer to the day-to-day administration of the criminal justice system.

The smoothing of established boundaries between all the agencies can be seen as an important by-product of the whole process. Speaking at the formal launch of the project attended by Home Office Minister David Maclean, Jane Beesley of the Hampshire Police's Administration of Justice Department observed, when talking about a number of exchanges between the police and CPS, that 'It was a revelation to me to find out that the problems we inherit from the CPS are not actually devised by them to cause additional work for the police, but are actually caused by the pressures placed on them by the criminal justice system, some of which we could go some way to help resolve.'

This simple but important observation raises an issue that I believe is central to the success of this or any other project seeking to improve the way criminal justice agencies work together. In our case it is not simply a matter of utilising new technology, or finding better, more efficient ways of exchanging information, it is essentially about understanding the culture and practices uderpinning each of our organisations and finding ways to bring about change that respects the differences but builds on the similarities in a way that is positive and outward looking. In the time that I have been involved with this project, the enthusiasm with which everyone has contributed, not only to achieving more efficient and effective exchanges of essential information between the agencies but also to a much better understanding of how individual agencies operate, has left an indelible impression on me. As the project, now devolved and managed locally, looks forward to a period of consolidation to be followed by further expansion, I really do see a period of continuing success that will bring lasting benefit to all those involved. I very much look forward to the day when the benefits we are seeing in Hampshire become part of the operation of the criminal justice system nationally.

Appendix B: Rule Summary by Category

Digital Signature

State: California

Court	Reference	Date
LA Superior Court	Local Rule 18	3/ 1/96
Electronic Filing and Service		
Santa Clara Superior Court	Local Rule 1.7	1/ 1/96
Electronic Filing and Service; definitions; service provider; certification authority; digital signature; standards; issuance of summons; original document; facsimile service to computer		
Statute	Government Code 16.5	1/ 1/98
Digital Signatures; signatures allowed; optional; exemptions; definition		

State: Florida

Court	Reference	Date
Statute	10-117.20	5/30/97
Electronic Notarization; procedure for electronic notarization (using digital signature)		
Statute	19-282.70-75	5/25/96
Electronic Signatures; definitions; certification; voluntary licensure		
Statute	32-471.025	5/30/97
Seals; unlawful to stamp, seal, or digitally sign with expired, revoked, or suspended certificate		
Statute	32-472.025	5/30/97
Seals; unlawful to stamp, seal, or digitally sign with expired, revoked, or suspended certificate		

State: Georgia

Court	Reference	Date
Statute	50-29-12	4/22/97
Information Technology Policy Act; electronic commerce encouraged; pilot projects, such as digital signature and public key infrastructure encouraged		

State: Illinois

Court	Reference	Date
Statute	15-405/14.01	6/27/97
Digital Signature Act; allowed; optional; definition		

State: Indiana

Court	Reference	Date
Statute	5-24-1-1 through 5-24-3-4	1/ 1/98

Electronic Digital Signature Act; definitions;effectiveness; rulemaking authority; procedural standards

State: Kansas

Court	Reference	Date
State	Code of Civil Procedure 26-60-2616	7/ 1/97

Digital Signature; definitions; approved substitute

State: Minnesota

Court	Reference	Date
Statute	Trade Regulations 325K.01-325k.26	1/ 1/98

Electronic Authentication Act

State: Mississippi

Court	Reference	Date
Statute	25-63-1 through 25-63-11	7/ 1/98

Digital Signature Act

State: New Hampshire

Court	Reference	Date
Statute	27B 294-D	7/ 1/97

New Hampshire Digital Signature Act; avoid direct involvement as certification authority or repository

State: New Mexico

Court	Reference	Date
Statute	14-15-1 through 14-15-6	7/ 1/97

Electronic Authentication Act

State: Ohio

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	3/10/97

Documents may be filed, signed, or verified by electronic means consistent with technical standards of the Judicial Conference once such standards are published and approved by this court.

State: Oregon

Court	Reference	Date
Statute	192.825 through 192.855	7/ 1/97

Electronic Signature Act

State: Rhode Island

Court	Reference	Date
Statute	42-127-1 through 42-127-6	1/ 1/98

Electronic Signatures Act

State: Texas

Court	Reference	Date
Statute	1-2A-108	9/ 1/97

Digital signature; definitions; misuse subject to criminal laws

Statute	10B-2054.060	9/ 1/97

Digital signature; allowed; misuse subject to criminal law; definitions

Statute	4A-403.027	6/19/97

Digital signatures; comptroller may establish procedures for digital signatures

Statute	6A-201.931 through 6A-201.933	9/ 1/97

Electronic issuance of licenses; digital signature defined; digital signature allowed on application

Statute	7E-623.074	9/ 1/97

Transportation department may authorize digital signature on electronic application

State: Utah

Court	Reference	Date
Statute	46-1-1 through 46-2-9	7/ 1/97

Notaries Public Reform Act

Statute	46-3-101 through 46-3-504	5/ 1/95

Utah Digital Signature Act

State: Virginia

Court	Reference	Date
Statute	2.1-563.31	1/ 1/98
Council on Information Management; duties listed; digital signature regulations		
Statute	59.1-467 through 59.1-469	1/ 1/98
Digital signatures; definitions; authentication; state agencies use of digital signatures authorized		

State: Washington

Court	Reference	Date
Statute	19.34.010 through 19.34.503	1/ 1/96
Washington Electronic Authentication Act		

Electronic Devices

State: California

Court	Reference	Date
San Diego Municipal Court	Local Rule 38	7/ 1/95
Cellular phones, laptop computers prohibited in jury deliberation room, pager at discretion of judge		

Electronic Filing

State: Arizona

Court	Reference	Date
Statute	12-113	1/ 1/98
Disposition of fees paid for electronic filing and access		
Statute	12-119.02	1/ 1/98
Supreme court electronic filing and access; fee; filing and access by rule; not more than $100 per year subscription, $2 per minute		
Statute	12-120.31	1/ 1/98
Electronic filing and access; fees and costs; distribution; court retains percentage of collections		
Statute	12-284.02	1/ 1/98
Electronic filing and access; fee; superior court electronic filing and access by supreme court rule fees same as appellate courts		
Statute	22-284	1/ 1/98
Electronic filing and access; fee; dedicated fund; superior court may provide for electronic filing of documents and access pursuant to supreme court rules; fees same as appellate courts		
Statute	22-408	1/ 1/98
Electronic filing and access; fees; presiding judge of superior court may provide for electronic filing and access for municipal courts pursuant to supreme court rules, after consultation with city		

State: California

Court	Reference	Date
LA Superior Court	Local Rule 18	3/ 1/96

Electronic Filing and Service; requirements for electronically submitted documents; enhanced service contractual requirements; issuance of summons; visible rendition; facsimile transfer; definitions

Orange County Superior Court	Local Rule 329	1/ 1/98

Electronic filing pilot program; pilot program authorized under CA Rules of Court 982.9, 1033

Santa Clara Superior Court	Local Rule 1.1.11	1/ 1/96

Documents served electronically or non-electronically on parties shall be filed in the same manner to the court.

Santa Clara Superior Court	Local Rule 1.5	1/ 1/96

Formatting of documents not filed electronically

Santa Clara Superior Court	Local Rule 1.7	1/ 1/96

Electronic Filing and Service; definitions; service provider; certification authority; digital signature; standards; issuance of summons; original document; facsimile service to computer

State: Delaware

Court	Reference	Date
Common Pleas Civil	Rule 5	10/15/97

Service and Filing of Pleadings and Other Papers

Superior Court	Interim Rule 79.1	7/ 1/91

Complex Litigation Automated Docket; cases assigned; fees; orders; passwords; service

State: Florida

Court	Reference	Date
State	Rules of Judicial Administration 2	1/ 1/98

Electronic Filing in State Court System; definition; application; documents affected; service; transmission difficulties; administration; followup filing if no signature; form of signature

State: Georgia

Court	Reference	Date
Statute	10-12-3 to 10-12-5	7/ 1/97

Electronic records and signatures; recently updated; check updates

State: Hawaii

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	10/30/97
Clerk may promulgate additional rules for papers as necessary		

State: Illinois

Court	Reference	Date
1st Circuit	Rule 1.14	7/ 1/95
Facsimile and electronic filing are not authorized		
US District Court SD	Rule 4	3/24/94
Facsimile and electronic filing are not authorized		

State: Iowa

Court	Reference	Date
Statute	16-3-907.8A	7/ 1/97
Electronic filing authorized for video probation hearings		

State: Kentucky

Court	Reference	Date
US Bankruptcy Court ED & WD	Local Bankruptcy Rule 5.7	8/ 1/97
Electronic filing permitted when authorized; procedure-payment account; procedures for transmitting; maintain original; filed when received; electronic version equals paper; electronic acknowledgement.		
US Bankruptcy Court WD	Local Bankruptcy Rule 49.3	8/ 1/97
Electronic filing permitted when authorized; procedure-payment account; procedures for transmitting; maintain original; filed when received; electronic version equals paper; electronic acknowledgement.		

State: Maryland

Court	Reference	Date
State	Rules of Procedure 1-322	1/ 1/97
Filing of Pleadings and Other Papers; no electronic filing except under Rule 16-307		
State	Rules of Procedure Court Admin 16-307	1/ 1/95
Electronic Filing of Pleadings and Papers; submission of EF pilot plan; state court administrator review; approval; duration; evaluation; extension; public availability of plan		

State: Michigan

Court	Reference	Date
District Court	4.100	9/ 2/97
Citation may be filed electronically or on paper		
District Court	6.600	9/ 2/97
Contested case may not be heard without signed paper citation. Electronic citations dismissed with prejudice if contested.		
District Court	8.125	9/ 2/97
Electronic citation containing all information that would be on a paper version, including full name of official who issued it, is deemed to be signed.		

State: Mississippi

Court	Reference	Date
Statute	11-7-189	7/ 1/97
Judgement roll may be kept on computer		
Statute	21-23-11	7/ 1/95
Clerk of the municipal court; dockets and minute orders		
Statute	89-5-25	5/28/62
Records filed or stored electronically may be in addition to, or in lieu of, the physical record on paper		
Statute	9-1-51 through 9-1-57	4/ 8/97
Electronic filing and storage of court documents		
Statute	9-21-3	4/ 8/97
Duties of Administrative Office of the Courts; promulgate standards, rules, regulations for computer electronic filing, and electronic storage		
Statute	9-21-51	4/ 8/97
Promulgation of rules for electronic filing and storage; AOC to study and report on state of automation and electronic records; compliance with AOC rules		
Statute	9-21-9	4/ 8/97
Duties and authority of AOC director; promulgate standards, rules, and regulations for computers, electronic filing, and electronic storage		
Statute	9-5-135 through 9-5-139	3/25/94
Duties of clerk; may elect to use electronic means		
Statute	9-5-157 through 9-5-173	3/25/94
Other duties of clerk		
Statute	9-5-201 through 9-5-215	7/ 1/94
General docket; docket and other records may be kept on computer, following AOC regulations		

Statute	9-7-127 through 9-7-41	3/25/94

Jury fee book; may be kept by electronic filing or storage or both

Statute	9-7-171 through 9-7-179	7/ 1/94

General docket; docket and other records may be kept on computer, following AOC regulations

State: Missouri

Court	Reference	Date
Circuit Court	Local Rule 4.1	9/13/93

All traffic tickets filed electronically by prosecuting attorney entering the data therefrom into the court computer system.

US District Court ED	Rule 13.01	1/ 1/96

Probation and Pretrial Services Records; court may require electronic filing and storage of original probation and pretrial services reports, including objections

State: Montana

Court	Reference	Date
Statute	3-1-114	11/ 5/96

Definitions; electronic filing; electronic storage of records

Statute	3-1-115	11/ 5/96

Electronic filing and storage of documents--supreme court rules; electronic documents substitute for paper; rule must address timely availability, use of paper, standards, retention, security

Statute	3-10-501	11/ 5/96

Contents of Justice's court docket; may keep court documents by electronic filing or storage or both

Statute	3-10-503	11/ 5/96

Index to Justice's court docket; may keep court documents by electronic filing or storage or both

Statute	3-10-511	11/ 5/96

Justice court records delivered to successor; electronically filed or stored documents delivered to successor

Statute	3-10-512	7/ 1/95

Upon death or removal of justice, paper or electronically filed documents shall be deposited with the clerk

Statute	3-11-206	11/ 5/96

City court records may be kept by electronic filing or storage or both

Statute	3-2-402	11/ 5/96

Duties of supreme court clerk; may keep court documents by electronic filing or storage or both

Statute	3-5-501	11/ 5/96

District court clerk duties; may keep court documents by electronic filing or storage or both

Statute	3-6-302	11/ 5/96

Municipal court records; may keep court documents by electronic filing or storage or both

State: Nebraska

Court	Reference	Date
Workers Compensation Court	Rule 29	7/ 1/97

First report of injury or illness may be filed in writing or by electronic means, if approved by compensation court. Facsimile copies are not accepted.

State: Nevada

Court	Reference	Date
Statute	171.103	10/ 1/97

Electronic filing of complaint; signature required; time stamp required

Statute	173.049	10/ 1/97

Clerk may accept information filed electronically; procedure; service; signature required; time stamp required

Statute	432B.515	10/ 1/97

Electronic filing of certain petitions and reports; signature required

Statute	62.206	10/ 1/97

Electronic filing of certain documents; petition from district attorney; others; must contain image of signature

State: New Hampshire

Court	Reference	Date
Statute	421-B:28-b	6/ 9/94

Electronic filings; admissible in evidence in accordance with rules of the supreme court

State: New Mexico

Court	Reference	Date
Children's Court	Children's Court Rules and Forms 10-103	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

District Court	Rules of Civil Procedure 1-011	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

District Court	Rules of Civil Procedure 2-301	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

District Court	Rules of Civil Procedure 5-206	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

Magistrate Court	Magistrate Court Rules 6-210	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law. Rules for facsimile filing.

Metropolitan Court	Metropolitan Court Rules 7-210	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law. Rules for facsimile filing.

Municipal Court	Municipal Court Rules 8-209	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law. Rules for facsimile filing.

State	Rules of Appellate Procedure 12-302	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

Statute	14-3-15.2	6/16/95

Electronic authentication; substitution for signature; must meet standards promulgated by commission

US Bankruptcy Court	Local Bankruptcy Rule 5005-4	10/ 1/96

Facsimile Filings; no prior judicial authorization required for facsimilie filing; electronic transmission; court to establish guidelines

US District Court	Administrative Order 97-26	1/ 1/96

ID and password for signature; registration procedures; electronic file stamp; attorneys retain originals; notices in electronic mailbox.

US District Court	Local Civil Rules 5	1/ 1/96

Rules for facsimile filing; fees paid; filing, service, and notice by electronic transmission

State: New York

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 9021-1	7/ 1/97

Entry of orders, judgements, and decrees; clerk shall enter all in electronic filing system, which constitutes entry of order.

US Bankruptcy Court ED	9011-1	7/ 1/97

Attorneys; duties; control of password

US Bankruptcy Court ND	Local Bankruptcy Rule 904.2	12/ 1/96

Filing Generally; no papers filed electronically or by facsimile are considered filed; originals must be submitted by mail

US Bankruptcy Court SD	Local Bankruptcy Rule 9011-1	12/ 1/96

Signing of Papers; electronic filing password only used by attorney and authorized members and employees of the attorney's firm

US Bankruptcy Court SD	Local Bankruptcy Rule 9021-1	12/ 1/96

Entry of Orders, Judgements, and Decrees; all orders, judgments, and decrees entered into electronic filing system are considered docketed and entered

US Bankruptcy Court SD	Local Bankruptcy Rule Appendix G	7/20/94

Pilot Program for CLAD General Order 111-134; cases assigned to CLAD; exhibit establishes administrative procedures; passwords; administrative procedures; court designates cases; forms

State: Ohio

Court	Reference	Date
Fifth Appellate District	Rule 2	5/ 1/97
Only motions may be filed electronically or by facsimile. No other pleadings allowed.		
State	Rules of Civil Procedure	7/ 1/94
Local rules may provide for electronic filing; signature assumed authentic; if shown otherwise, pleadings or papers shall be stricken.		
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	3/10/97
Documents may be filed, signed, or verified by electronic means consistent with technical standards of the Judicial Conference once such standards are published and approved by this court.		

State: Oklahoma

Court	Reference	Date
Statute	20-40-3004	7/ 1/97
Electronic filing of documents; in supreme court and district courts; rules promulgated by AOC, approved by supreme court		

State: Oregon

Court	Reference	Date
Statute	14-153.770	12/31/95
Electronic filing of complaint; signature not required as on citation; court to establish rules; verification; public access to documents		
Tax Court Regular Division	Rule 7	1/ 1/97
Summons Generally; telegraphic transmission; summons and complaint may be transmitted electronically as provided in rule 8 D		

State: Pennsylvania

Court	Reference	Date
State	Rules of Criminal Procedure 95	1/ 1/97
Proceedings in Summary Cases Charging Parking Violations; parking citation may be filed electronically		
State	Rules of Criminal Procedure 61	1/ 1/97
Procedures Following Filing of Citation--Issuance of Summons; if citation filed electronically, summons also shall include listed data elements		
US Bankruptcy Court MD	Bankruptcy Practice Order Northern Tier	12/ 1/96
Electronic filing authorized under F.R.B.P. 5005 (a) (2).		
US District Court ED	Clerk's Office Procedural Handbook	5/ 1/97
Electronic filing		

State: Rhode Island

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5081-1	11/ 1/97

Signatures; judges; use of endorsement stamp or electronic signature by clerk authorized; equals original signature.

State: Tennessee

Court	Reference	Date
Statute	16-1-115	6/13/97

Electronic signatures have same force and effect as written signatures

State: Texas

Court	Reference	Date
State	Rules of Appellate Procedure 9	9/ 1/97

Court of appeals by local rule may permit documents to be filed, signed, or verified electronically if consistent with Supreme Court technology standards.

Statute	2D-51.801 through 2D-51.807	9/ 1/87

Electronic filing of certain documents

Statute	2F-77.031	9/ 1/97

Judicial committee on information technology; standards; statewide automation; security; pilot programs

Statute	6C-205.005	9/ 1/89

Electronic storage of records; chapter not in conflict with electronic filing in district and county courts

US Bankruptcy Court ND	Local Bankruptcy Rule 5005.4	4/15/97

Clerk authorized to implement electronic filing and noticing subject to approval by the court

US District Court ED	Local Rule CR-49	10/27/97

Electronic filing not allowed unless authorized by clerk;document filed and served when received

US District Court ED	Local Rule CV-5	10/27/97

Electronic filing not allowed unless authorized by clerk;document filed and served when received

US District Court WD	Local Rule 9013	1/ 1/94

Clerk may implement electronic filing with approval of court

US District Court WD	Operating Procedures	5/ 1/94

Clerk may implement electronic filing with approval of court

US District Court WD	Operating Procedures Clerks Office	2/ 1/97

Facsimile filings not accepted. Electronic filings accepted if attorney is registered ELF user

State: Utah

Court	Reference	Date
Code of Judicial Adminstration	Appendix G	4/15/95
Child support worksheets; provision for electronic filing		

State: Virginia

Court	Reference	Date
Statute	17-2-3.01	7/ 1/98
Electronic filing with clerk; expired 7/1/98; was it renewed?		
Statute	17-83.1	12/31/97
Electronic filing with clerk; definition; authorized; completion of filing; transmission and distribution of data; acknowledgement; encoding; media; signature required		

State: Washington

Court	Reference	Date
State	Rule 7	3/19/93
Local Rules--Filing and Effective Date; administrator for the courts establishes specifications for court to file its local rules electronically		
Statute	19.34.900	7/27/97
Other references to Washington Electronic Authentication Act		

FAX Filing

State: California

Court	Reference	Date
Santa Clara Superior Court	Local Rule 1.7	1/ 1/95
Electronic Filing and Service; definitions; service provider; certification authority; digital signature; standards; issuance of summons; original document; facsimile service to computer		

State: Delaware

Court	Reference	Date
Common Pleas Civil	Rule 5	10/15/97
Service and Filing of Pleadings and Other Papers		

State: Illinois

Court	Reference	Date
1st Circuit	Rule 1.14	7/ 1/95
Facsimile and electronic filing are not authorized		
US District Court SD	Rule 4	3/24/94
Facsimile and electronic filing are not authorized		

State: Nebraska

Court	Reference	Date
US Bankruptcy Court	Local Bankrutcy Rule 5005-4	4/15/97
Fax filings not accepted except when authorized in advance. Rules for fax filings.		

State: New Hampshire

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 9004-1	1/ 1/97
Electronically transmitted facsimiles or other substitute copies of documents shall not be construed as signed original pleading documents.		

State: New Mexico

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	10/ 1/96
Facsimile Filings; no prior judicial authorization required for facsimilie filing; electronic transmission; court to establish guidelines		

State: New York

Court	Reference	Date
US Bankruptcy Court ND	Local Bankruptcy Rule 904.2	12/ 1/96
Filing Generally; no papers filed electronically or by facsimile are considered filed; originals must be submitted by mail		

State: Ohio

Court	Reference	Date
Fifth Appellate District	Rule 2	5/ 1/97
Only motions may be filed electronically or by facsimile. No other pleadings allowed.		
Juvenile Court	Rules of Juvenile Procedure 8	7/ 1/96
Filing by Facsimile Transmission; procedure; equipment standards; historical and statutory notes		

State: Oregon

Court	Reference	Date
Tax Court Regular Division	Rule 8	1/ 1/90
Process; telegraphic transmission of writ, order, or paper for service		

State: Tennessee

Court	Reference	Date
US Bankruptcy Court ED	Rule 5005-4	4/15/97
Papers may only be filed by facsimile with express permission of court. Original shall be properly substituted.		

State: Texas

Court	Reference	Date
US District Court WD	Operating Procedures Clerks Office	2/ 1/97
Facsimile filings not accepted. Electronic filings accepted if attorney is registered ELF user		

Information in Electronic Format

State: California

Court	Reference	Date
Santa Clara Superior Court	Local Rule 3.1	1/ 1/95
Child and Spousal Support; pleadings; computer analysis of support submitted		

Appendix C: Rule Summary by State

Arizona

Electronic Filing

Court	Reference	Date
Statute	12-113	1/ 1/98
Disposition of fees paid for electronic filing and access		
Statute	12-119.02	1/ 1/98
Supreme court electronic filing and access; fee; filing and access by rule; not more than $100 per year subscription, $2 per minute		
Statute	12-120.31	1/ 1/98
Electronic filing and access; fees and costs; distribution; court retains percentage of collections		
Statute	12-284.02	1/ 1/98
Electronic filing and access; fee; superior court electronic filing and access by supreme court rule fees same as appellate courts		
Statute	22-284	1/ 1/98
Electronic filing and access; fee; dedicated fund; superior court may provide for electronic filing of documents and access pursuant to supreme court rules; fees same as appellate courts		
Statute	22-408	1/ 1/98
Electronic filing and access; fees; presiding judge of superior court may provide for electronic filing and access for municipal courts pursuant to supreme court rules, after consultation with city		

California

Digital Signature

Court	Reference	Date
LA Superior Court	Local Rule 18	3/ 1/96
Electronic Filing and Service		
Santa Clara Superior Court	Local Rule 1.7	1/ 1/96
Electronic Filing and Service; definitions; service provider; certification authority; digital signature; standards; issuance of summons; original document; facsimile service to computer		
Statute	Government Code 16.5	1/ 1/98
Digital Signatures; signatures allowed; optional; exemptions; definition		

Electronic Devices

Court	Reference	Date
San Diego Municipal Court	Local Rule 38	7/ 1/95

Cellular phones, laptop computers prohibited in jury deliberation room, pager at discretion of judge

Electronic Filing

Court	Reference	Date
LA Superior Court	Local Rule 18	3/ 1/96

Electronic Filing and Service; requirements for electronically submitted documents; enhanced service contractual requirements; issuance of summons; visible rendition; facsimile transfer; definitions

Orange County Superior Court	Local Rule 329	1/ 1/98

Electronic filing pilot program; pilot program authorized under CA Rules of Court 982.9, 1033

Santa Clara Superior Court	Local Rule 1.1.11	1/ 1/96

Documents served electronically or non-electronically on parties shall be filed in the same manner to the court.

Santa Clara Superior Court	Local Rule 1.5	1/ 1/96

Formatting of documents not filed electronically

Santa Clara Superior Court	Local Rule 1.7	1/ 1/96

Electronic Filing and Service; definitions; service provider; certification authority; digital signature; standards; issuance of summons; original document; facsimile service to computer

FAX Filing

Court	Reference	Date
Santa Clara Superior Court	Local Rule 1.7	1/ 1/95

Electronic Filing and Service; definitions; service provider; certification authority; digital signature; standards; issuance of summons; original document; facsimile service to computer

Information in Electronic Format

Court	Reference	Date
Santa Clara Superior Court	Local Rule 3.1	1/ 1/95

Child and Spousal Support; pleadings; computer analysis of support submitted

Delaware

Electronic Filing

Court	Reference	Date
Common Pleas Civil	Rule 5	10/15/97

Service and Filing of Pleadings and Other Papers

Superior Court	Interim Rule 79.1	7/ 1/91

Complex Litigation Automated Docket; cases assigned; fees; orders; passwords; service

FAX Filing

Court	Reference	Date
Common Pleas Civil	Rule 5	10/15/97

Service and Filing of Pleadings and Other Papers

Florida

Digital Signature

Court	Reference	Date
Statute	10-117.20	5/30/97

Electronic Notarization; procedure for electronic notarization (using digital signature)

Statute	19-282.70-75	5/25/96

Electronic Signatures; definitions; certification; voluntary licensure

Statute	32-471.025	5/30/97

Seals; unlawful to stamp, seal, or digitally sign with expired, revoked, or suspended certificate

Statute	32-472.025	5/30/97

Seals; unlawful to stamp, seal, or digitally sign with expired, revoked, or suspended certificate

Electronic Filing

Court	Reference	Date
State	Rules of Judicial Administration 2	1/ 1/98

Electronic Filing in State Court System; definition; application; documents affected; service; transmission difficulties; administration; followup filing if no signature; form of signature

Georgia

Digital Signature

Court	Reference	Date
Statute	50-29-12	4/22/97

Information Technology Policy Act; electronic commerce encouraged; pilot projects, such as digital signature and public key infrastructure encouraged

Electronic Filing

Court	Reference	Date
Statute	10-12-3 to 10-12-5	7/ 1/97

Electronic records and signatures; recently updated; check updates

Hawaii

Electronic Filing

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	10/30/97
Clerk may promulgate additional rules for papers as necessary		

Iowa

Electronic Filing

Court	Reference	Date
Statute	16-3-907.8A	7/ 1/97
Electronic filing authorized for video probation hearings		

Illinois

Digital Signature

Court	Reference	Date
Statute	15-405/14.01	6/27/97
Digital Signature Act; allowed; optional; definition		

Electronic Filing

Court	Reference	Date
1st Circuit	Rule 1.14	7/ 1/95
Facsimile and electronic filing are not authorized		
US District Court SD	Rule 4	3/24/94
Facsimile and electronic filing are not authorized		

FAX Filing

Court	Reference	Date
1st Circuit	Rule 1.14	7/ 1/95
Facsimile and electronic filing are not authorized		
US District Court SD	Rule 4	3/24/94
Facsimile and electronic filing are not authorized		

Indiana

Digital Signature

Court	Reference	Date
Statute	5-24-1-1 through 5-24-3-4	1/ 1/98
Electronic Digital Signature Act; definitions;effectiveness; rulemaking authority; procedural standards		

Kansas

Digital Signature

Court	Reference	Date
State	Code of Civil Procedure 26-60-2616	7/ 1/97
Digital Signature; definitions; approved substitute		

Kentucky

Electronic Filing

Court	Reference	Date
US Bankruptcy Court ED & WD	Local Bankruptcy Rule 5.7	8/ 1/97
Electronic filing permitted when authorized; procedure-payment account; procedures for transmitting; maintain original; filed when received; electronic version equals paper; electronic acknowledgement.		
US Bankruptcy Court WD	Local Bankruptcy Rule 49.3	8/ 1/97
Electronic filing permitted when authorized; procedure-payment account; procedures for transmitting; maintain original; filed when received; electronic version equals paper; electronic acknowledgement.		

Maryland

Electronic Filing

Court	Reference	Date
State	Rules of Procedure 1-322	1/ 1/97
Filing of Pleadings and Other Papers; no electronic filing except under Rule 16-307		
State	Rules of Procedure Court Admin 16-307	1/ 1/95
Electronic Filing of Pleadings and Papers; submission of EF pilot plan; state court administrator review; approval; duration; evaluation; extension; public availability of plan		

Michigan

Electronic Filing

Court	Reference	Date
District Court	4.100	9/ 2/97
Citation may be filed electronically or on paper		
District Court	6.600	9/ 2/97
Contested case may not be heard without signed paper citation. Electronic citations dismissed with prejudice if contested.		
District Court	8.125	9/ 2/97
Electronic citation containing all information that would be on a paper version, including full name of official who issued it, is deemed to be signed.		

Minnesota

Digital Signature

Court	Reference	Date
Statute	Trade Regulations 325K.01-325k.26	1/ 1/98
Electronic Authentication Act		

Missouri

Electronic Filing

Court	Reference	Date
Circuit Court	Local Rule 4.1	9/13/93
All traffic tickets filed electronically by prosecuting attorney entering the data therefrom into the court computer system.		
US District Court ED	Rule 13.01	1/ 1/96
Probation and Pretrial Services Records; court may require electronic filing and storage of original probation and pretrial services reports, including objections		

Mississippi

Digital Signature

Court	Reference	Date
Statute	25-63-1 through 25-63-11	7/ 1/98
Digital Signature Act		

Electronic Filing

Court	Reference	Date
Statute	11-7-189	7/ 1/97
Judgement roll may be kept on computer		
Statute	21-23-11	7/ 1/95
Clerk of the municipal court; dockets and minute orders		
Statute	89-5-25	5/28/62
Records filed or stored electronically may be in addition to, or in lieu of, the physical record on paper		
Statute	9-1-51 through 9-1-57	4/ 8/97
Electronic filing and storage of court documents		
Statute	9-21-3	4/ 8/97
Duties of Administrative Office of the Courts; promulgate standards, rules, regulations for computer electronic filing, and electronic storage		
Statute	9-21-51	4/ 8/97
Promulgation of rules for electronic filing and storage; AOC to study and report on state of automation and electronic records; compliance with AOC rules		
Statute	9-21-9	4/ 8/97
Duties and authority of AOC director; promulgate standards, rules, and regulations for computers, electronic filing, and electronic storage		
Statute	9-5-135 through 9-5-139	3/25/94
Duties of clerk; may elect to use electronic means		
Statute	9-5-157 through 9-5-173	3/25/94
Other duties of clerk		
Statute	9-5-201 through 9-5-215	7/ 1/94
General docket; docket and other records may be kept on computer, following AOC regulations		
Statute	9-7-127 through 9-7-41	3/25/94
Jury fee book; may be kept by electronic filing or storage or both		
Statute	9-7-171 through 9-7-179	7/ 1/94
General docket; docket and other records may be kept on computer, following AOC regulations		

Montana

Electronic Filing

Court	Reference	Date
Statute	3-1-114	11/ 5/96
Definitions; electronic filing; electronic storage of records		

Statute	3-1-115	11/ 5/96

Electronic filing and storage of documents--supreme court rules; electronic documents substitute for paper; rule must address timely availability, use of paper, standards, retention, security

Statute	3-10-501	11/ 5/96

Contents of Justice's court docket; may keep court documents by electronic filing or storage or both

Statute	3-10-503	11/ 5/96

Index to Justice's court docket; may keep court documents by electronic filing or storage or both

Statute	3-10-511	11/ 5/96

Justice court records delivered to successor; electronically filed or stored documents delivered to successor

Statute	3-10-512	7/ 1/95

Upon death or removal of justice, paper or electronically filed documents shall be deposited with the clerk

Statute	3-11-206	11/ 5/96

City court records may be kept by electronic filing or storage or both

Statute	3-2-402	11/ 5/96

Duties of supreme court clerk; may keep court documents by electronic filing or storage or both

Statute	3-5-501	11/ 5/96

District court clerk duties; may keep court documents by electronic filing or storage or both

Statute	3-6-302	11/ 5/96

Municipal court records; may keep court documents by electronic filing or storage or both

Nebraska

Electronic Filing

Court	Reference	Date
Workers Compensation Court	Rule 29	7/ 1/97

First report of injury or illness may be filed in writing or by electronic means, if approved by compensation court. Facsimile copies are not accepted.

FAX Filing

Court	Reference	Date
US Bankruptcy Court	Local Bankrutcy Rule 5005-4	4/15/97

Fax filings not accepted except when authorized in advance. Rules for fax filings.

New Hampshire

Digital Signature

Court	Reference	Date
Statute	27B 294-D	7/ 1/97

New Hampshire Digital Signature Act; avoid direct involvement as certification authority or repository

Electronic Filing

Court	Reference	Date
Statute	421-B:28-b	6/ 9/94

Electronic filings; admissible in evidence in accordance with rules of the supreme court

FAX Filing

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 9004-1	1/ 1/97

Electronically transmitted facsimiles or other substitute copies of documents shall not be construed as signed original pleading documents.

New Mexico

Digital Signature

Court	Reference	Date
Statute	14-15-1 through 14-15-6	7/ 1/97

Electronic Authentication Act

Electronic Filing

Court	Reference	Date
Children's Court	Children's Court Rules and Forms 10-103	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

District Court	Rules of Civil Procedure 1-011	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

District Court	Rules of Civil Procedure 2-301	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

District Court	Rules of Civil Procedure 5-206	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

Magistrate Court	Magistrate Court Rules 6-210	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law. Rules for facsimile filing.

Metropolitan Court	Metropolitan Court Rules 7-210	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law. Rules for facsimile filing.

Municipal Court	Municipal Court Rules 8-209	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law. Rules for facsimile filing.

State	Rules of Appellate Procedure 12-302	1/ 1/97

"Signature" means original, copy, computer-generated, or other signature authorized by law.

Statute	14-3-15.2	6/16/95

Electronic authentication; substitution for signature; must meet standards promulgated by commission

US Bankruptcy Court	Local Bankruptcy Rule 5005-4	10/ 1/96

Facsimile Filings; no prior judicial authorization required for facsimilie filing; electronic transmission; court to establish guidelines

US District Court	Administrative Order 97-26	1/ 1/96

ID and password for signature; registration procedures; electronic file stamp; attorneys retain originals; notices in electronic mailbox.

US District Court	Local Civil Rules 5	1/ 1/96

Rules for facsimile filing; fees paid; filing, service, and notice by electronic transmission

FAX Filing

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	10/ 1/96

Facsimile Filings; no prior judicial authorization required for facsimilie filing; electronic transmission; court to establish guidelines

Nevada

Electronic Filing

Court	Reference	Date
Statute	171.103	10/ 1/97

Electronic filing of complaint; signature required; time stamp required

Statute	173.049	10/ 1/97

Clerk may accept information filed electronically; procedure; service; signature required; time stamp required

Statute	432B.515	10/ 1/97

Electronic filing of certain petitions and reports; signature required

Statute	62.206	10/ 1/97

Electronic filing of certain documents; petition from district attorney; others; must contain image of signature

New York

Electronic Filing

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 9021-1	7/ 1/97

Entry of orders, judgements, and decrees; clerk shall enter all in electronic filing system, which constitutes entry of order.

US Bankruptcy Court ED	9011-1	7/ 1/97

Attorneys; duties; control of password

US Bankruptcy Court ND	Local Bankruptcy Rule 904.2	12/ 1/96

Filing Generally; no papers filed electronically or by facsimile are considered filed; originals must be submitted by mail

US Bankruptcy Court SD	Local Bankruptcy Rule 9011-1	12/ 1/96

Signing of Papers; electronic filing password only used by attorney and authorized members and employees of the attorney's firm

US Bankruptcy Court SD	Local Bankruptcy Rule 9021-1	12/ 1/96

Entry of Orders, Judgements, and Decrees; all orders, judgments, and decrees entered into electronic filing system are considered docketed and entered

US Bankruptcy Court SD	Local Bankruptcy Rule Appendix G	7/20/94

Pilot Program for CLAD General Order 111-134; cases assigned to CLAD; exhibit establishes administrative procedures; passwords; administrative procedures; court designates cases; forms

FAX Filing

Court	Reference	Date
US Bankruptcy Court ND	Local Bankruptcy Rule 904.2	12/ 1/96

Filing Generally; no papers filed electronically or by facsimile are considered filed; originals must be submitted by mail

Ohio

Digital Signature

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	3/10/97

Documents may be filed, signed, or verified by electronic means consistent with technical standards of the Judicial Conference once such standards are published and approved by this court.

Electronic Filing

Court	Reference	Date
Fifth Appellate District	Rule 2	5/ 1/97
Only motions may be filed electronically or by facsimile. No other pleadings allowed.		
State	Rules of Civil Procedure	7/ 1/94
Local rules may provide for electronic filing; signature assumed authentic; if shown otherwise, pleadings or papers shall be stricken.		
US Bankruptcy Court	Local Bankruptcy Rule 5005-4	3/10/97
Documents may be filed, signed, or verified by electronic means consistent with technical standards of the Judicial Conference once such standards are published and approved by this court.		

FAX Filing

Court	Reference	Date
Fifth Appellate District	Rule 2	5/ 1/97
Only motions may be filed electronically or by facsimile. No other pleadings allowed.		
Juvenile Court	Rules of Juvenile Procedure 8	7/ 1/96
Filing by Facsimile Transmission; procedure; equipment standards; historical and statutory notes		

Oklahoma

Electronic Filing

Court	Reference	Date
Statute	20-40-3004	7/ 1/97
Electronic filing of documents; in supreme court and district courts; rules promulgated by AOC, approved by supreme court		

Oregon

Digital Signature

Court	Reference	Date
Statute	192.825 through 192.855	7/ 1/97
Electronic Signature Act		

Electronic Filing

Court	Reference	Date
Statute	14-153.770	12/31/95
Electronic filing of complaint; signature not required as on citation; court to establish rules; verification; public access to documents		

Tax Court Regular Division	Rule 7	1/ 1/97

Summons Generally; telegraphic transmission; summons and complaint may be transmitted electronically as provided in rule 8 D

FAX Filing

Court	Reference	Date
Tax Court Regular Division	Rule 8	1/ 1/90

Process; telegraphic transmission of writ, order, or paper for service

Pennsylvania

Electronic Filing

Court	Reference	Date
State	Rules of Criminal Procedure 95	1/ 1/97

Proceedings in Summary Cases Charging Parking Violations; parking citation may be filed electronically

State	Rules of Criminal Procedure 61	1/ 1/97

Procedures Following Filing of Citation--Issuance of Summons; if citation filed electronically, summons also shall include listed data elements

US Bankruptcy Court MD	Bankruptcy Practice Order Northern Tier	12/ 1/96

Electronic filing authorized under F.R.B.P. 5005 (a) (2).

US District Court ED	Clerk's Office Procedural Handbook	5/ 1/97

Electronic filing

Rhode Island

Digital Signature

Court	Reference	Date
Statute	42-127-1 through 42-127-6	1/ 1/98

Electronic Signatures Act

Electronic Filing

Court	Reference	Date
US Bankruptcy Court	Local Bankruptcy Rule 5081-1	11/ 1/97

Signatures; judges; use of endorsement stamp or electronic signature by clerk authorized; equals original signature.

Tennessee

Electronic Filing

Court	Reference	Date
Statute	16-1-115	6/13/97
Electronic signatures have same force and effect as written signatures		

FAX Filing

Court	Reference	Date
US Bankruptcy Court ED	Rule 5005-4	4/15/97
Papers may only be filed by facsimile with express permission of court. Original shall be properly substituted.		

Texas

Digital Signature

Court	Reference	Date
Statute	1-2A-108	9/ 1/97
Digital signature; definitions; misuse subject to criminal laws		
Statute	10B-2054.060	9/ 1/97
Digital signature; allowed; misuse subject to criminal law; definitions		
Statute	4A-403.027	6/19/97
Digital signatures; comptroller may establish procedures for digital signatures		
Statute	6A-201.931 through 6A-201.933	9/ 1/97
Electronic issuance of licenses; digital signature defined; digital signature allowed on application		
Statute	7E-623.074	9/ 1/97
Transportation department may authorize digital signature on electronic application		

Electronic Filing

Court	Reference	Date
State	Rules of Appellate Procedure 9	9/ 1/97
Court of appeals by local rule may permit documents to be filed, signed, or verified electronically if consistent with Supreme Court technology standards.		
Statute	2D-51.801 through 2D-51.807	9/ 1/87
Electronic filing of certain documents		
Statute	2F-77.031	9/ 1/97
Judicial committee on information technology; standards; statewide automation; security; pilot programs		

Statute	6C-205.005	9/ 1/89
Electronic storage of records; chapter not in conflict with electronic filing in district and county courts		
US Bankruptcy Court ND	Local Bankruptcy Rule 5005.4	4/15/97
Clerk authorized to implement electronic filing and noticing subject to approval by the court		
US District Court ED	Local Rule CR-49	10/27/97
Electronic filing not allowed unless authorized by clerk;document filed and served when received		
US District Court ED	Local Rule CV-5	10/27/97
Electronic filing not allowed unless authorized by clerk;document filed and served when received		
US District Court WD	Local Rule 9013	1/ 1/94
Clerk may implement electronic filing with approval of court		
US District Court WD	Operating Procedures	5/ 1/94
Clerk may implement electronic filing with approval of court		
US District Court WD	Operating Procedures Clerks Office	2/ 1/97
Facsimile filings not accepted. Electronic filings accepted if attorney is registered ELF user		

FAX Filing

Court	Reference	Date
US District Court WD	Operating Procedures Clerks Office	2/ 1/97
Facsimile filings not accepted. Electronic filings accepted if attorney is registered ELF user		

Utah

Digital Signature

Court	Reference	Date
Statute	46-1-1 through 46-2-9	7/ 1/97
Notaries Public Reform Act		
Statute	46-3-101 through 46-3-504	5/ 1/95
Utah Digital Signature Act		

Electronic Filing

Court	Reference	Date
Code of Judicial Adminstration	Appendix G	4/15/95
Child support worksheets; provision for electronic filing		

Virginia

Digital Signature

Court	Reference	Date
Statute	2.1-563.31	1/ 1/98
Council on Information Management; duties listed; digital signature regulations		
Statute	59.1-467 through 59.1-469	1/ 1/98
Digital signatures; definitions; authentication; state agencies use of digital signatures authorized		

Electronic Filing

Court	Reference	Date
Statute	17-2-3.01	7/ 1/98
Electronic filing with clerk; expired 7/1/98; was it renewed?		
Statute	17-83.1	12/31/97
Electronic filing with clerk; definition; authorized; completion of filing; transmission and distribution of data; acknowledgement; encoding; media; signature required		

Washington

Digital Signature

Court	Reference	Date
Statute	19.34.010 through 19.34.503	1/ 1/96
Washington Electronic Authentication Act		

Electronic Filing

Court	Reference	Date
State	Rule 7	3/19/93
Local Rules--Filing and Effective Date; administrator for the courts establishes specifications for court to file its local rules electronically		
Statute	19.34.900	7/27/97
Other references to Washington Electronic Authentication Act		

Appendix D: Data Elements for Initial Filings in Civil Cases

Compiled by

Christopher M. Shelton
National Center for State Courts

The matrix on the following pages lists typical data elements needed for initial filings in civil cases, together with the cover sheets or filing forms on which those elements are provided to the courts by filers in different states.

Civil Action Data Elements	State of North Carolina	Circuit Court (Baltimore/ Prince George's)	Superior Court of DeKalb County (GA)	Alabama Unified Judicial System
Initial Filing	Civil Action Cover Sheet	Case Information Report	Civil Case Initiation Form	Cover Sheet (Civil Case)
Arbitration Requested?	Stipulate to arbitration?	ADR requested?		Mediation Requested?
Arbitration Tried?		ADR been tried?		
Attorney Address City	Name And Address of Attorney, or Party if Not Respresented		Attorney for Plaintiff (Defendant) (Name, add. & phone)	
Attorney Address Line 1	Name And Address of Attorney, or Party if Not Respresented		Attorney for Plaintiff (Defendant) (Name, add. & phone)	
Attorney Address Line 2	Name And Address of Attorney, or Party if Not Respresented		Attorney for Plaintiff (Defendant) (Name, add. & phone)	
Attorney Address Line 3	Name And Address of Attorney, or Party if Not Respresented		Attorney for Plaintiff (Defendant) (Name, add. & phone)	
Attorney Address State	Name And Address of Attorney, or Party if Not Respresented		Attorney for Plaintiff (Defendant) (Name, add. & phone)	
Attorney Address Zip Code	Name And Address of Attorney, or Party if Not Respresented		Attorney for Plaintiff (Defendant) (Name, add. & phone)	
Attorney Bar Number	Attorney Bar Number		Georgia Bar Number	
Attorney Bar Number Suffix				
Attorney Code				Attorney Code (6-digit field)
Attorney Law Firm	Name of Firm			
Attorney Name	Name And Address of Attorney, or Party if Not Respresented			
Attorney Phone Number				
Case Number	File Number	Case Number	Case Number	Case Number
Case Origin	Origin (Initial Filing or Subsequent Filing)		Origin (Original, Removed, Reinstated, Transferred)	Origin (Initial, Remanded, Appeal, Transferred, Other)
Case Style		Case Name: Plaintiff field V. Defendant field		
Claim	Claim for Relief For	Nature of Action	Case Type/Category	Nature of Suit
Class Action Suit?				
Companion Case Number(s)		Case #	Case Number	
Companion Case?			Companion Case or Same issue of fact or grows out of the same transaction	
Complex Litigation?	Complex Litigiation			
Consolidated (Y or N)				
Court Jurisdiction	In the General Court of Justice: District or Superior Court Division	Circuit Court for: [City or County]		In the Circuit Court of [field] County
Damages		Damages/Relief		Relief Requested? [Monetary Award or No Monetary Award]
Declaration of Non Military Status				
Defendant (Name of)	Name of Defendant (1, 2 and 3)		Defendant	Defendant
Defendant(s) Against Whom Crossclaim Asserted	Defendant(s) Against Whom Crossclaim Asserted			
Facsimile Number	Fax Number (Attorney or pro se litigant)			
Fictitious Business Name Declaration				
File Date	Date	Date		Date of Filing
Form Filed By Plaintiff or Defendant		Form Filed By (P or D)		
Judge (Name of)				
Jury Trial Demanded?	Jury Demaned in Pleading	Jury Demand [Y or N]		Jury Trial Demanded? [Y / N]
Party Address Line 1				
Party Address Line 2				
Party Address Line 3				
Party City				
Party Code				Plaintiff and Defendant Type
Party Name				
Party State				
Party Telephone Number				
Party ZIP Code	Zip Code			
Plaintiff (Name of)	Name of Plaintiff (1,2 and 3)		Plaintiff	Plaintiff
Plaintiff (s) Against Whom Counterclaim Asserted	Plaintiff (s) Against Whom Counterclaim Asserted			
Pleading Type	Type of Pleading (Complaint, Reply, Answer, etc.)			
Pro Se Code (Y or N)				
Registered Owner of the Vehicle?				

Civil Action Data Elements	**Washington State**	**State of Wisconsin**	**State of Florida**
Initial Filing	Case Information Cover Sheet	Pretrial/Scheduling Data Sheet	Civil Cover Sheet
Arbitration Requested?		Preferred dispute resloution procedures the court should order	
Arbitration Tried?			
Attorney Address City			
Attorney Address Line 1			
Attorney Address Line 2			
Attorney Address Line 3			
Attorney Address State			
Attorney Address Zip Code			
Attorney Bar Number	Bar Membership Number		
Attorney Bar Number Suffix			
Attorney Code			
Attorney Law Firm			
Attorney Name	Attorney Name		
Attorney Phone Number			
Case Number	Case Number	Case Number	Case Number
Case Origin			
Case Style	Case Title		Case Style
Claim	Cause of Action/Category	Nature of Lawsuit	Type of Case
Class Action Suit?			
Companion Case Number(s)			
Companion Case?			
Complex Litigation?			
Consolidated (Y or N)			
Court Jurisdiction	[field] County Superior Court		Name of Court
Damages			
Declaration of Non Military Status			
Defendant (Name of)		Defendant	Defendant
Defendant(s) Against Whom Crossclaim Asserted			
Facsimile Number			
Fictitious Business Name Declaration			
File Date			Date
Form Filed By Plaintiff or Defendant			
Judge (Name of)			Judge
Jury Trial Demanded?			Jury Trial Demanded in Complaint? [Y or N]
Party Address Line 1			
Party Address Line 2			
Party Address Line 3			
Party City			
Party Code			
Party Name			
Party State			
Party Telephone Number			
Party ZIP Code			
Plaintiff (Name of)		Plaintiff	Plaintiff
Plaintiff (s) Against Whom Counterclaim Asserted			
Pleading Type			
Pro Se Code (Y or N)			
Registered Owner of the Vehicle?			

Civil Action Data Elements	Judicial Council of CA	Municipal Court of CA, Riverside	State of Louisiana
Initial Filing	Civil Case Cover Sheet	Civil Form	Civil Case Form
Arbitration Requested?			
Arbitration Tried?			
Attorney Address City	Attorney or Party Without Attorney (Name and Address)		
Attorney Address Line 1	Attorney or Party Without Attorney (Name and Address)		
Attorney Address Line 2	Attorney or Party Without Attorney (Name and Address)		
Attorney Address Line 3	Attorney or Party Without Attorney (Name and Address)		
Attorney Address State	Attorney or Party Without Attorney (Name and Address)		
Attorney Address Zip Code	Attorney or Party Without Attorney (Name and Address)		
Attorney Bar Number			
Attorney Bar Number Suffix			
Attorney Code			
Attorney Law Firm			
Attorney Name	Attorney or Party Without Attorney (Name and Address)		
Attorney Phone Number	Telephone Number		
Case Number	Case Number	Case Number	
Case Origin			Type of Filing (New or Refiling)
Case Style	Case Name	Title	
Claim	Case Category		Case Type
Class Action Suit?	Is this a class action suit? [Y or N]		
Companion Case Number(s)			
Companion Case?			
Complex Litigation?			
Consolidated (Y or N)			
Court Jurisdiction	Name of Court, Judicial District, and Branch Court		Judicial District Number, Parish Number, Court Division
Damages	Type of remedies sought: (Monetary, Nonmonetary, Punitive)	Amount owed	
Declaration of Non Military Status		No defendant named is in the military service [none or name of defendant]	
Defendant (Name of)	Attorney For (Name)	Defendant	
Defendant(s) Against Whom Crossclaim Asserted			
Facsimile Number	Fax [Number]		
Fictitious Business Name Declaration		Doing business as: Individual, partnership, corporation, association, other	
File Date	Date		File Date
Form Filed By Plaintiff or Defendant			
Judge (Name of)			
Jury Trial Demanded?			
Party Address Line 1		Address (street)	
Party Address Line 2			
Party Address Line 3			
Party City		City	
Party Code			
Party Name			
Party State			
Party Telephone Number		Telphone Number (Home and Work)	
Party ZIP Code		Zip	
Plaintiff (Name of)	Attorney For (Name)	Plaintiff	
Plaintiff (s) Against Whom Counterclaim Asserted			
Pleading Type			
Pro Se Code (Y or N)			
Registered Owner of the Vehicle?		Registered Owner of the Vehicle? [Y or N]	

Appendix E: Sample Court Rules

The following statutes, regulations, rules, and other materials illustrate efforts by states to manage the implementation and operation of new technologies, e.g., electronic filing of documents in courts and digital signature. The following materials are included:

1. *Los Angeles County Superior Court Rule 18.00 Electronic Filing and Service*
2. *Mississippi Code 1972 Annotated 9-1-51 through 9-1-57 Electronic Filing and Storage of Court Documents*
3. *Florida Rules of Judicial Administration 2.090 Electronic Filing of Matters in all Proceedings within the State Courts System*
4. *Utah Digital Signature Act*
5. *Utah Digital Signature Administrative Rules R154 Commerce, Corporations and Commercial Code*
6. *Utah Certificate Authority License and Disclosure Record*
7. *California Government Code Section 16.5 Digital Signature*
8. *Proposed California Digital Signature Regulations*
9. *Santa Clara County Superior Court Rule 1.7 Electronic Filing and Service*
10. *Delaware Superior Court Rules of Civil Procedure Interim Rule 79.1 Complex Litigation Automated Docket*
11. *Bankruptcy Rules of the U.S. District Courts for the Southern and Eastern Districts Local Rules Appendix G In re: Pilot Program for Complex Litigation Automated Docket, General Order M-134*
12. *Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania XLI. Electronic Filing and Retrieval of Documents*

Los Angeles County Superior Court Rules

Rule 18.00 Electronic Filing and Service

(a) Requirements for Electronically Submitted Documents. A litigant or the litigant's attorney may file an electronic document in a case via an electronic filing service, if:

(1) The filing litigant or the litigant's attorney executes a contract with the court in a form approved by the executive officer of the court, which contract shall include a promise not to send harmful or deleterious matter into the court's information system;

(2) All of the electronic document is digitally signed by all persons required to sign, and each such digital signature is verifiable pursuant to Rule 18.01 on digital signatures;

(3) The electronic document is received at an address specified. Rules governing the size of paper, margins, and other specifications based on characteristics peculiar to paper, whether in these or other court rules, shall not apply to electronic documents filed pursuant to this rule, except that such documents, when printed in accordance with the rules governing paper documents, may not exceed any limits on the number of pages that may be filed.

(b) Enhanced Service: Contractual Requirements. Filing documents electronically is an enhanced information service provided by arrangement with one or more private-sector firms under contract with the court. Such a firm may require payment of a fee and/or impose other reasonable requirements by contract with the filing litigant or the litigant's attorney as conditions for processing an electronic filing.

(c) Return Notice of Filing. Upon receiving an acceptable electronic document, the electronic filing system or clerk shall return to the sender a statement confirming acceptance of the filing. The confirmation shall include a notation of the date and time of filing. If an electronic document is received but unacceptable, the electronic filing system or a clerk shall also notify the sender of the document's rejection and the grounds for rejection. A copy of this confirmation or rejection will be retained in the permanent electronic case file maintained by the court.

(d) Time of Filing. An electronic document may be electronically submitted to the court at any time of the day, and shall be considered filed on the date and time that it is accepted. Acceptance shall be determined by the clerk, and shall be deemed to occur (i) on the date the filing was submitted if the submission began during normal business hours of the clerk's office, and (ii) on the next day the clerk's office is open for business if submission began after normal business hours of the clerk's office. Notwithstanding the foregoing, the court may authorize the electronic filing service to automatically accept certain electronic documents specified on a list provided by the court and published by the electronic filing service, in which case such filings shall be deemed accepted as of the date and time the filing was submitted, regardless of whether the office of the clerk is open for business.

(e) Electronic Issuance of Summons. On request, the electronic filing system may issue a digitally signed summons bearing a graphical image of the seal of the court. A printed version of such summons shall have the same force and effect as a summons issued by the clerk on paper and under the seal of the court.

(f) Visible Renditions of Electronic Documents. A visible presentation of an electronic document is equivalent to the original of the document according to the following restrictions:

(1) A screen display of a document transmitted by facsimile transmission is equivalent to a paper print-out of the transmitted document, if the display of the document image is at a degree of resolution equal to the resolution at which the facsimile is stored in the records of the court.

(2) A screen display or paper print-out of an electronic document in image form is equivalent to the electronic original, if the display or print-out is at a degree of resolution equal to the resolution at which the document is stored in the records of the court.

(3) A screen display or paper print-out is equivalent to the original of a textual document.

(g) Electronically Mailed Service. In circumstances where a document may be served by paper mail or fax on a person who has executed a contract with the court for electronic filings.

(1) A textual document may be served on such person by electronic mail to the receiver's electronic mail address;

(2) A document in image form may be served on such person by electronic mail to the receiver's electronic mail address with the prior, written consent of the receiver. An electronic mail address is refutably presumed valid for a particular receiver if the receiver files electronic documents in court from the address, and the sender has no notice that the address is invalid. If served pursuant to this rule, time is calculated as set forth in Code of Civil Procedure section 1013(e).

(h) Facsimile Transfer to Computer File. The court may receive a facsimile transmission into a computer file, rather than receiving such a transfer onto paper. For purposes of these rules, however, such a document shall not be considered an electronic document, but rather, shall be governed by the rules governing fax filings.

(i) Definitions. For purposes of this rule:

(1) "Digital signature" has the meaning assigned to it in Rule 18.01.

(2) "Document in image form" means an electronic document recorded as a matrix of dots forming a picture, rather than as a textual document.

(3) "Electronic document" means text, however encoded or recorded including a textual document, or a document in image form, to be filed in a case pending before the court.

(4) "Electronic filing system" means the computer equipment and software receiving and processing electronic documents on behalf of and by authority of the court.

(5) "Electronic mail" means the transport or communication of computer-based information by the electronic filing service.

(6) "Screen" means an electronic device for representing computer-based information using visible light. Cathode ray tubes and liquid crystal displays are two examples of screens.

(7) "Textual document" means a machine-readable document in digital form encoded according to the American Standard Code of Information Interchange (ASCII) or Standard 646 of the International Organization for Standardization (IOS).

Rule 18.01 Digital Signatures on Electronic Documents

(a) Executive Officer May Authorize.

(1) Certification Authorities. The executive officer may authorize specified persons to act as certification authorities to issue certificates and otherwise provide services that will facilitate the use of digital signatures on electronically filed documents, and may take reasonable action to assure competence and prudence by such persons in acting as certification authorities. Further, the executive officer may terminate any authority granted pursuant to this rule in accordance with any applicable agreement between the court and the certification authority following reasonable notice and an opportunity to be heard. Persons authorized to act as certification authorities may require payment of a fee, impose other reasonable requirements by contract with the filing litigant or the litigant's attorney as conditions for the services to be provided, and define the practices it employs in issuing certificates via a certification practice statement.

(2) Repository. The executive officer may authorize specified persons, including certification authorities, to establish and maintain a repository for the court.

(b) Certificate Issuance.

(1) Prerequisites to Issuance. A certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

(a) The certification authority has received a signed request for issuance of a certificate by the prospective subscriber;

(b) The certification authority confirms that:

(i) The prospective subscriber is the person identified in the request and the person to be identified in the certificate to be issued;

(ii) The prospective subscriber bears a distinguished name and;

(iii) The prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate.

(c) The certification authority confirms that the prospective subscriber holds a key pair capable:

(i) Of affixing a digital signature by using the private key corresponding to the public key to be listed in the certificate; and

(ii) Of verifying by using the public key a digital signature affixed by the corresponding private key.

(2) Use of Authentication Agent. For purposes of fulfilling its obligations under Rule 18.01(b)(1)(ii), a certification authority may rely on an authentication agent. Attorneys may act as authentication agents for clients they represent.

(3) Contents of a Certificate. Each certificate issued by a certification authority shall consist of a computer-based record that is digitally signed by the issuing certification authority and that (a) identifies the issuing certification authority; (b) identifies its subscriber; (c) contains the subscriber's public key; and (d) contains such other information and limitations as the certification authority shall deem appropriate.

(4) Publication of the Certificate. If the subscriber accepts the certificate, the certification authority shall publish a signed copy of the certificate in the repository provided by the court.

(5) Suspension or Revocation by Certification Authority for Faulty Issuance. After issuing a certificate, a certification authority shall revoke it immediately upon

confirming that it was not issued as required by this rule, and may suspend it while investigating to confirm grounds for revocation. The certification authority shall give notice as practicable to the subscriber of a certificate revoked or suspended pursuant to this subsection.

(c) Representation by the Subscriber Accepting a Certificate. By accepting a certificate issued by a certification authority, the subscriber identified in the certificate certifies to the court and all others who justifiably rely on a digital signature affixed to an electronic document filed with the court and verifiable by the public key listed in the certificate, that:

(1) Each digital signature affixed by means of the private key corresponding to the public key listed in the certificate is a legally valid signature of the subscriber for purposes of filing documents in court, unless the certificate is suspended, revoked, or has expired;

(2) To the best of the subscriber's knowledge, no unauthorized person has access to the private key corresponding to the public key listed in the certificate;

(3) All representations made by the subscriber to the certification authority or its authentication agent and material to the information contained in the certificate are true; and

(4) The information contained in the certificate is true to the best of the subscriber's knowledge.

(d) Representation by an Attorney Acting as an Authentication Agent. An attorney who acts as an authentication agent for the certification authority with respect to a prospective subscriber certifies to the certification authority, and to all who justifiably rely on a digital signature affixed to an electronic document filed with the court and verifiable by the public key listed in the certificate subsequently issued to such subscriber, that the subscriber is the person identified in the signed request delivered to the certification authority and the person to be identified in the certificate to be issued, and that the prospective subscriber bears a distinguished name.

(e) Control of the Private Key.

(1) Subscriber's Responsibility for Signatures and Private Key Security. A digital signature affixed by the private key corresponding to the public key in a duly accepted certificate is the signature of the subscriber named in the certificate for purposes of any document filed in a case pending before the court. By accepting a certificate issued by a certification authority, the subscriber identified in the certificate assumes a duty to retain exclusive control of the private key and keep it confidential. The court may depart from the effect of this rule in extraordinary circumstances, but only upon a showing of good cause or excusable neglect.

(2) Private Key Is Property of the Subscriber. A private key is the property of the subscriber who rightfully holds it.

(3) Certification Authority Is a Fiduciary if Holding Subscriber's Private Key. A certification authority may hold the private key corresponding to a public key listed in a certificate which it has issued only upon express [written] authorization of the subscriber named in the certificate. In such case, it holds the private key as a fiduciary of the subscriber named in the certificate, regardless of any provision to the contrary in a contract between the subscriber and the certification authority. The certification authority shall not use the private key of a subscriber named in a certificate issued by the

certification authority, except upon order of the court.

(4) Attorney Is a Fiduciary if Holding Client's Private Key. An attorney may hold the private key of the attorney's client corresponding to a public key listed in a certificate that has been issued to the attorney's client as a subscriber only upon express authorization of the subscriber named in the certificate. In such case, the attorney holds the private key of the attorney's client as a fiduciary of the client named in the certificate, regardless of any provision to the contrary in a contract between the attorney and the attorney's client. The attorney may use the private key of the subscriber/client named in a certificate issued by the certification authority only upon express authorization from the client or upon order of the court.

(5) Representation by an Attorney Who Uses a Client's Private Key. An attorney who uses the private key of the attorney's client corresponding to a public key listed in a certificate that has been issued to the attorney's client as a subscriber certifies to the court, all other litigants and their attorneys, and all third parties who justifiably rely on a digital signature affixed to an electronic document filed with the court and verifiable by the public key listed in the certificate, that the attorney has authority to sign digitally on behalf of the client, and, if that authority is limited in any way, adequate safeguards exist to prevent a digital signature from exceeding the bounds of the client's authority.

(f) Certification Authority's Representations. By issuing a certificate, a certification authority certifies to all who justifiably rely on a digital signature affixed to an electronic document filed with the court and verifiable by the public key listed in the certificate, that the certification authority has, in accordance with any certification practice statement of which the relying person has notice, complied with all applicable requirements of this rule for issuance of the certificate. A person has notice of the contents of a certification practice statement if such person has actual notice, or if such certification practice statement is incorporated by reference in the certificate for the public key used to create the digital signature on which such person relies, and is publicly available from the court of the electronic filing service.

(g) Suspension of a Certificate.

(1) Suspension by Request. Unless the certification authority and subscriber agree otherwise, the certification authority which issued a certificate shall suspend the certificate for a period of 48 hours upon request by a person identifying himself as (i) the subscriber named in the certificate, (ii) an agent, law partner, or employee of the same law firm as the subscriber, or (iii) an employee or member of the immediate family of the subscriber. The certification authority has no obligation to confirm the identity or agency of the person requesting suspension.

(2) Publication in Repository. Immediately upon suspension of a certificate, the suspending certification authority shall publish a digitally signed notice of the suspension in the repository provided by the court.

(3) Termination of Requested Suspension. A certification authority shall terminate a suspension initiated by request only:

(a) On request for termination of the suspension by the subscriber named in the suspended certificate, after the certification authority has confirmed the identity of the person making the request;

(b) On request for termination of the suspension by an agent of the subscriber named in the suspended certificate, after the certification authority has confirmed that the

person making the request is authorized to do so;

(c) When the certification authority discovers and confirms that the request for the suspension was made without authorization by the subscriber; however, this subsection imposes no obligation on the certification authority to confirm a request for suspension.

(4) Alternate Contractual Procedures. The contract between a subscriber and a certification authority may limit or eliminate suspension by the certification authority upon request, or may provide otherwise for termination of a suspension or disclosure of information about a suspension.

(h) Revocation of a Certificate.

(1) Revocation Required on Request. A certification authority shall revoke a certificate which it issued after receiving and confirming a request for revocation by the subscriber named in the certificate, [or the court]. If a certification authority receives a subscriber's written request accompanied by evidence reasonably sufficient to confirm the request and any required fee, the certification authority shall confirm and revoke the certificate within one business day thereafter.

(2) Revocation at Death. A certification authority shall revoke a certificate which it issued upon receiving a certified copy of the subscriber's death certificate or upon confirming by other evidence that the subscriber is dead.

(3) Revocation in Emergency. A certification authority may revoke one or more certificates which it issued if the certificates are or become unreliable, after giving notice to the subscriber listed in the certificate.

(4) Publication of Notice. Immediately upon revocation of a certificate, the revoking certification authority shall publish a digitally signed notice of the revocation in the repository provided by the court.

(5) Effect of Revocation Request for Subscriber. Beginning one business day after the subscriber requests revocation of a certificate in writing, supplies to the issuing certification authority information reasonably sufficient to confirm the request, and pays any required fee, a subscriber ceases to certify with respect to such certificate as provided in subsection (c) above and has no further duty to keep the applicable private key secure as required by subsection (e).

(6) Effect of Publication on Certification Authority. Upon publication of notice of revocation, a certification authority is discharged of its warranties based on issuance of the revoked certificate and ceases to certify as provided in section (f) above.

(i) Expiration of a Certificate. A certificate shall indicate the date on which it expires, which shall be no later than two years after its issuance. When a certificate expires, the subscriber and certification authority cease to certify as provided in this chapter and the certification authority is discharged of its duties based on issuance, in relation to the expired certificate.

(j) Definitions. For purposes of this rule:

"Accept a certificate" means to take manual delivery of a certificate, or to request or cause a certificate to be published.

"Asymmetric cryptosystem" means a computer algorithm or series of algorithms which utilize two different keys, one for encrypting and the other for decrypting a given message, and the keys have the property that, knowing one key, it is computationally infeasible to discover the other key.

"Authentication agent" means an attorney who acts on behalf of a certification authority in satisfying the prerequisites to issuance of a certificate specified by these rules.

"Bit" means a binary digit, that is, a number, often encoded in a computer- readable form, which has a value of either 0 or 1.

"Certificate" means a computer-based record identifying a subscriber and containing the subscriber's public key and such other information as required by this rule.

"Certification authority" means a person who is authorized by the executive officer pursuant to subsection (a) of this rule to issue certificates.

"Certification practice statement" means a statement of the practices that a certification authority employs in issuing certificates generally, or employed in issuing a particular certificate.

"Certify" means to declare with reference to a certificate, with ample opportunity to reflect, and with a duty to apprise oneself of all material facts.

"Confirm" means to ascertain through inquiry and investigation carried out with all the effort and resources commercially reasonable under the circumstances.

"Correspond" means, in relation to keys, that one key belongs to the same key pair as the other.

"Digital signature" is a sequence of bits which a person intending to sign creates in relation to a clearly delimited message by running the message through a one-way function, then encrypting the resulting message digest using an asymmetrical cryptosystem and the person's private key.

"Distinguished name" means a sequence of alphanumeric characters identifying the person bearing the name and unique in relation to the repository provided by the court.

"Issue a certificate" means to create and digitally sign a certificate and to deliver a copy of the certificate to the subscriber named in the certificate.

"Key pair" means a private key and its corresponding public key, the keys in an asymmetric cryptosystem having the property that one of the pair will decrypt what the other encrypts.

"Material" means germane to, and having substantial consequences for an actual transaction involving a digital signature.

"Message" means a machine-readable document in digital form recorded by means of any medium and intended to be signed.

"One-way function" means an algorithm mapping or translating one set of bits into another set in such a way that:

(1) A message yields the same result every time it is passed through the one-way function;

(2) It is computationally infeasible that a message passed through the one- way function can be derived or reconstituted from the results of the function; and

(3) There is at most only a negligible probability that two messages passing through the same one-way function will produce the same result.

"Person" means a human being, corporation, partnership, governmental body, or any other entity capable of signing a document.

"Private key" means a sequence of bits intended in an asymmetric cryptosystem to be known only to the owner of the key and used to affix a digital signature to a message.

"Public key" means a sequence of bits intended in an asymmetric cryptosystem to

be known to anyone and used to verify a signature.

"Publish" means to record or place on file in a repository.

"Repository" means a database of certificates and notices of suspension and revocation of certificates for use by the court and any other person in verifying digital signatures on court documents.

"Revoke a certificate" means to make a certificate ineffective or void from a specified time and forward perpetually. Revocation is effected by notation or inclusion in the repository provided by the court, and does not imply that a revoked certificate is destroyed or made illegible.

"Rightfully holds a private key" means to know or be able to readily ascertain a private key:

(1) For which a corresponding public key has not been published in a certificate on file in the repository provided by the court;

(2) Which the holder or the holder's agents have not revealed to any person who is not authorized to affix the holder's digital signature; and

(3) Which the holder has not obtained through theft, deceit, eavesdropping, or other unlawful means.

"Subscriber" means a person holding a private key which corresponds to a public key listed in a certificate identifying the subscriber.

"Suspend" means to make ineffective or void temporarily from a specified time forward. It does not imply that a suspended certificate is destroyed or made illegible.

"Verify a digital signature" means to decrypt a digital signature using the public key listed in a valid certificate, pass the message through the one-way function used in affixing the digital signature, and then determine that the result of passing the message through the one-way function and the decrypted digital signature are identical.

Rule 18.02 Court Digital Signatures

(a) Executive Officer May Appoint. The executive officer may authorize specified court officers to act as certification authorities for the court and for court officers acting within the scope of their offices.

(b) Limitations on the Use of Judicial Private Keys. A person holding a judicial private key may use that private key only for court business within the scope of the person's duties as an officer of the court. No person may use a judicial private key except the person named in the certificate containing the corresponding public key. Misuse of private keys in violation of this rule is grounds for discipline of a court employee, contempt of court penalties for a person not employed by the court, and criminal sanctions under applicable law.

(c) Private Key Security. A court officer holding a judicial private key shall keep the key secure. Except as provided in subsection (d) below, no person shall copy a private key of the court or a court officer under any circumstances.

(d) Private Key Escrow With Executive Officer.

(1) A court officer acting as a certification authority may issue a certificate only by written request endorsed by the executive officer of the court.

(2) The executive officer shall retain securely a copy of every judicial private key for which a certificate is issued by a court officer serving as a certification authority.

(3) The executive officer shall not use or divulge a private key retained pursuant to this subsection except upon an order of the presiding judge based on a finding that:

(a) The private key has been lost from the possession of the court officer having primary custody of it;

(b) The court officer having primary custody of the private key is not available at a time when the key must be used;

(c) The court officer having primary custody of the private key refuses to use it without adequate legal grounds for the refusal; or

(d) Other good cause exists in law and fact for use of the private key apart from the court officer having primary custody of it.

The executive officer shall report every usage of an escrowed private key pursuant to this subsection. Nothing in this subsection precludes disciplinary action or contempt proceedings for improper use or nonuse of a judicial private key.

(e) Suspension and Revocation. A certification authority appointed pursuant to this rule may suspend any certificate issued by the certification authority, with or without notice to the subscriber, if the certification authority has reason to suspect a compromise of the private key. In addition, certificates issued pursuant to this rule may be suspended or revoked in substantially the same manner as provided in Rule 18.01 above.

(f) Effect of Digital Signature. A digital signature verified by a judicial public key is equivalent to the signature of the court by the hand of the subscriber listed in the certificate.

(g) Seal of the Court. The seal of the court may be placed on an electronic document by appending to the document a digital image of the seal of the court as it appears on paper, and digitally signing that image using a judicial private key.

(h) Definitions. The definitions of Rule 18.01 apply to this rule. In addition, for purposes of this rule:

"Judicial private key" means the private key corresponding to a public key named in a certificate issued by a certification authority appointed pursuant to subsection "(a)" of this rule.

Mississippi Code 1972 Annotated 9-1-51 through 9-1-57 Electronic Filing and Storage of Court Documents

Section 9-1-51. Definitions.

For purposes of Sections 9-1-51 through 9-1-57, the following terms shall have the meanings ascribed herein unless the context shall otherwise require:

(a) "Court" shall mean the Supreme Court, Court of Appeals, circuit courts, chancery courts, county courts, youth courts, family courts, justice courts and the municipal courts of this state.

(b) "Clerk" shall mean the clerks of any court.

(c) "Judge" shall mean the senior judge of any court.

(d) "County office" shall mean the office of the circuit clerk, chancery clerk, tax assessor and tax collector of every county of this state.

(e) "Documents," "court records," or "court-related records" shall mean and include, but not be limited to, all contents in the file or record of any case or matter docketed by the court, administrative orders, court minutes, court dockets and ledgers, and other documents, instruments or papers required by law to be filed with the court.

(f) "Electronic filing of documents" shall mean the transmission of data to a clerk of any court or state agency by the communication of information which is originally displayed in written form and thereafter converted to digital electronic signals, transformed by computer and stored by the clerk or state agency either on microfilm, magnetic tape, optical discs or any other medium.

(g) "Electronic storage of documents" shall mean the storage, retention and reproduction of documents using microfilm, microfiche, data processing, computers or other electronic process which correctly and legibly stores and reproduces or which forms a medium for storage, copying or reproducing documents.

(h) "Filing system" or "storage system" shall mean the system used by a court or county office for the electronic filing or storage of documents.

Section 9-1-53. Authority to electronically file and store court documents.

Courts and county offices are hereby authorized but not required to institute procedures for the electronic filing and electronic storage of court documents to further the efficient administration and operation of the courts. Electronically filed or stored documents may be kept in lieu of any paper documents. Courts governed by rules promulgated by the Mississippi Supreme Court that institute electronic filing and electronic storage of court documents and offices of circuit and chancery clerks that institute electronic filing and electronic storage of court documents shall do so in conformity with such rules and regulations prescribed by the Administrative Office of Courts and adopted by the Mississippi Supreme Court concerning court records or court-related records. The provisions of Sections 9-1-51 through 9-1-57 shall not be construed to amend or repeal any other provision of existing state law which requires or provides for the maintenance of official written documents, records, dockets, books, ledgers or proceedings by a court or clerk of court in those courts which do not elect to exercise the discretion granted by this section. It is hereby declared to be the intent of the Legislature that official written documents, records, dockets, books, ledgers or proceedings may be filed, stored, maintained, reproduced and recorded in the manner authorized by Sections 9-1-51 through 9-1-57 or as otherwise provided by law, in the discretion of the clerk.

Section 9-1-57. Plan for electronic storage system.

A plan for the storage system shall require, but not be limited to, the following:

(a) All original documents shall be recorded and released into the system within a specified minimum time period after presentation to the clerk;

(b) Original paper records may be used during the pendency of any legal proceeding;

(c) The plan shall include setting standards for organizing, identifying, coding and indexing so that the image produced during the duplicating process can be certified as a true and correct copy of the original and may be retrieved rapidly;

(d) All materials used in the duplicating process which correctly and legibly reproduces or which forms a medium of copying or reproducing all public records, as herein authorized, and all processes of development, fixation and washing of said photographic duplicates shall be of a quality approved for permanent photographic records by the United States Bureau of Standards;

(e) The plan shall provide for retention of the court records consistent with other law and in conformity with rules and regulations prescribed by the Administrative Office of Courts and adopted by the Mississippi Supreme Court and shall provide security provisions to guard against physical loss, alterations and deterioration; and

(f) All transcripts, exemplifications, copies or reproductions on paper or on film of an image or images of any microfilmed or otherwise duplicated record shall be deemed to be certified copies of the original for all purposes.

Florida Rules of Judicial Administration 2.090 Electronic Filing of Matters in all Proceedings within the State Courts System

(a) Definition. "Electronic transmission of documents" means the transmission by electronic signals, to or from a court or clerk of the court, of information which when received can be transformed and stored or reproduced on paper, microfilm, magnetic storage device, optical imaging system, or other electronic record keeping system authorized by the Supreme Court of Florida in a format sufficient to communicate the information on the original document in a readable format.

(b) Application. Any court or clerk of the court may accept the electronic transmission of documents for filing after the clerk, together with input from the chief judge of the circuit, has obtained approval of the procedures and program for doing so from the Supreme Court of Florida.

(c) Documents Affected.

(1) All documents that are court records, as defined in rule 2.075(a)(1), may be filed by electronic transmission provided that:

(A) the clerk of court has the ability to accept and retain such documents;

(B) the clerk of court or the chief judge of the circuit has requested permission to accept documents filed by electronic transmission; and

(C) the Supreme Court of Florida has entered an order granting permission to the clerk of court to accept documents filed by electronic transmission. Any attorney, party, or other person who file a document by electronic transmission shall immediately thereafter, file the identical document in paper form, with an original signature of the attorney, party, or other person if a signature is otherwise required by these rules (hereinafter called the follow- up filing).

(2) The follow-up filing of any document that has previously been filed by electronic transmission may be discontinued if:

(A) after a 90-day period of accepting electronically filed documents, the clerk of court or the chief judge of the circuit certifies to the Supreme Court of Florida that the electronic filing system is efficient, reliable and meets the demands of all parties;

(B) the clerk of court or the chief judge of the circuit requests permission to discontinue that portion of the rule requiring a follow-up filing of documents in paper form, except as otherwise required by general law, statute, or court rule; and

(C) the Supreme Court of Florida enters an order directing the clerk of court to discontinue accepting the follow-up filing.

(d) Service.

(1) Electronic transmission may be used by a court for the service of all orders of whatever nature provided the clerk, together with input from the chief judge of the circuit, has obtained approval from the Supreme Court of Florida of the specific procedures and program to be used in transmitting the orders. All other requirements for the service of such an order shall be met.

(2) Any document electronically transmitted to a court or clerk of the court shall also be served on all parties and interested persons in accordance with the applicable rules of court.

(e) Transmission Difficulties. Any attorney, party, or other person who elects to file any document by electronic transmission shall be responsible for any delay, disruption,

interruption of the electronic signals, and readability of the document, and accepts the full risk that the document may not be properly filed with the clerk as a result.

(f) Administration.

(1) Any clerk of the court who, after obtaining Supreme Court of Florida approval, accepts for filing documents that have been electronically transmitted shall:

(A) provide electronic or telephonic access to its equipment during regular business hours; and

(B) accept electronic transmission of documents up to 10 pages in length.

(2) All attorneys, parties, or other persons using this rule to file documents are required to make arrangements with the court or clerk of the court for the payment of any charges authorized by general law or the Supreme Court of Florida before filing any document by electronic transmission.

(3) The filing date for an electronically transmitted document shall be the date the last page thereof is received by the court or clerk of the court.

(4) Any court or clerk of the court may extend the hours of access or increase the page limitations set forth in this subdivision.

Utah Digital Signature Act
Utah Code Annotated, 1953
46-3-101 Title.

This chapter is known as the "Utah Digital Signature Act."

46-3-102 Purposes and construction.

This chapter shall be construed consistent with what is commercially reasonable under the circumstances and to effectuate the following purposes:

(1) to facilitate commerce by means of reliable electronic messages;

(2) to minimize the incidence of forged digital signatures and fraud in electronic commerce;

(3) to implement legally the general import of relevant standards, such as X.509 of the International Telecommunication Union (formerly International Telegraph and Telephone Consultative Committee or CCITT); and

(4) to establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.

46-3-103 Definitions.

For purposes of this chapter, and unless the context expressly indicates otherwise:

(1) "Accept a certificate" means:

(a) to manifest approval of a certificate, while knowing or having notice of its contents; or

(b) to apply to a licensed certification authority for a certificate, without canceling or revoking the application, if the certification authority subsequently issues a certificate based on the application.

(2) "Asymmetric cryptosystem" means an algorithm or series of algorithms which provide a secure key pair.

(3) "Certificate" means a computer-based record which:

(a) identifies the certification authority issuing it;

(b) names or identifies its subscriber;

(c) contains the subscriber's public key; and

(d) is digitally signed by the certification authority issuing it.

(4) "Certification authority" means a person who issues a certificate.

(5) "Certification authority disclosure record" means an on-line, publicly accessible record which concerns a licensed certification authority and is kept by the division. A certification authority disclosure record has the contents specified by rule of the division pursuant to Section 46-3-104.

(6) "Certification practice statement" means a declaration of the practices which a certification authority employs in issuing certificates generally, or employs in issuing a material certificate.

(7) "Certify" means the declaration of material facts by the certification authority regarding a certificate.

(8) "Confirm" means to ascertain through appropriate inquiry and investigation.

(9) "Correspond," with reference to keys, means to belong to the same key pair.

(10) "Digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

(a) the transformation was created using the private key that corresponds to the signer's public key; and

(b) the message has been altered since the transformation was made.

(11) "Division" means the Division of Corporations and Commercial Code within the Utah Department of Commerce.

(12) "Forge a digital signature" means either:

(a) to create a digital signature without the authorization of the rightful holder of the private key; or

(b) to create a digital signature verifiable by a certificate listing as subscriber a person who either:

(i) does not exist; or

(ii) does not hold the private key corresponding to the public key listed in the certificate.

(13) "Hold a private key" means to be able to utilize a private key.

(14) "Incorporate by reference" means to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated.

(15) "Issue a certificate" means the acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.

(16) "Key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, keys which have the property that the public key can verify a digital signature that the private key creates.

(17) "Licensed certification authority" means a certification authority to whom a license has been issued by the division and whose license is in effect.

(18) "Message" means a digital representation of information.

(19) "Notify" means to communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person.

(20) "Operative personnel" means one or more natural persons acting as a certification authority or its agent, or in the employment of or under contract with a certification authority, and who have:

(a) managerial or policy-making responsibilities for the certification authority; or

(b) duties directly involving the issuance of certificates, creation of private keys, or administration of a certification authority's computing facilities.

(21) "Person" means a human being or any organization capable of signing a document, either legally or as a matter of fact.

(22) "Private key" means the key of a key pair used to create a digital signature.

(23) "Public key" means the key of a key pair used to verify a digital signature.

(24) "Publish" means to record or file in a repository.

(25) "Qualified right to payment" means an award of damages against a licensed certification authority by a court having jurisdiction over the certification authority in a civil action for violation of this chapter.

(26) "Recipient" means a person who receives or has a digital signature and is in a position to rely on it.

(27) "Recognized repository" means a repository recognized by the division pursuant to Section 46-3-501.

(28) "Recommended reliance limit" means the limitation on the monetary amount recommended for reliance on a certificate pursuant to Subsection 46-3-309(1).

(29) "Repository" means a system for storing and retrieving certificates and other information relevant to digital signatures.

(30) "Revoke a certificate" means to make a certificate ineffective permanently from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked certificates, and does not imply that a revoked certificate is destroyed or made illegible.

(31) "Rightfully hold a private key" means to be able to utilize a private key:

(a) which the holder or the holder's agents have not disclosed to any person in violation of Subsection 46-3-305(1); and

(b) which the holder has not obtained through theft, deceit, eavesdropping, or other unlawful means.

(32) "Signer" means a person who creates a digital signature for a message.

(33) "Subscriber" means a person who:

(a) is the subject listed in a certificate;

(b) accepts the certificate; and

(c) holds a private key which corresponds to a public key listed in that certificate.

(34) (a) "Suitable guaranty" means either a surety bond executed by a surety authorized by the Utah Insurance Department to do business in this state, or an irrevocable letter of credit issued by a financial institution authorized to do business in this state by the Utah Department of Financial Institutions, which, in either event, satisfies all of the following requirements, that it:

(i) is issued payable to the division for the benefit of persons holding qualified rights of payment against the licensed certification authority named as the principal of the bond or customer of the letter of credit;

(ii) is in an amount specified by rule of the division pursuant to Section 46-3-104;

(iii) states that it is issued for filing pursuant to this chapter;

(iv) specifies a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority; and

(v) is in a form prescribed by rule of the division.

(b) A suitable guaranty may also provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty.

(c) A financial institution acting as a certification authority may satisfy the requirements of this subsection from its assets or capital, to the extent of its lending limit as provided in Title 7, Financial Institutions Act.

(35) "Suspend a certificate" means to make a certificate ineffective temporarily from a specified time forward.

(36) "Time-stamp" means either:

(a) to append or attach to a message, digital signature, or certificate a digitally signed notation indicating at least the date and time the notation was appended or attached, and the identity of the person appending or attaching the notation; or

(b) the notation thus appended or attached.

(37) "Transactional certificate" means a valid certificate incorporating by reference one or more digital signatures.

(38) "Trustworthy system" means computer hardware and software which:

(a) are reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability, reliability, and correct operation; and

(c) are reasonably suited to performing their intended functions.

(39) (a) "Valid certificate" means a certificate which:

(i) a licensed certification authority has issued;

(ii) the subscriber listed in it has accepted;

(iii) has not been revoked or suspended; and

(iv) has not expired.

(b) A transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference.

(40) "Verify a digital signature" means, in relation to a given digital signature, message, and public key, to determine accurately that:

(a) the digital signature was created by the private key corresponding to the public key; and

(b) the message has not been altered since its digital signature was created.

46-3-104 Role of the division.

(1) The division shall be a certification authority, and may issue, suspend, and revoke certificates in the manner prescribed for licensed certification authorities in Part 3 of this chapter.

(2) The division shall maintain a publicly accessible database containing a certification authority disclosure record for each licensed certification authority. The division shall publish the contents of the database in at least one recognized repository.

(3) In accordance with Title 63, Chapter 46a, Utah Administrative Rulemaking Act, the division shall make rules as required by this chapter and in furtherance of its purposes, including rules:

(a) governing licensed certification authorities, their practice, and the termination of a certification authority's practice;

(b) determining an amount appropriate for a suitable guaranty, in light of:

(i) the burden a suitable guaranty places upon licensed certification authorities; and

(ii) the assurance of financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities;

(c) for reviewing software for use in creating digital signatures and publish reports concerning software;

(d) specifying reasonable requirements for the form of certificates issued by licensed certification authorities, in accordance with generally accepted standards for digital signature certificates;

(e) specifying reasonable requirements for recordkeeping by licensed certification authorities;

(f) specifying reasonable requirements for the content, form, and sources of information in certification authority disclosure records, the updating and timeliness of such information, and other practices and policies relating to certification authority disclosure records; and

(g) specifying the form of certification practice statements.

46-3-201 Licensure and qualifications of certification authorities.

(1) To obtain or retain a license a certification authority shall:

(a) be the subscriber of a certificate published in a recognized repository;

(b) employ as operative personnel only persons who have not been convicted of a felony or a crime involving fraud, false statement, or deception;

(c) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;

(d) file with the division a suitable guaranty, unless the certification authority is the governor, a department or division of state government, the attorney general, state auditor, state treasurer, the judicial council, a city, a county, or the Legislature or its staff offices provided that:

(i) each of the above-named governmental entities may act through designated officials authorized by ordinance, rule, or statute to perform certification authority functions; and

(ii) one of the above-named governmental entities is the subscriber of all certificates issued by the certification authority;

(e) have the right to use a trustworthy system, including a secure means for controlling usage of its private key;

(f) present proof to the division of having working capital reasonably sufficient, according to rules of the division, to enable the applicant to conduct business as a certification authority;

(g) maintain an office in Utah or have established a registered agent for service of process in Utah; and

(h) comply with all other licensing requirements established by division rule.

(2) The division shall issue a license to a certification authority which:

(a) is qualified under Subsection (1);

(b) applies in writing to the division for a license; and

(c) pays the required filing fee.

(3) (a) The division may classify and issue licenses according to specified limitations, such as a maximum number of outstanding certificates, cumulative maximum of recommended reliance limits in certificates issued by the certification authority, or issuance only within a single firm or organization.

(b) A certification authority acts as an unlicensed certification authority when issuing a certificate exceeding the limits of the license.

(4) (a) The division may revoke or suspend a certification authority's license for failure to comply with this chapter, or for failure to remain qualified pursuant to Subsection (1).

(b) The division's actions under this subsection are subject to the procedures for adjudicative proceedings in Title 63, Chapter 46b, Administrative Procedures Act.

(5) The division may recognize by rule the licensing or authorization of certification authorities by other governmental entities, provided that those licensing or authorization requirements are substantially similar to those of this state. If licensing by another governmental entity is so recognized:

(a) Part 4 of this chapter, which relates to presumptions and legal effects, applies to certificates issued by the certification authorities licensed or authorized by that governmental entity in the same manner as it applies to licensed certification authorities of this state; and

(b) the liability limits of Section 46-3-309 apply to the certification authorities licensed or authorized by that governmental entity in the same manner as they apply to licensed certification authorities of this state.

(6) Unless the parties provide otherwise by contract between themselves, the licensing requirements in this section do not affect the effectiveness, enforceability, or validity of any digital signature except that Part 4 of this chapter does not apply to a digital signature which cannot be verified by a certificate issued by a licensed certification authority. Further, the liability limits of Section 46-3-309 do not apply to unlicensed certification authorities.

46-3-202 Performance audits and investigations.

(1) A certified public accountant having expertise in computer security, or an accredited computer security professional, shall audit the operations of each licensed certification authority at least once each year to evaluate compliance with this chapter. The division may specify qualifications for auditors in greater detail by rule.

(2) (a) Based on information gathered in the audit, the auditor shall categorize the licensed certification authority's compliance as one of the following:

(i) full compliance, which means the certification authority appears to conform to all applicable statutory and regulatory requirements;

(ii) substantial compliance, which means the certification authority generally appears to conform to all applicable statutory and regulatory requirements; however, one or more instances of noncompliance or inability to demonstrate compliance were found in the audited sample, but were likely to be inconsequential;

(iii) partial compliance, which means the certification authority appears to comply with some statutory and regulatory requirements, but was found not to have complied or not to be able to demonstrate compliance with one or more important safeguards; or

(iv) noncompliance, which means the certification authority complies with few or none of the statutory and regulatory requirements, fails to keep adequate records to demonstrate compliance with more than a few requirements, or refused to submit to an audit.

(b) The auditor shall report the date of the audit of the licensed certification authority and resulting categorization to the division.

(c) The division shall publish in the certification authority disclosure record it maintains for the certification authority, the date of the audit, and the resulting categorization of the certification authority.

(3) (a) The division may exempt a licensed certification authority from the requirements of Subsection (1) if:

(i) the certification authority to be exempted requests exemption in writing;

(ii) the most recent performance audit, if any, of the certification authority resulted in a finding of full or substantial compliance; and

(iii) the certification authority declares under oath or affirmation that one or more of the following is true with respect to the certification authority:

(A) the certification authority has issued fewer than six certificates during the past year and the total of the recommended reliance limits of all such certificates does not exceed $10,000;

(B) the aggregate lifetime of all certificates issued by the certification authority during the past year is less than 30 days and the total of the recommended reliance limits of all such certificates does not exceed $10,000; or

(C) the recommended reliance limits of all certificates outstanding and issued by the certification authority total less than $1,000.

(b) If the certification authority's declaration pursuant to Subsection (3)(a) falsely states a material fact, the certification authority shall have failed to comply with the performance audit requirement of this subsection.

(c) If a licensed certification authority is exempt under this subsection, the division shall publish in the certification authority disclosure record it maintains for the certification authority a statement that the certification authority is exempt from the performance audit requirement.

46-3-203 Enforcement of requirements for licensed certificate authorities.

(1) The division may investigate the activities of a licensed certification authority material to its compliance with this chapter and issue orders to a certification authority to further its investigation and insure compliance with this chapter.

(2) As provided in Section 46-3-201, the division may restrict a certification authority's license for its failure to comply with an order of the division, or may suspend or revoke the license of a certification authority.

(3) Any person who knowingly or intentionally violates an order of the division issued pursuant to this section or Section 46-3-204 is subject to a civil penalty of not more than $5,000 per violation or 90% of the recommended reliance limit of a material certificate, whichever is less.

(4) The division may order a certification authority in violation of this chapter to pay the costs incurred by the division in prosecuting and adjudicating proceedings relative to, and in enforcement of, the order.

(5) Pursuant to Title 63, Chapter 46b, Administrative Procedures Act:

(a) the division shall exercise its authority under this section in accordance with procedures for adjudicative proceedings;

(b) a licensed certification authority may obtain judicial review of the division's actions under this section; and

(c) if the division seeks injunctive relief, as provided in Section 46-3-204, to compel compliance with any of its orders, the division may collect the cost of enforcement as provided in Subsection 63-46b-19(1)(d)(iii).

46-3-204 Dangerous activities by any certification authority prohibited.

(1) A certification authority, whether licensed or not, may not conduct its business in a manner that creates an unreasonable risk of loss to subscribers of the certification authority, to persons relying on certificates issued by the certification authority, or to a repository.

(2) (a) The division may publish in one or more recognized repositories brief statements advising subscribers, persons relying on digital signatures, and repositories about any activities of a licensed or unlicensed certification authority, of which the division has actual knowledge, which create a risk prohibited by Subsection (1).

(b) The certification authority named in a statement as creating such a risk may protest the publication of the statement by filing a brief, written defense. Upon receipt of such a protest, the division shall:

(i) publish the written defense along with the division's statement;

(ii) publish notice that a hearing has been scheduled to determine the facts and to decide the matter; and

(iii) promptly give the protesting certification authority notice and a hearing as provided in Title 63, Chapter 46b, Administrative Procedures Act.

(c) (i) Following the hearing, the division shall:

(A) rescind the advisory statement if its publication was unwarranted pursuant to this section;

(B) cancel the advisory statement if its publication is no longer warranted;

(C) continue or amend the advisory statement if it remains warranted; or

(D) take further legal action to eliminate or reduce a risk prohibited by Subsection (1).

(ii) The division shall publish its decision in one or more recognized repositories.

(3) As provided in Title 63, Chapter 46b, Administrative Procedures Act, the division may issue orders and obtain injunctions or other civil relief to prevent or restrain a certification authority from violating this section, regardless of whether the certification authority is licensed. This section does not create a right of action in any person other than the division.

46-3-301 General requirements for certification authorities.

(1) A licensed certification authority or subscriber shall use only a trustworthy system:

(a) to issue, suspend, or revoke a certificate;

(b) to publish or give notice of the issuance, suspension, or revocation of a certificate; and

(c) to create a private key.

(2) A licensed certification authority shall disclose any material certification practice statement, and any fact material to either the reliability of a certificate which it has issued or its ability to perform its services. A certification authority may require a signed, written, and reasonably specific inquiry from an identified person, and payment of reasonable compensation, as conditions precedent to effecting a disclosure required in this subsection.

46-3-302 Issuance of a certificate.

(1) A licensed certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

(a) the certification authority has received a request for issuance signed by the prospective subscriber; and

(b) the certification authority has confirmed that:

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) if the prospective subscriber is acting through one or more agents, the subscriber authorized the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate after due diligence;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature; and

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

(c) The requirements of this subsection may not be waived or disclaimed by the licensed certification authority or the subscriber.

(2) (a) If the subscriber accepts the issued certificate, the certification authority shall publish a signed copy of the certificate in a recognized repository agreed upon by the certification authority and the subscriber named in the certificate, unless the contract between the certification authority and the subscriber provides otherwise.

(b) If the subscriber does not accept the certificate, a licensed certification authority shall not publish the certificate or shall cancel its publication if the certificate has already been published.

(3) Nothing in this section precludes a licensed certification authority from conforming to standards, certification practice statements, security plans, or contractual requirements more rigorous than, but consistent with, this chapter.

(4) (a) A licensed certification authority which has issued a certificate:

(i) shall revoke a certificate immediately upon confirming that it was not issued as required by this section; or

(ii) may suspend, for a reasonable period of time not to exceed 48 hours, a certificate which it has issued in order to conduct an investigation to confirm grounds for revocation under Subsection (i).

(b) The certification authority shall give notice of the revocation or suspension to the subscriber as soon as practicable.

(5) (a) The division may order the licensed certification authority to suspend or revoke a certificate which the certification authority issued if, after giving the certification authority and subscriber any required notice and opportunity for a hearing in accordance with Title 63, Chapter 46b, Administrative Procedures Act, the division determines that:

(i) the certificate was issued without substantial compliance with this section; and

(ii) the noncompliance poses a significant risk to persons reasonably relying on the certificate.

(b) The division may suspend a certificate for a reasonable period of time not to exceed 48 hours upon determining that an emergency requires an immediate remedy and in accordance with Title 63, Chapter 46b, Administrative Procedures Act.

46-3-303 Warranties and obligations of certification authority upon issuance of a certificate.

(1) (a) By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:

(i) the certificate contains no information known to the certification authority to be false;

(ii) the certificate satisfies all material requirements of this chapter; and

(iii) the certification authority has not exceeded any limits of its license in issuing the certificate.

(b) The certification authority may not disclaim or limit the warranties of this subsection.

(2) Unless the subscriber and certification authority otherwise agree, a certification authority, by issuing a certificate, shall:

(a) act promptly to suspend or revoke a certificate in accordance with Sections 46-3-306 and 46-3-307; and

(b) notify the subscriber within a reasonable time of any facts known to the certification authority which significantly affect the validity or reliability of the certificate once it is issued.

(3) By issuing a certificate, a licensed certification authority certifies to all who reasonably rely on the information contained in the certificate that:

(a) the information in the certificate and listed as confirmed by the certification authority is accurate;

(b) all foreseeable information material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(c) the subscriber has accepted the certificate; and

(d) the licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate.

(4) By publishing a certificate, a licensed certification authority certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

46-3-304 Representations and duties upon acceptance of a certificate.

(1) By accepting a certificate issued by a licensed certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that:

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(b) all representations made by the subscriber to the certification authority and material to information listed in the certificate are true;

(c) all material representations made by the subscriber to a certification authority or made in the certificate and not confirmed by the certification authority in issuing the certificate are true.

(2) An agent, requesting on behalf of a principal that a certificate be issued naming the principal as subscriber, certifies that the agent:

(a) holds all authority legally required to apply for issuance of a certificate naming the principal as subscriber; and

(b) has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, that adequate safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

(3) A person may not disclaim or contractually limit the application of this section, nor obtain indemnity for its effects, if the disclaimer, limitation, or indemnity restricts liability for misrepresentation as against persons reasonably relying on the certificate.

(4) (a) By accepting a certificate, a subscriber undertakes to indemnify the issuing certification authority for any loss or damage caused by issuance or publication of a certificate in reliance on a false and material representation of fact by the subscriber, or the failure by the subscriber to disclose a material fact if the representation or failure to disclose was made either with intent to deceive the certification authority or a person relying on the certificate or was made with negligence.

(b) If the certification authority issued the certificate at the request of an agent of the subscriber, the agent personally undertakes to indemnify the certification authority pursuant to Subsection (a) as if the agent was an accepting subscriber in his own right. The indemnity provided in Subsection (a) may not be disclaimed or contractually limited in scope, however, a contract may provide consistent, additional terms regarding the indemnification.

(5) In obtaining information of the subscriber material to issuance of a certificate, the certification authority may require the subscriber to certify the accuracy of relevant information under oath or affirmation of truthfulness and under penalty of criminal prohibitions against false, sworn statements.

46-3-305 Control of the private key.

(1) By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature.

(2) A private key is the personal property of the subscriber who rightfully holds it.

(3) If a certification authority holds the private key corresponding to a public key listed in a certificate which it has issued, the certification authority holds the private key as a fiduciary of the subscriber named in the certificate, and may use that private key only with the subscriber's prior, written approval, unless the subscriber expressly grants the private key to the certification authority and expressly permits the certification authority to hold the private key according to other terms.

46-3-306 Suspension of a certificate -- Criminal penalty.

(1) (a) Unless the certification authority and the subscriber agree otherwise, the licensed certification authority which issued a certificate which is not a transactional certificate shall suspend the certificate for a period not exceeding 48 hours:

(i) upon request by a person identifying himself as the subscriber named in the certificate, or as a person in a position likely to know of a compromise of the security of a subscriber's private key, such as an agent, business associate, employee, or member of the immediate family of the subscriber; or

(ii) by order of the division pursuant to Subsection 46-3-302(5).

(b) The certification authority need not confirm the identity or agency of the person requesting suspension under Subsection (1)(a)(i).

(2) (a) Unless the certificate provides otherwise or the certificate is a transactional certificate, the division, a court clerk, or a county clerk may suspend a certificate issued by a licensed certification authority for a period of 48 hours, if:

(i) a person requests suspension and identifies himself as the subscriber named in the certificate or as an agent, business associate, employee, or member of the immediate family of the subscriber; and

(ii) the requester represents that the certification authority which issued the certificate is unavailable.

(b) The division, court clerk, or county clerk may:

(i) require the person requesting suspension under Subsection (2)(a) to provide evidence, including a statement under oath or affirmation, regarding any information described in Subsection (2)(a); and

(ii) suspend or decline to suspend the certificate in its discretion.

(c) The division, attorney general, or county attorney may investigate suspensions by the division, a court clerk, or a county clerk for possible wrongdoing by persons requesting suspension under Subsection (2)(a).

(3) (a) Immediately upon suspension of a certificate by a licensed certification authority, the licensed certification authority shall publish notice, signed by the licensed certification authority, of the suspension in any repositories specified in the certificate for publication of notice of suspension. If any repository specified in the certificate no longer exists or refuses to accept publication, or is no longer recognized pursuant to Section 46-3-501, the licensed certification authority shall publish the notice in any recognized repository.

(b) If a certificate is suspended by the division, a court clerk, or a county clerk, the division or clerk shall give notice as required in Subsection (3)(a) for a licensed certification authority, provided that the person requesting suspension pays in advance any fee required by a repository for publication of the notice of suspension.

(4) A certification authority shall terminate a suspension initiated by request only:

(a) if the subscriber named in the suspended certificate requests termination of the suspension and the certification authority has confirmed that the person requesting suspension is the subscriber or an agent of the subscriber authorized to terminate the suspension; or

(b) when the certification authority discovers and confirms that the request for the suspension was made without authorization by the subscriber, provided that this subsection does not require the certification authority to confirm a request for suspension.

(5) The contract between a subscriber and a licensed certification authority may limit or preclude requested suspension by the certification authority, or may provide otherwise for termination of a requested suspension. However, if the contract limits or precludes suspension by the division, a court clerk, or a county clerk when the issuing certification authority is unavailable, the limitation or preclusion shall be effective only if notice of the limitation or preclusion is published in the certificate.

(6) A person may not knowingly or intentionally misrepresent to a certification authority his identity or authorization in requesting suspension of a certificate. Violation of this subsection is a class B misdemeanor.

(7) While the certificate is suspended, the subscriber is released from the duty to keep the private key secure pursuant to Subsection 46-3-305(1).

46-3-307 Revocation of a certificate.

(1) A licensed certification authority shall revoke a certificate which it issued, but which is not a transactional certificate, after:

(a) receiving a request for revocation by the subscriber named in the certificate; and

(b) confirming that the person requesting revocation is that subscriber, or is an agent of that subscriber with authority to request the revocation.

(2) A licensed certification authority shall confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and any agency of the person requesting the suspension.

(3) A licensed certification authority shall revoke a certificate which it issued:

(a) upon receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is dead; or

(b) upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

(4) A licensed certification authority may revoke one or more certificates which it issued if the certificates are or become unreliable, regardless of whether the subscriber consents to the revocation.

(5) Immediately upon revocation of a certificate by a licensed certification authority, the licensed certification authority shall publish signed notice of the revocation in any repository specified in the certificate for publication of notice of revocation. If any repository specified in the certificate no longer exists or refuses to accept publication, or is no longer recognized pursuant to Section 46-3-501, the licensed certification authority shall publish the notice in any recognized repository.

(6) A subscriber ceases to certify the information, as provided in Section 46-3-304, and has no further duty to keep the private key secure, as required by Section 46-3-305, in relation to a certificate whose revocation the subscriber has requested, beginning with the earlier of either:

(a) when notice of the revocation is published as required in Subsection (5); or

(b) two business days after the subscriber requests revocation in writing, supplies to the issuing certification authority information reasonably sufficient to confirm the request, and pays any contractually required fee.

(7) Upon notification as required by Subsection (5), a licensed certification authority is discharged of its warranties based on issuance of the revoked certificate and ceases to certify the information, as provided in Section 46-3-303, in relation to the revoked certificate.

46-3-308 Expiration of a certificate.

A certificate shall indicate the date on which it expires. When a certificate expires, the subscriber and certification authority cease to certify the information in the certificate as provided in this chapter and the certification authority is discharged of its duties based on issuance of that certificate.

46-3-309 Recommended reliance limits and liability.

(1) By specifying a recommended reliance limit in a certificate, the issuing certification authority and the accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

(2) Unless a licensed certification authority waives application of this subsection, a licensed certification authority is:

(a) not liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of this chapter;

(b) not liable in excess of the amount specified in the certificate as its recommended reliance limit for either:

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or

(ii) failure to comply with Section 46-3-302 in issuing the certificate;

(c) liable only for direct, compensatory damages in any action to recover a loss due to reliance on the certificate, which damages do not include:

(i) punitive or exemplary damages;

(ii) damages for lost profits, savings, or opportunity; or

(iii) damages for pain or suffering.

46-3-310 Collection based on suitable guaranty.

(1) (a) Notwithstanding any provision in the suitable guaranty to the contrary:

(i) if the suitable guaranty is a surety bond, a person may recover from the surety the full amount of a qualified right to payment against the principal named in the bond, or, if there is more than one such qualified right to payment during the term of the bond, a ratable share, up to a maximum total liability of the surety equal to the amount of the bond; or

(ii) if the suitable guaranty is a letter of credit, a person may recover from the issuing financial institution the full amount of a qualified right to payment against the customer named in the letter of credit, or, if there is more than one qualified right to payment during the term of the letter of credit, a ratable share, up to a maximum total liability of the issuer equal to the amount of the credit.

(b) Claimants may recover successively on the same suitable guaranty, provided that the total liability on the suitable guaranty to all persons making claims based upon

qualified rights of payment during its term may not exceed the amount of the suitable guaranty.

(2) In addition to recovering the amount of a qualified right to payment, a claimant may recover from the proceeds of the guaranty, until depleted, reasonable attorney fees and court costs incurred by the claimant in collecting the claim, provided that the total liability on the suitable guaranty to all persons making claims based upon qualified rights of payment or recovering attorney fees and court costs during its term may not exceed the amount of the suitable guaranty.

(3) To recover a qualified right to payment against a surety or issuer of a suitable guaranty, the claimant shall file written notice of the claim with the division stating the name and address of the claimant, the amount claimed, and the grounds for the qualified right to payment, and any other information required by rule of the division.

(4) Recovery of a qualified right to payment from the proceeds of the suitable guaranty shall be forever barred unless:

(a) the claimant substantially complies with Subsection (3); and

(b) notice of the claim is filed within two years after the occurrence of the violation of this chapter which is the basis for the claim.

46-3-401 Satisfaction of signature requirements.

(1) Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature if:

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(b) that digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient has no knowledge or notice that the signer either:

(i) breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature.

(2) Nothing in this chapter precludes any symbol from being valid as a signature under other applicable law, including Uniform Commercial Code, Subsection 70A-1-201(39).

(3) This section does not limit the authority of the State Tax Commission to prescribe the form of tax returns or other documents filed with the State Tax Commission.

46-3-402 Unreliable digital signatures.

Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances. If the recipient determines not to rely on a digital signature pursuant to this section, the recipient shall promptly notify the signer of its determination not to rely on the digital signature.

46-3-403 Digitally signed document is written.

(1) A message is as valid, enforceable, and effective as if it had been written on paper, if it:

(a) bears in its entirety a digital signature; and

(b) that digital signature is verified by the public key listed in a certificate which:

(i) was issued by a licensed certification authority; and

(ii) was valid at the time the digital signature was created.

(2) Nothing in this chapter precludes any message, document, or record from being considered written or in writing under other applicable state law.

46-3-404 Digitally signed originals.

A copy of a digitally signed message is as effective, valid, and enforceable as the original of the message, unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, effective, and enforceable message.

46-3-405 Certificate as an acknowledgment.

Unless otherwise provided by law or contract, a certificate issued by a licensed certification authority is an acknowledgment of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature or whether the signer physically appeared before the certification authority when the digital signature was created, if that digital signature is:

(1) verifiable by that certificate; and

(2) affixed when that certificate was valid.

46-3-406 Presumptions in adjudicating disputes.

In adjudicating a dispute involving a digital signature, a court of this state shall presume that:

(1) a certificate digitally signed by a licensed certification authority and either published in a recognized repository or made available by the issuing certification authority or by the subscriber listed in the certificate is issued by the certification authority which digitally signed it and is accepted by the subscriber listed in it;

(2) the information listed in a valid certificate, as defined in Section 46-3-103, and confirmed by a licensed certification authority issuing the certificate is accurate;

(3) if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:

(a) that the digital signature is the digital signature of the subscriber listed in that certificate;

(b) that the digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient of that digital signature has no knowledge or notice that the signer:

(i) breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature; and

(4) a digital signature was created before it was time stamped by a disinterested person utilizing a trustworthy system.

46-3-501 Recognition of repositories.

(1) A repository may apply to the division for recognition by filing a written request and providing evidence to the division that the repository meets the requirements of Subsection (2). The division shall determine whether to grant or deny the request in the manner provided for adjudicative proceedings in Title 63, Chapter 46b, Administrative Procedures Act.

(2) The division shall recognize a repository, after finding that the repository:

(a) is operated under the direction of a licensed certification authority;

(b) includes a database containing:

(i) certificates published in the repository;

(ii) notices of suspended or revoked certificates published by licensed certification authorities or other persons suspending or revoking certificates as provided in Sections 46-3-306 and 46-3-307;

(iii) certification authority disclosure records for licensed certification authorities;

(iv) all orders or advisory statements published by the division in regulating certification authorities; and

(v) other information as determined by rule of the division;

(c) operates by means of a trustworthy system;

(d) contains no significant amount of information which the division finds is known or likely to be untrue, inaccurate, or not reasonably reliable;

(e) contains certificates published by certification authorities required to conform to rules of practice which the division finds to be substantially similar to, or more stringent toward the certification authorities, than those of this state;

(f) keeps an archive of certificates that have been suspended or revoked, or that have expired within at least the past three years; and

(g) complies with other requirements prescribed by rule of the division.

(3) The division's recognition of a repository may be discontinued upon the repository's written request for discontinuance filed with the division at least 30 days before discontinuance.

(4) The division may discontinue recognition of a repository:

(a) upon passage of an expiration date specified by the division in granting recognition; or

(b) in accordance with the procedures for adjudicative proceedings prescribed by Title 63, Chapter 46b, Administrative Procedures Act, if the division concludes that the repository no longer satisfies the conditions for recognition listed in this section or in rules of the division.

46-3-502 Liability of repositories.

(1) Notwithstanding any disclaimer by the repository or any contract to the contrary between the repository, a certification authority, or a subscriber, a repository is liable for a loss incurred by a person reasonably relying on a digital signature verified by the public key listed in a suspended or revoked certificate if:

(a) the loss was incurred more than one business day after receipt by the repository of a request to publish notice of the suspension or revocation; and

(b) the repository had failed to publish the notice of suspension or revocation when the person relied on the digital signature.

(2) Unless waived, a recognized repository or the owner or operator of a recognized repository is:

(a) not liable:

(i) for failure to publish notice of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;

(ii) for any damages pursuant to Subsection (1) in excess of the amount specified in the certificate as the recommended reliance limit;

(iii) for misrepresentation in a certificate published by a licensed certification authority;

(iv) for accurately recording or reporting information which a licensed certification authority, the division, a county clerk, or court clerk has published as provided in this chapter, including information about suspension or revocation of a certificate; or

(v) for reporting information about a certification authority, a certificate, or a subscriber, if such information is published as provided in this chapter or a rule of the division, or is published by order of the division in the performance of its licensing and regulatory duties pursuant to this chapter; and

(b) liable pursuant to Subsection (1) only for direct compensatory damages, which do not include:

(i) punitive or exemplary damages;

(ii) damages for lost profits, savings, or opportunity; or

(iii) damages for pain or suffering.

46-3-504 Exemptions.

(1) The following governmental entity records are exempt from Title 63, Chapter 2, Government Records Access and Management Act:

(a) records containing information that would disclose, or might lead to the disclosure of private keys, asymmetric cryptosystems, or algorithms; or

(b) records, the disclosure of which might jeopardize the security of an issued certificate or a certificate to be issued.

(2) For purposes of this section, "record" has the meaning described in Section 63-2-103.

Utah Digital Signature Administrative Rules
R154 Commerce, Corporations and Commercial Code

R154-10. Utah Digital Signature Act Rules.

R154-10-100. Authority and Purpose.

These rules are adopted by the division under the authority of Subsection 46-3-102(4), to enable the division to facilitate the implementation of the Utah Digital Signature Act.

R154-10-101. Definitions.
For purposes of these rules, in addition to the definitions set forth in Section 46-3-103, the following terms are herein defined:

(1) "Distinguished name" means data unambiguously identifying the person or entity bearing the name.

(2) "ISO" means the International Organization for Standardization.

(3) "Primary certification practice statement" means a certification practice statement which includes references to all other material certification practice statements.

(4) "Utah Act" means the Utah Digital Signature Act as found in Section 46-3-101 et-seq.

(5) "Working Capital" means the difference obtained by subtracting current liabilities from current assets.

R154-10-102. Certification Authority Filing Amounts.
A certification authority, upon filing an application for a license, shall pay the following amounts annually:

(1) a $500.00 filing fee; and

(2) additional costs that reflect expenses incurred to evaluate software and hardware systems if they have not been previously approved by the division. Additional amount(s) shall be paid when the actual cost is incurred by the division to have an information systems consultant evaluate whether the software and hardware systems utilized by the certification authority are trustworthy systems and meet prevailing national and international standards.

R154-10-201. Amount and Form of Suitable Guaranty.

(1) A suitable guaranty shall be in an amount of seventy-five thousand dollars ($75,000.00);

(2) The suitable guaranty shall specify a term of one (1) year commencing on the effective date of the certification authority license and terminating upon the expiration, revocation or termination of the license; and

(3) The suitable guaranty shall provide coverage for a claim made against a certification authority where:

(a) the claimed violation occurred within the period that the certification authority license was in effect; and

(b) the claimant filed a written notice of the claim with the division within two (2) years following the occurrence of the incident that gave rise to the claim.

R154-10-202. Certification Authority Disclosure Records.

(1) A certification authority disclosure record shall contain:

(a) an indication that the certification authority disclosure record is provided and maintained by this state;

(b) the name, street address, and voice telephone number of the certification authority;

(c) the telephone number of the certification authority's facsimile transmission machine, if the certification authority has such a machine;

(d) the electronic mail or other address by which the certification authority may be contacted electronically;

(e) the distinguished name of the certification authority;

(f) the current public key or keys of the certification authority by which its digital signatures on published certificates may be verified;

(g) the restrictions, if any, placed on the certification authority's license pursuant to Subsection 46-3-201(3);

(h) if the certification authority's license has been revoked or is currently suspended, the date of revocation or suspension, and the grounds for revocation or suspension;

(i) the amount of the certification authority's suitable guaranty, to be updated periodically, as specified by the Division;

(j) the total amount of all claims filed with the Division for payment from the suitable guaranty filed by the certification authority, to be updated periodically, as specified by the Division;

(k) a brief description of any limit known to the Division and applicable to the certification authority's liability or legal capacity to pay damages in tort, or for breach of a duty prescribed in this chapter, unless the limitation is specified in this chapter;

(l) the categorization pursuant to Subsection 46-3-202(2) of the certification authority's compliance with this chapter and resulting from the most recent performance audit of the certification authority's activities, and the date of the most recent performance audit;

(m) any event which substantially affects the certification authority's ability to conduct its business or the validity of a certificate published in the repository provided by the Division or in a recognized repository;

(n) if a certificate containing the public key required to verify one or more certificates issued by the certification authority has been revoked or is currently suspended, the date of its revocation or suspension; and

(o) if the certification authority has a material, primary certification practice statement, indications of its location, the method or procedure by which it may be retrieved, its form and structure, its authorship, and its date, as prescribed in rule 302.

(2) A certification authority disclosure record shall be digitally signed by the Division in its official capacity.

(3) Certification authority disclosure records are public records of the state of Utah pursuant to the Utah Government Records Access and Management Act, Chapter 2 of Title 63.

(4) The contents of the certification disclosure record shall be in a form and method specified by the Division.

R154-10-203. Certification Authority Proof of Sufficient Working Capital.

A certification authority, upon filing an application for a license, shall provide the division with a written acknowledgment stating the following:

(1) that the certification authority has working capital reasonably sufficient to conduct business as a certification authority for a period of one year; and

(2) that the certification authority has no less than $5,000.00 in working capital.

R154-10-301. Certificate Content and Form.

(1) A certificate, other than a transactional certificate, issued by a licensed certification authority shall contain or incorporate by reference:

(a) an indication that the form and type of the certificate is in accordance with this rule;

(b) an indication that the certification authority issuing the certificate is licensed by this state;

(c) the serial number of the certificate, which must be unique among the certificates issued by the certification authority;

(d) the name by which the subscriber is generally known;

(e) the distinguished name of the subscriber;

(f) a public key corresponding to a private key held by the subscriber;

(g) an identifier of the algorithms with which the subscriber's public key was intended to be used;

(h) the date and time on which the certificate was both issued and accepted;

(i) the date and time on which the certificate expires;

(j) the distinguished name of the certification authority issuing the certificate;

(k) an identifier of the algorithm(s) used to sign the certificate, in the form generally accepted in the subscriber's industry;

(l) the recommended reliance limit for the certificate;

(m) either the distinguished name of one or more repositories designated for publication of notice of revocation or suspension, or a specification of the method by which notice of revocation or suspension is to be given pursuant to Subsections 46-3-306(3) and 46-3-307(5);

(n) if a primary certification practice statement applies to the certificate, an indication of its location, the method or procedure by which it may be retrieved, its form and structure, its authorship, and its date as prescribed in Section R154-10-302.

(2) A transactional certificate shall substantially comply with these requirements, and may include additional data.

(3) A certificate issued by a licensed certification authority may, at the option of the subscriber and certification authority, contain or incorporate by reference additional information as determined by the licensed certification authority.

(4) The data in a certificate shall be specified in the form generally accepted for the transactions for which the subscriber expects that the certificate will be used. Further, unless another form is generally accepted for such transactions:

(a) the certificate shall be in the form specified by standard X.509v.3 of the International Telecommunication Union.

(5) The contents of the certificate shall be in a form and method specified by the Division.

R154-10-302. Form of Certification Practice Statement.

(1) If a certificate indicates or incorporates a certification practice statement by reference, or if a certification authority disclosure record refers to a primary certification practice statement, the certificate or certification authority disclosure record shall provide

the following information in the form prescribed in Sections R154-10-301 and R154-10-302, and Section R154-10-202:

(a) the location of the certification practice statement, in the form of a Universal Resource Locator or by another form generally accepted for the transactions in which the subscriber expects the certificate to be used;

(b) the method or procedure by which the certification practice statement may be retrieved or by another form generally accepted for the transactions in which the subscriber expects the certificate to be used;

(c) the form and structure of the certification practice statement, which shall be either the form recommended in subsection (2) of this rule, in the Hypertext Markup Language version 2.0, or in the form generally accepted for the transactions in which the subscriber expects the certificate to be used;

(d) the authorship of the certification practice statement, either in the form recommended in subsection (2) of this rule, or in a form generally accepted in the transactions for which the subscriber expects that the certificate will be used; and

(e) its date, either in the form recommended in subsection (2) of this rule or in a form generally accepted in the transactions for which the subscriber expects that the certificate will be used.

(2) Unless the certificate of certification authority disclosure record clearly indicates otherwise and another form is generally accepted in the transactions for which the subscriber expects that the certificate will be used, a certification practice statement shall be in the form of a document marked in accordance with the Standard Generalized Markup Language, ISO standard 8879 (1986, as amended 1988), or in a form and method specified by the Division.

R154-10-303. Record-keeping by Certification Authorities.

(1) A licensed certification authority shall maintain documentation of compliance with the Utah Act. The documentation shall include evidence demonstrating that the certification authority has:

(a) accepted as evidence of identity such identification documents or other evidence presented by the person or entity named in a certificate that the certification authority has issued; confirmed identification of the person or entity named in a certificate that the certification authority has issued;

(b) accepted as evidence of identity such identification documents or other evidence presented by the person or entity requesting revocation of each certificate that the certification authority has revoked;

(c) evidence collected by the certification authority pertaining to the validity of all other facts listed in a certificate which the certification authority has issued; and

(d) complied with the Utah Act in issuing, publishing, suspending, and revoking a certificate.

(2) Identification of the person or entity named in a certificate shall be presumed to be established where a licensed certification authority has been presented identification documents consisting of at least one of the following:

(a) an identification document issued by or under the authority of the United States, or such similar identification document issued under the authority of another country;

(b) a birth certificate issued in the United States;

(c) a driver's license issued by a State of the United States; or

(d) a personal identification card issued by a State of the United States.

(3) Other forms of identification documents may be substituted for those listed in paragraph (2) above upon written approval of the division prior to the issuance of the certificate or class of certificates.

(4) Except for requests for suspension of a certificate, the licensed certification authority may require a subscriber or agent of a subscriber to submit documentation and other evidence reasonably sufficient to enable the certification authority to comply with this section.

(5) A licensed certification authority shall retain its records of the issuance, acceptance, and any suspension or revocation of a certificate for a period of not less than ten years after the certificate is revoked or expires. The licensed certification authority shall itself retain custody of such records, unless the licensed certification authority turns over its records to the Division or another licensed certification authority upon ceasing to act as a certification authority.

(6) A licensed certification authority shall keep its records under circumstances of safekeeping and security which are commercially reasonable in light of the recommended reliance limits of the certificates.

(7) The contents of the records shall be in a form and method specified by the Division.

(8) All required information filed with the Division by the certification authority shall be in the English language.

(9) Documentation of all evidence and records required to be maintained by a licensed certification authority may be maintained in an electronic format approved by the Division.

R154-10-304. Cessation of Certification Authority Activities.

(1) Before ceasing to act as a certification authority, a licensed certification authority shall:

(a) give to the subscriber of each unrevoked or unexpired certificate issued by the certification authority at least 90 days written notice of the certification authority's intention to discontinue acting as a certification authority;

(b) 90 days or more after the notice required in Subsection (1)(a) of this section, revoke all certificates which then remain unrevoked or unexpired, regardless of whether the subscriber has requested revocation;

(c) give written notice of revocation to the subscriber of each certificate revoked pursuant to subsection (1)(b) of this section; and

(d) unless a contract between the certification authority and the subscriber provides otherwise, pay reasonable restitution to the subscriber for revoking the certificate before its expiration date.

(2) To provide uninterrupted certification authority services, the discontinuing certification authority may arrange with another certification authority for reissuance of the remaining certificates without charge, except as provided below for certification practice statements, or unless the subscriber of a certificate agrees to a charge. The

succeeding certification authority shall create its own digital signature on all reissued certificates. In reissuing a certificate pursuant to this subsection:

(a) the succeeding certification authority becomes subrogated to the rights and defenses of the discontinuing certification authority; and

(b) unless the contract between the discontinuing certification authority and the subscriber provides otherwise, all certification practice statements of the discontinuing certification authority continue in effect under the new certification authority, unless the new certification authority gives sixty days' notice of the changes to be made in the applicable certification practice statements.

(3) The requirements of this section may be varied by contract, except that the contract shall not permit the licensed certification authority to discontinue its certification authority activities without first giving each subscriber of an unexpired or unrevoked certificate at least ten days written notice, or without revoking all outstanding certificates upon cessation of certification authority activities.

(4) Before ceasing to act as a certification authority, a licensed certification authority shall notify the Division of its intention to cease acting as a certification authority. The written notice shall be filed with the Division at least two months, but not more than six months, before the certification authority ceases to act as a certification authority. Further, the written notice shall be entitled "Notice of Intention to Discontinue Certification Authority Business" and include the following information:

(a) name of certification authority;

(b) distinguished name of withdrawing certification authority;

(c) number of certificates issued and currently valid;

(d) date on which the certification authority intends to discontinue business;

(e) date on which notice will be given to subscribers of issued and valid certificates (append copy of notice to subscribers);

(f) indicate whether the withdrawing certification authority will be succeeded by another licensed certification authority;

(g) name of succeeding certification authority, if any;

(h) distinguished name of succeeding certification authority, if any;

(5) If a certification authority dies while licensed, the estate of the certification authority shall comply with the procedures of this section or any applicable contract for termination of the deceased certification authority's activities. If a certification authority becomes incapacitated within the meaning of Subsection 75-1-201(18), a court may either appoint a guardian as provided in the Utah Uniform Probate Code article 5, part 3, or, on the petition of an interested party, appoint a receiver to terminate the incapacitated certification authority's business as required by this section.

R154-10-401. Recognition of Repositories.

(1) For a repository to be recognized as provided in Section 46-3-501, the licensed certification authority operating the repository shall file with the Division a request which:

(a) states the full name, postal mailing address, address for service of process, physical location of hardware containing the repository, telephone number, electronic mail address, and distinguished name of the person or entity filing the application;

(b) states the full name, address, telephone number, electronic mail address, and distinguished name of the licensed certification authority under whose direction the repository is operated;

(c) describes in detail, noting compliance with any applicable technical standards:

(i) the design and implementation of the repository's trustworthy system;

(ii) the contents of the repository;

(iii) all form requirements applicable to contents of the repository;

(iv) the criteria for determining who may publish information in the repository;

(v) procedures for processing newly published certificates and notices of suspension and revocation;

(vi) processes to account for usage of the repository and access to the information published in it; and

(vii) fees to be charged, if any for access to certification authority disclosure records and orders or advisory statements issued by the Division, if recognition is granted.

(d) promises, if recognition is granted, to effect prompt publication of:

(i) all certification authority disclosure records published in the repository by the Division;

(ii) all updates or cancellations of existing certification authority disclosure records published in the repository by the Division;

(iii) all orders or advisory statements published in the repository by the Division.

(e) includes a copy of all applicable certification practice statements of the repository and the repository's archival policy. However, nothing in this section requires a repository to disclose trade secrets or information that could adversely affect the security of the trustworthy system.

(f) acknowledges that the licensed certification authority operating the repository has and will continuously maintain in this state:

(i) an office or a registered agent who is either an individual resident in this state, a domestic corporation, or a foreign corporation authorized to transact business in this state; and

(ii) a custodian of the data and records of the repository (regardless of whether the hardware containing the repository is located outside of the State of Utah), upon whom any process, notice, or demand required or permitted by law may be served. The custodian of the records may be the same person or entity as the registered agent.

(g) states the full name, address, telephone number, electronic mail address and address for service of process of the agent and the custodian referred to in the preceding subsection;

(h) acknowledges that the licensed certification authority operating the repository submits the repository data to all lawful process, notice, demand, and orders issued by the State of Utah and its political subdivisions;

(i) the licensed certification authority operating the repository shall promptly notify the Division of any changes in the information required by this rule.

(2) The Division will proceed in the manner provided for formal adjudicative proceedings in the Utah Administrative Procedures Act, title 63, chapter 46b, to review the request for recognition and the evidence supporting it, unless:

(a) the request is to renew recognition;

(b) the request is filed within three months of the date on which recognition is scheduled to expire; and

(c) the Division determines in light of the repository's prior record of service and performance that a hearing is not necessary.

(3) The Division hereby delegates to each recognized repository all privileges held by the Division at common law with respect to the publication of certification authority disclosure records and the orders or advisory statements of the Division.

R154-10-402. Qualification of Auditors.

(1) An Auditor performing an audit of a licensed certification authority, as provided in Subsection 46-3-202(1), shall have the following qualifications:

(a) be a licensed certified public accountant (CPA) in good standing;

(b) have knowledge of trusted computer information systems, trusted telecommunications networking environments, and the professional audit techniques to test these systems; and

(c) have knowledge of digital signature technology, standards and practices.

(2) The Auditor performing an audit of a licensed certification authority, upon the filing of audit results, shall provide the division with an affirmative statement that auditor meets the foregoing requirements.

R154-10-501. Waiver of Requirements.

(1) The division will duly consider requests to waive any requirement of this rule if conflicts arise in implementation of these standards and procedures.

Utah Certification Authority License

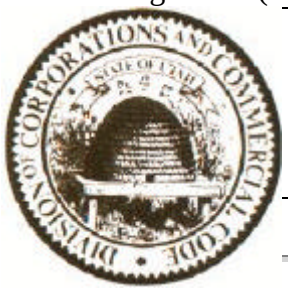
Utah Department of Commerce, Division of Corporations and Commercial Code hereby licenses

Digital Signature Trust Co.

as a licensed certification authority pursuant to the Utah Digital Signature Act, Utah Code Annotated title 46, chapter 3 (1996).

This license takes effect beginning 1997 Nov 13 00:00:00 GMT and expires 1998 May 13 00:00:00 GMT, unless it is sooner revoked by posting notice in the certificate revocation list (CRL) in the manner described for the certification authority disclosure record appended below. Further provisions applicable to this license appear in the certification authority disclosure record appended below.

IN WITNESS WHEREOF, Utah Department of Commerce has affixed its digital signature to this document as a certificate of the license hereby granted on this date, 1997 Nov 13 00:00:00 GMT, using the Secure Hash Algorithm 1 with the RSA signing algorithm (object identifier of algorithm: "id-sha1-with-rsa-signature").



Korla T. Woods
Director, Division of Corporations and Commercial Code
Kenneth Allen
Digital Signature Coordinator
License Number: 101

Certification Authority Disclosure Record

Utah Department of Commerce, Division of Corporations and Commercial Code hereby provides, maintains, and publishes the following Certification Authority Disclosure Record regarding Digital Signature Trust Co. (the "licensee") as of this date, 1997 Nov 13 00:00:00 GMT, pursuant to section 46-3-104(2) of the Utah Digital Signature Act (1996).

1. **Licensee's Distinguished Name and Street Address**. The licensee is currently identified on the records of Utah Department of Commerce by the following distinguished name and street address:

   Organization name: Digital Signature Trust Co.

   Country name: us

   Contact person (common name): Digital Signature Trust Co. - Reliance Standard Basic

2. **Licensee's Electronic Addresses**. The licensee is currently identified on the Internet by the following:

   URI: A uniform resource identifier (or locator or URL) of "michelle.jolicoeur@digsigtrust.com" for use on the Worldwide Web.

3. **Licensee's Public Key**. Utah Department of Commerce has confirmed that a certificate has been issued by a licensed certification authority listing the licensee as its subscriber and indicating according to its terms that the licensee holds that certain private key which corresponds to the public key equal to the following number expressed in hexadecimal (base 16) form:

   30818902818100C0E32A548B3003A66B76A2453EC6F654F58C
   2528C2E07D13D7DE642282D1DD73B70E6ACB6BB24684B8C
   5414B6BE54C9D170BCDCB413D904972CF2011211E8CAB85
   C6679D9304AD93D523229A07530CD4B77A181982A94383EB
   7A2E894E5C0A48E8C9152A30CD95E9A151C8D2EEF2F4B023
   92 AC87FAFA2CDC5A783E8FF4824C690203010001

   However, Utah Department of Commerce has not itself confirmed that the licensee holds that private key, but rather relies upon the aforementioned certificate of the licensed certification authority to provide that confirmation. That certificate also provides that the aforementioned public key is for use with the RSA Encryption for digital signature purposes (object identifier of algorithm: "rsaEncryption").

4. **Version**. The condensed form of this license is a certificate conforming to version 3 of ITU X.509 (draft dated June 1997). (Technically, this version is indicated by a numeral "2" in the concise form of the certificate because ITU X.509 specifies that version counting start at zero.)

5. **Revocation**. This certification authority disclosure record and the foregoing license can both be revoked by posting notice of revocation in the certificate revocation list issued by Utah Department of Commerce and posted at

http://www.digsigtrust.com/crl/utahdcmrc, or in any other form as determined by the Utah Department of Commerce. This certification authority disclosure record is deemed revoked if the foregoing license is revoked. This record and the foregoing license are of no further effect after they are revoked.

6. **Timing of Statements and Accuracy Over Time**. Unless otherwise expressly noted, all statements and representations in this record are made as of 1997 Nov 13 00:00:00 GMT. Utah Department of Commerce does not conduct a constant, on-going investigation sufficient to determine if any of the statements made in this record becomes inaccurate after this record is issued. Consequently, events could occur between 1997 Nov 13 00:00:00 GMT and the time when a user relies on this record, and those events could render the statements or representations in this record no longer accurate. Users are advised to obtain updated information from primary sources as needed.
7. **Further Information about Utah Department of Commerce**. Utah Department of Commerce is currently further identified by the following names and addresses:
    - **Distinguished Name**. Utah Department of Commerce is currently identified by the distinguished name of:

      Organization name: State of Utah
      Organizational unit name: Department of Commerce
      Country name: us
      Contact person (common name): Licensing CA

    - **Electronic Addresses of Utah Department of Commerce**. The Utah Department of Commerce is currently accessible via the Internet by the following:

      E-mail address: An Internet e-mail (electronic mail) address of "brsec.kallen@email.state.ut.us".
      URI: A uniform resource identifier (or locator) of "http://www.commerce.state.ut.us" for use on the WorldWide Web.
8. **Date Format**. Dates in this record and the foregoing license appear in the form exemplified by the following: "97 Nov 24 12:34:52 GMT". In that example, "97" indicates the year, "Nov" the month, "24" the day, "12" the hour (using a 24-hour clock), "34" the minutes after the hour, and "52" the seconds after the minute. "GMT" stands for "Greenwich mean time".
9. **Jurisdication and Choice of Law**. This record is issued by Utah Department of Commerce, an administrative agency of the state of Utah, the United States of America. Accordingly the substantive law of the state of Utah will govern the interpretation of this certificate and all issues regarding it and the authority of Utah Department of Commerce. Furthermore, the courts of the state of Utah will have exclusive jurisdiction over all claims and issues arising under or related to the foregoing certificate of license, this certification authority disclosure record, and the authority of Utah Department of Commerce.

10. **Effect of ITU X.509 and Technical Standards**. The concise form of this record conforms to the form specified in ITU X.509 and similar standards, which have been formulated for the technological interchange of defined fields of information. Such standards prescribe the structure and format of the concise form of this and similar digital records and the methods for transmitting and making them available. The concise form of this record fully complies with those standards in those respects. In relation to the commercial, business, and legal significance of a document, standards such as ITU X.509 leave room for interpretation and elaboration in specific applications and implementations. For that reason, should any discrepancy exist between this document (including this full-text form of this record) and ITU X.509 or any other technological standard, this full-text form shall take precedence.
11. **Formatting Variance Insignificant**. This document is designed for use in WorldWide Web browsers and similar technology reading and interpreting the HyperText Markup Language (HTML). Variations, usually minor ones, can occur in the appearance and format of HTML documents shown in different browsers, depending on the browser manufacturer's implementation of HTML, the browser user's preferences, and similar facts not material to the meaning and significance of this document. In interpreting this document, such variations in the presentation of HTML code are insignificant, and all representations of HTML in any browser or other software product conforming to HTML standards and/or common industry usage are to be considered equivalent.
12. **Form Identifier**. This is full-text certificate form http://www.digsigtrust.com/ftc/dstlicense.htm, version 1.
13. **Inquiries**. All inquiries or comments regarding this record may be directed to Utah Department of Commerce at the addresses listed above or at telephone number +1801 530-6026.
14. **Definitions**. For purposes of this record, terms have the meanings indicated in the Utah Digital Signature Act and administrative rules pursuant to it.

IN WITNESS of this document, Utah Department of Commerce has digitally signed it using the Secure Hash Algorithm 1 with the RSA signing algorithm (object identifier of algorithm: "id-sha1-with-rsa-signature").

Utah Department of Commerce, Division of Corporations and Commercial Code.

California Government Code Section 16.5 Digital Signature

(a) In any written communication with a public entity, as defined in Section 811.2, in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this section. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:

(1) It is unique to the person using it.

(2) It is capable of verification.

(3) It is under the sole control of the person using it.

(4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.

(5) It conforms to regulations adopted by the Secretary of State. Initial regulations shall be adopted no later than January 1, 1997. In developing these regulations, the secretary shall seek the advice of public and private entities, including, but not limited to, the Department of Information Technology, the California Environmental Protection Agency, and the Department of General Services. Before the secretary adopts the regulations, he or she shall hold at least one public hearing to receive comments.

(b) The use or acceptance of a digital signature shall be at the option of the parties. Nothing in this section shall require a public entity to use or permit the use of a digital signature.

(c) Digital signatures employed pursuant to Section 71066 of the Public Resources Code are exempted from this section.

(d) "Digital signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.

Final Draft of California Digital Signature Regulations

California Administrative Code

Title 2. Administration

DIVISION 7. SECRETARY OF STATE
Table of Contents
CHAPTER 10. DIGITAL SIGNATURES

Section 22000 Definitions

Section 22001 Digital Signatures Must Be Created By an Acceptable Technology

Section 22000. Definitions

a. For purposes of this chapter, and unless the context expressly indicates otherwise:

1. "Digitally-signed communication" is a message that has been processed by a computer in such a manner that ties the message to the individual that signed the message.

2. "Message" means a digital representation of information intended to serve as a written communication with a public entity.

3. "Person" means a human being or any organization capable of signing a document, either legally or as a matter of fact.

4. "Public entity" means the public entity as defined by California Government Code Section 811.2.

5. "Signer" means the person who signs a digitally signed communication with the use of an acceptable technology to uniquely link the message with the person sending it.

6. "Technology" means the computer hardware and/or software-based method or process used to create digital signatures.

22001. Digital Signatures Must Be Created By An Acceptable Technology

a. For a digital signature to be valid for use by a public entity, it must be created by a technology that is accepted for use by the State of California.

22002. Criteria for State to Determine if a Digital Signature Technology is Acceptable for Use By Public Entities

a. An acceptable technology must be capable of creating signatures that conform to requirements set forth in California Government Code Section 16.5, specifically,

1. It is unique to the person using it;

2. It is capable of verification;

3. It is under the sole control of the person using it;

4. It is linked to data in such a manner that if the data are changed, the digital signature is invalidated;

5. It conforms to Title 2. Division 7. Chapter 10 of the California Code of Regulations.

22003. List of Acceptable Technologies

a. The technology known as Public Key Cryptography is an acceptable technology for use by public entities in California, provided that the digital signature is created consistent with the provisions in Section 22003(a)(1)-(5).

1. Definitions — For purposes of Section 22003(a), and unless the context expressly indicates otherwise:

A. "Acceptable Certification Authorities" means a certification authority that meets the requirements of either Section 22003(a)(6)(C) or Section 22003(a)(6)(D).

B. "Approved List of Certification Authorities" means the list of Certification Authorities approved by the Department of Information Technology to issue certificates for digital signature transactions involving public entities in California.

C. "Asymmetric cryptosystem" means a computer algorithm or series of algorithms which utilize two different keys with the following characteristics:

i. one key signs a given message;

ii. one key verifies a given message; and,

iii. the keys have the property that, knowing one key, it is computationally infeasible to discover the other key.

D. "Certificate" means a computer-based record which:

i. identifies the certification authority issuing it;

ii. names or identifies its subscriber;

iii. contains the subscriber's public key; and

iv. is digitally signed by the certification authority issuing or amending it, and

v. conforms to widely-used standards.

E. "Certification Authority" means a person or entity that issues a certificate, or in the case of certain certification processes, certifies amendments to an existing certificate.

F. "Key pair" means a private key and its corresponding public key in an asymmetric cryptosystem. The keys have the property that the public key can verify a digital signature that the private key creates.

G. "Practice statement" means documentation of the practices, procedures and controls employed by a Certification Authority.

H. "Private key" means the key of a key pair used to create a digital signature.

I. "Proof of Identification" means the document or documents presented to a Certification Authority to establish the identity of a subscriber.

J. "Public key" means the key of a key pair used to verify a digital signature.

K. "Subscriber" means a person who:

i. is the subject listed in a certificate;

ii. accepts the certificate; and

iii. holds a private key which corresponds to a public key listed in that certificate.

2. California Government Code §16.5 requires that a digital signature be ‘unique to the person using it’. A public key-based digital signature may be considered unique to the person using it, if:

A. the private key used to create the signature on the document is known only to the signer, and

B. the digital signature is created when a person runs a message through a one-way function, creating a message digest, then encrypting the resulting message digest using an asymmetrical cryptosystem and the signer's private key, and,

C. although not all digitally signed communications will require the signer to obtain a certificate, the signer is capable of being issued a certificate to certify that he or she controls the key pair used to create the signature, and

D. it is computationally infeasible to derive the private key from knowledge of the public key.

3. California Government Code §16.5 requires that a digital signature be 'capable of verification'. A public-key based digital signature is capable of verification if:

A. the acceptor of the digitally signed document can verify the document was digitally signed by using the signer's public key to decrypt the message; and

B. if a certificate is a required component of a transaction with a public agency, the issuing Certification Authority, either through a certification practice statement or through the content of the certificate itself, must identify which, if any, form(s) of identification it required of the signer prior to issuing the certificate.

4. California Government Code §16.5 requires that the digital signature remain 'under the sole control of the person using it'. Whether a signature is accompanied by a certificate or not, the person who holds the key pair, or the subscriber identified in the certificate, assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature.

5. The digital signature must be linked to the message of the document in such a way that if the data are changed, the digital signature is invalidated.

6. Acceptable Certification Authorities

A. The California Department of Information Technology shall maintain an "Approved List of Certificate Authorities" authorized to issue certificates for digitally signed communication with public entities in California.

B. Public entities shall only accept certificates from Certification Authorities that appear on the "Approved List of Certification Authorities" authorized to issue certificates by the California Department of Information Technology.

C. The Department of Information Technology shall place Certification Authorities on the "Approved List of Certification Authorities" after the Certification Authority provides the Department of Information Technology with a copy of an unqualified performance audit performed in accordance with standards set in the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards No. 70 (S.A.S. 70) "Reports on the Processing of Service Transactions by Service Organizations" (1992) to ensure that the Certification Authorities practices and policies are consistent with their stated control objectives. The AICPA Statement on Auditing Standards No. 70 is hereby incorporated by reference.

i. Certification Authorities that have been in operation for one year or less shall undergo a SAS 70 Type One audit — A Report of Policies and Procedures Placed in Operation, receiving an unqualified opinion.

ii. Certification Authorities that have been in operation for longer than one year shall undergo a SAS 70 Type Two audit — A Report Of Policies And

Procedures Placed In Operation And Test Of Operating Effectiveness, receiving an unqualified opinion.

iii. To remain on the "Approved List of Certification Authorities" a Certification Authority must provide proof of compliance with Section 20003(a)(6)(C)(ii) to the Department of Information technology every two years after initially being placed on the list.

D. In lieu of completing the auditing requirement in Section 22003(a)(6)(C), Certification Authorities may be placed on the "Approved List of Certification Authorities" upon providing the Department of Information Technology with proof of accreditation by a national or international accreditation body, acceptable to the Department of Information Technology whose requirements for accreditation are consistent with the requirements of Section 22003(a)(1)-(5).

i. Certification Authorities shall be removed from the "Approved List of Acceptable Certifications Authorities" unless they provide current proof of accreditation to the Department of Information Technology at least once per year.

ii. If the Department of Information Technology is informed that a Certification Authority has had its accreditation revoked, the Certification Authority shall be removed from the "Approved List of Certification Authorities" immediately.

b. The technology known as "Signature Dynamics" is an acceptable technology for use by public entities in California, provided that the signature is created consistent with the provisions in Section 22003(b)(1)-(5).

1. Definitions — For the purposes of Section 22003(b), and unless the context expressly indicates otherwise:

A. "Handwriting Measurements" means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.

B. "Signature Digest" is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.

C. "Expert" means a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert pursuant to California Evidence Code §720.

D. "Signature Dynamics" means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

2. California Government Code §16.5 requires that a digital signature be ‘unique to the person using it’. A signature digest produced by Signature Dynamics technology may be considered unique to the person using it, if:

A. the signature digest records the handwriting measurements of the person signing the document using signature dynamics technology, and

B. the signature digest is cryptographically bound to the handwriting measurements, and

C. after the signature digest has been bound to the handwriting measurements, it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.

3. California Government Code §16.5 requires that a digital signature be capable of verification. A signature digest produced by signature dynamics technology is capable of verification if:

A. the acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison, and

B. if signature verification is a required component of a transaction with a public entity, the handwriting measurements can allow an expert handwriting and document examiner to assess the authenticity of a signature.

4. California Government Code §16.5 requires that a digital signature remain 'under the sole control of the person using it'. A signature digest is under the sole control of the person using it if:

A. the signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message, and

B. the signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.

5. The signature digest produced by signature dynamics technology must be linked to the message in such a way that if the data in the message are changed, the signature digest is invalidated.

22004. Provisions for Adding New Technologies to the List of Acceptable Technologies

a. Any individual or company can, by providing a written request that includes a full explanation of a proposed technology which meets the requirements of Section 22002, petition the California Department of Information Technology to review the technology. If the Department of Information Technology determines that the technology is acceptable for use with the state, they shall draft proposed regulations for the Secretary of State to review and adopt which would add the proposed technology to the list of acceptable technologies in Section 22003.

b. The Department of Information Technology has 180 days from the date of the request to review the petition and either accept or reject it. If the Department of Information Technology does not approve the request within 180 days, the petitioner's request shall be considered denied.

1. If the petitioner's proposed technology meets the requirements of California Government Code § 16.5, the Department of Information Technology shall prepare and submit proposed amendments of Section 22003 to the Secretary of State to reflect the state's acceptance of the new technology for use by public agencies in California.

2. If the proposed technology is rejected, the petitioner can appeal the decision through the Administrative Procedures Act, Government Code Section 11500.

22005. Criteria for Public Entities To Use In Accepting Digital Signatures

a. Prior to accepting a digital signature, public entities shall ensure that the level of security used to identify the signer of a document is sufficient for the transaction being conducted.

b. Prior to accepting a digital signature, public entities shall ensure that the level of security used to transmit the signature is sufficient for the transaction being conducted.

c. If a certificate is a required component of a digital signature transaction, public entities shall ensure that the certificate format used by the signer is sufficient for the security and interoperability needs of the public entity.

Santa Clara County Superior Court Rule 1.7 Electronic Filing and Service

Section 1.7.1 Definitions

A. Service Provider. "Service Provider" means a private sector firm or other business entity authorized by the Court to provide electronic filing services. A Service Provider is contractually obligated to provide specified electronic services to the Bar, the public and the Court, to transfer filings and messages to and from the Court, and to act as Certification Authority.

B. Certification Authority. "Certification Authority" means an entity appointed by the Court, operating under the relevant laws of the State of California or rules of the Judicial Council, and duly licensed (if applicable) to issue and revoke digital key bit sequences (private and public keys of an asymmetric crypto system) used to affix a Digital Signature to an electronic document by a subscriber.

C. Digital Signature. "Digital Signature" means a sequence of bits derived from an electronic document by an algorithm using a digital key assigned to a subscriber by a Certification Authority with the property that the integrity, origin and authenticity of the document to which it is applied can be validated. "Digitally Signed" means the application of a Digital Signature to a document.

Section 1.7.2 Standards

A. Electronic Filing. A party may file an electronic pleading or other paper with the Court provided it has executed an agreement with a Service Provider and Digitally Signs the documents filed electronically. Any papers filed shall include exhibits attached.

B. Enhanced Service; Contractual Requirements. Filing documents electronically is an enhanced service and may be provided by arrangement with one or more Service Providers approved by the Court. Service Providers may require payment of a fee or impose other reasonable requirements by contract with the filing party as conditions for processing electronic documents.

C. Return Notice of Filing. The Court shall return to the sender of an electronic filing a Digitally Signed confirmation of the acceptance or rejection of the filing. The confirmation shall include a notation of the date of filing.

D. Date of Filing. A filing accepted by the Court will be deemed filed on the date of transmission if received during normal business hours of the Court and on the next Court business day otherwise.

E. Electronic Issuance of Summons. A Digitally Signed summons issued via the electronic filing system shall be as valid as a summons issued by the clerk on paper and under the seal of the Court.

F. Original Document. A Digitally Signed electronically filed document as it resides on the Court's computer, and print-outs of said document, shall be considered originals satisfying the best evidence rule (Cal.Ev.Code s 1500). The Court may require the party to produce the original of an exhibit that has been filed electronically.

G. Electronic Service. In circumstances where a document may be served by paper mail or fax, a document may be served electronically via a Service Provider. Service is completed at the time of transmission, and service that occurs after 5 p.m. shall be deemed to have occurred on the next Court day.

H. Facsimile Transfer to Computer File. Filings made pursuant to California Rule of Court 2001 are exempted from this rule.

Delaware Superior Court Rules of Civil Procedure Interim Rule 79.1
Complex Litigation Automated Docket

1. The pilot program shall be known as Complex Litigation Automated Docket for the Superior Court of the State of Delaware and shall be referred to below as CLAD.

2. The following civil actions are assigned to participate in CLAD and shall be bound by this Interim Rule:

ACC Chemical Co. & Getty Chemical Co. v. Fireman's
Fund Insurance Co.
C.A. No. 89C-DE-201 (New Castle)

American Home Products Corp. v. Adriatic Insurance Co.
C.A. No. 91C-04-119 (New Castle)

Burlington Northern Railroad Co. v. Allianz
C.A. No. 90C-JL-108 (New Castle)

Clark Equipment v. Liberty Mutual
C.A. No. 89C-OC-173 (New Castle)

E.I. duPont de Nemours & Co. v. Admiral Insurance Co.
C.A. No. 89C-AU-99 (New Castle)

Hoechst Celanese Corp. v. National Union Fire Insurance Co. of Pittsburgh,
Pennsylvania
C.A. No. 89C-SE-35 (New Castle)

Monsanto Co. v. Aetna Casualty and Surety Co.
C.A. No. 88C-JA-118 (New Castle)

National Union Fire Insurance Co. v. Stauffer Chemical Co.
C.A. No. 87C-SE-11 (New Castle)

North American Philips Corp. v. Aetna Casualty and Surety Co.
C.A. No. 88C-JA-155 (New Castle)

Playtex, Inc. v. Columbia Casualty
C.A. No. 88C-MR-233 (New Castle)

Sequa Corp. v. Aetna Casualty and Surety Co.
C.A. No. 89C-AP-1 (New Castle)

3. Each party in each of the above cases is directed to pay a one-time assessment in the amount of $200.00 for each of the cases in which that party is named for the purposes of establishing the fund necessary to operate CLAD.

4. All assessments shall be made payable to the Complex Litigation Automated Docket for the Superior Court of the State of Delaware and shall be delivered to the Prothonotary no later than July 31, 1991.

5. When the President Judge of the Superior Court determines that it is appropriate for one of the above-assigned cases or for any other civil case to commence participation in CLAD, he shall direct the Judge assigned to that case to issue the following order:

IT IS ORDERED that, effective _____, 199___, all parties shall serve and file all pleadings and other papers with the Court in compliance with Interim Rule 79.1.

_____

Judge

6. The Prothonotary shall establish a procedure for the distribution of passwords to permit access to CLAD. The passwords shall be issued as follows:

(a) Upon request, any member of the Delaware Bar who enters an appearance on behalf of a party shall be issued a password for that specific case for a registration charge of $20.00;

(b) Upon request, any member of the public shall be issued a general non-case-specific password with a registration charge of $50.00 annually.

7. The Prothonotary shall expend the funds solely for the purpose of operating and maintaining CLAD.

8a. No Delaware lawyer shall knowingly permit or cause to permit his/her password to be utilized by anyone other than an employee of his/her law firm.

8b. No person shall knowingly utilize or cause another person to utilize the password of another (1) without permission of the holder of the password, or (2) in violation of this Rule.

9. The utilization of a password for the purposes of filing a pleading shall constitute a signature of the registrant of that password under Superior Court Civil Rule 11.

10. Only members of the Delaware Bar registered as counsel in a given case may file pleadings or other papers in that case on CLAD.

11. The Prothonotary shall establish administrative procedures for the electronic filing of pleadings and other papers. A copy of these procedures will be provided with each case-specific password registered for CLAD.

12. The electronic filing of a pleading or paper will be considered service under Superior Court Civil Rule 5. However, counsel shall be required to serve by hand or fax, on all Delaware counsel appearing in that case and file with the Prothonotary, a notice of service under Rule 5 in the following form:

Please take notice that the following pleading has been electronically filed by (name of party) on the Complex Litigation Automated Docket for the Superior Court of the State of Delaware on _____, 1991: (name of pleading) Signature of Delaware Counsel

13. This Rule does not affect discovery pleadings served under Superior Court Civil Rule 5(d)(1). However, the certificate of service for those pleadings shall be filed electronically.

14. This Rule does not alter the Court's expectation that Delaware counsel will maintain an appropriate familiarity in the proceedings for each case in which counsel is involved.

15. This Interim Rule shall be effective July 1, 1991.

16. An original of this Order shall be filed with the Prothonotary for each county.

Bankruptcy Rules of the U.S. District Courts for the Southern and Eastern Districts Local Rules Appendix G In re: Pilot Program for Complex Litigation Automated Docket, General Order M-134

WHEREAS, the Office of the Clerk has suffered a severe reduction in staffing; and

WHEREAS, under 28 U.S.C. s 156(c), the Court may utilize facilities or services either on or off the Court's premises; and

WHEREAS, under 28 U.S.C. s 156(c), the costs of such services are not charged to the United States; and

WHEREAS, a proposal for a program for establishing electronic filing and service of pleading and papers known as Complex Litigation Automated Docket ("CLAD") has been reviewed, and the Court agrees to the pilot program;

NOW, THEREFORE, IT IS ORDERED that:

1. a. Initially, the following case is assigned to participate in CLAD and shall be bound by this General Order: In re R.H. Macy & Co., Inc., et. al, 92 B 40477 (BRL) (Jointly Administered).

b. The following representatives of Parties in Interest in the above-referenced cases shall (i) participate in the CLAD Bulletin Board Services ("CLAD BBS") for the electronic retrieval and filing of pleadings and other documents in said cases and (ii) be entitled to electronic service of notice of filings:

Weil, Gotshal & Manges
767 Fifth Avenue
New York, NY 10153
Attn: Harvey R. Miller, Esq.
Richard Krasnow, Esq.
Judy G.Z. Liu, Esq.

Kaye, Scholer, Fierman, Hays & Handler
Attorneys for the 49 Stores Bank Syndicate
425 Park Avenue
New York, NY 10022
Attn: Michael Crames, Esq.
Arthur Steinberg, Esq.

Zalkin, Rodin & Goodman
Attorneys for Chemical Bank
750 Third Avenue
New York, NY 10022
Attn: Richard S. Toder, Esq.

O'Melveny & Myers
153 East 53rd Street
New York, NY 10022
Attn: Joel B. Zweibel, Esq.

Berlack, Israels & Liberman
120 West 45th Street
New York, NY 10036
Attn: Robert Miller, Esq.
Bari J. Mattes, Esq.

Stroock, Stroock & Lavan
7 Hanover Square
New York, NY 10004
Attn: Daniel H. Golden, Esq.
Lisa Beckerman, Esq.
Otterbourg, Steindler, Houston & Rosen, P.C.
230 Park Avenue
New York, NY 10169
Attn: Scott L. Hazan, Esq.
Glenn B. Rice, Esq.
Enid Stuart, Esq.
Brett H. Miller, Esq.
Debra SuDock, Esq.
Richard J. Rubin, Esq.
Shearman & Sterling
Attorneys for Citibank, N.A.
and Citicorp Real Estate, Inc.
153 East 53rd Street
New York, NY 10022
Attn: Douglas P. Bartner, Esq.
Julie Koshgarian, Esq.
R. Paul Wickes, Esq.
Ira E. Wiener, Esq.
Fried, Frank, Harris, Shriver & Jacobs
One New York Plaza
New York, NY 10004
Attn: Herbert Minkel, Esq.
Wachtell, Lipton, Rosen & Katz
51 West 52nd Street
New York, NY 10019
Attn: Chaim J. Fortgang, Esq.
Jones, Day, Reavis & Pogue
599 Lexington Avenue
New York, NY 10022
Attn: Marc Kirschner, Esq.
Lawrence Gottesman, Esq.

2. The attached Exhibit shall establish the "Administrative Procedures for Electronically Filed Cases" for CLAD ("CLAD Procedures"), including the procedure for distribution of a password to permit electronic filing of pleadings and other documents, and the CLAD Procedures be, and they hereby are, approved by the Court.

3. With respect to the electronic filing of pleadings and other documents on CLAD BBS, the filing party shall identify the initials and last four digits of the social security number of the attorney signing such pleading or other document, which shall constitute a signature of the responsible attorney under Rule 9011 of the Federal Rules of Bankruptcy

Procedure; and the original signature of the attorney approving said pleading or other document shall be maintained in that attorney's files.

4. No attorney shall knowingly permit or cause to permit his/her password to be utilized by anyone other than an authorized employee of his/her law firm.

5. No person shall knowingly utilize or cause another person to utilize the password of another without permission of the holder of the password.

6. Only the attorneys designated above may file with, and retrieve pleadings or other documents from, the CLAD BBS. Only attorneys who have filed a Notice of Appearance in a case assigned to CLAD may retrieve pleadings or other documents in that case from the CLAD Private Database (as set forth in the CLAD Procedures).

7. The electronic filing of a pleading or other document in accordance with CLAD Procedures shall constitute docketing of that pleading or other document.

8. The Office of the Clerk by Deputy Clerks of the Court will enter all orders, decrees, judgments, and proceedings of the court into CLAD which shall constitute official docketing of the order, decree, judgment or proceeding for all purposes.

9. Each person, including the Office of the Clerk, electronically filing a pleading or other document with CLAD shall serve, in the manner provided for below, the "Notice of Electronic Filing" or "Notice of Electronic-Conventional Filing" (as appropriate) generated by CLAD and shall serve such notice on all attorneys entitled to electronic notice of filings. Such service shall be made by hand or facsimile, in the first instance, or by overnight mail if hand delivery or facsimile service is impracticable, which shall constitute service of the pleading or document in accordance with the CLAD Procedures. The Office of the Clerk may use regular mail when facsimile service is impracticable. The filing party shall not be required to serve any other documents in connection with such filing (except as otherwise provided for in the CLAD Procedures for conventionally filed pleadings or other documents) on any party entitled to electronic notice, including the pleading or other document filed by that party.

10. The original of this Order shall be filed in accordance with the CLAD procedures by the Clerk of the Court and conventionally with the Clerk of the Court.

CLAD ADMINISTRATIVE PROCEDURES

COMPLEX LITIGATION AUTOMATED DOCKET ("CLAD")
UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK
"Administrative Procedures for Electronically Filed Cases"
July 1994
Exhibit to General Order M-134

TABLE OF CONTENTS

I. Registration for the CLAD Bulletin Board Service ("CLAD BBS") and the CLAD Private Database. [FN1]

FN1. CLAD Private Database is a database for the purposes of retrieving documents filed on CLAD only. No documents may be filed in the CLAD Private Database.

A. Designation of Cases. The Court shall (i) select those cases which shall be assigned to CLAD and (ii) designate those parties entitled to file and retrieve pleadings and other documents on the CLAD BBS in each such case. Cases shall be assigned to, and parties shall be designated to participate in, CLAD BBS pursuant to an order of the Court authorizing same in each such case.

B. Passwords. Access to the CLAD BBS or the CLAD Private Database requires a password, which may be obtained as follows:

1. Each party entitled to participate in CLAD BBS cases for the electronic retrieval and filing of pleadings and other documents in accordance with an order of the Court shall be entitled to one CLAD BBS password for each attorney in each such case and each adversary proceeding in such case. The CLAD BBS password will permit the attorney to file pleadings and other documents with, and retrieve pleadings and other documents from, the CLAD BBS.

2. Any person or organization, other than those referred to in paragraph I.B.1., above, may apply to the Office of the Clerk, United States Bankruptcy Court for the Southern District of New York for registered access to the CLAD Private Database. Registration under this subparagraph will entitle the registrant to retrieval, but not filing, privileges for CLAD cases subject to the limitations and fees imposed by the vendor.

C. Registration.

1. The attached registration form shall be used for registration under either paragraph I.B.1. for the CLAD BBS or paragraph I.B.2. for the CLAD Private Database. Additional forms are available from the Office of the Clerk.

2. All registration forms shall be mailed or delivered to the Office of the Clerk, United States Bankruptcy Court, Southern District of New York, One Bowling Green, New York, New York 10004-1408, Attn: CLAD/Viola Mathews. Each registration form shall be accompanied by a self-addressed envelope.

3. Attorneys applying for registration and password for the CLAD BBS shall receive a telephone call from the Office of the Clerk indicating that the envelope containing the CLAD BBS password or passwords is available for pick-up. Out of state attorneys applying for registration for the CLAD BBS may contact the Office of the Clerk to arrange for office delivery.

4. Attorneys applying for registration for the CLAD Private Database must include a self-addressed, stamped envelope with the registration form sent to the Office of the Clerk.

II. Electronic Filing and Service of Documents.

A. Filing.

1. Except as expressly provided for in paragraph III.A., below, all motions, pleadings, memoranda of law, or other documents required to be filed with the Court in connection with a case assigned to CLAD shall be electronically filed on the CLAD BBS by those parties designated by the Court to file documents electronically.

2. All documents relating to the motion, application or other matter that are being filed at the same time by the same party may be electronically filed together under one docket number, e.g., the motion, affidavit and supporting memorandum of law.

B. Service.

1. After a pleading or other document is electronically filed, the party shall serve the "Notice of Electronic Filing" or the "Notice of Electronic-Conventional Filing" (as appropriate) generated by CLAD, on those parties entitled to electronic notice, by hand or facsimile in the first instance, or by overnight mail if hand or facsimile service is impracticable. In addition, a paper copy of the electronically filed pleading or other document shall be (i) delivered, by hand or overnight mail, to the chambers of the presiding judge in the case assigned to CLAD together with a copy of the "Notice of Electronic Filing" or the "Notice of Electronic-Conventional Filing" (as appropriate), and (ii) served on those parties not entitled to electronic notice but nevertheless entitled to notice of said pleading or other document in accordance with, and shall be served in the manner provided for in, the Federal Rules of Bankruptcy Procedure except as otherwise provided by the order of the Court.

2. Except as provided for in Paragraph III.B., below, for conventionally filed documents, the filing party shall not be required to serve any pleading or other documents (other than the "Notice of Electronic Filing" or the "Notice of Electronic-Conventional Filing" (as appropriate) generated by CLAD) on any party entitled to electronic notice.

C. Signatures; Affidavits of Service.

1. Original signatures on pleadings, affidavits, and other documents filed electronically shall not be filed with the Office of the Clerk. Each party electronically filing a pleading or other documents on the CLAD BBS (whether or not in conjunction with a conventional filing of a document related thereto) shall maintain in his or her files the original signature on the original paper copy of said pleading or other document. However, the pleading or other document electronically filed shall indicate a conformed signature, e.g., "s/Jane Doe."

2. Affidavits of service shall no longer be filed with the Office of the Clerk and shall not be filed with the CLAD BBS. Each party electronically filing a pleading or other document on the CLAD BBS (whether or not in conjunction with a conventional filing of a document related thereto) shall maintain such affidavits of service in his or her files.

D. Fees.

1. Fees Payable to CLAD. A twenty dollar ($20.00) filing fee shall be payable to CLAD for each docket number obtained in connection with an electronic filing on the CLAD BBS. In addition, a twenty cents per page (20 cents/page) fee (the "Downloading Fee") shall be payable to CLAD for each document retrieved from CLAD; provided, however, that the Downloading Fee shall be waived for the first retrieval of a pleading or other document from the CLAD BBS by any party entitled to notice and service of such pleading or other document in accordance with the Federal Rules of Bankruptcy Procedure or as otherwise provided by order of the Court.

2. Fees Payable to the Clerk. For filings that require a fee to be paid to the Office of the Clerk, authorization for credit card payment may be made with the financial officer of the Office of the Clerk.

E. Orders. All signed orders (including, without limitation, notice of proposed orders, orders to show cause, etc.) shall be filed electronically by the presiding judge in a case assigned to CLAD. In order to facilitate such filing, the party presenting the proposed order shall provide the presiding judge with a 3.5 inch floppy disk containing the proposed order, together with any document to be electronically filed in connection

therewith. Said party shall also provide the presiding judge with a paper copy of all such documents. Said party shall further coordinate with the presiding judge's chambers to facilitate the filing of conventional documents, if any, related to said order. The Office of the Clerk through deputy clerks of Court (normally but not limited to the courtroom deputy for the judge assigned to the case) will make the appropriate entry on CLAD to facilitate the docketing on an order.

F. Title of Docket Entries.

1. The person electronically filing a pleading or other document will be responsible for designating that the title of the document falls within one of the categories contained in Schedule D hereto.

2. The title of a pleading or other document filed electronically MUST (i) identify the party filing said pleading or other document and (ii) be of sufficient detail to describe the subject matter of said pleading or other document.

CORRECT: Debtor's motion to sell nonresidential real property located in Block 11, Lot 6 New York City to Buy It, Inc.

INCORRECT: Motion to sell property

3. The title of a docket entry MUST identify all documents being electronically filed together under one docket number.

CORRECT: Debtor's Notice of Motion to Assume XYZ lease with Motion, Affidavit and Memorandum of Law in support thereof.

INCORRECT: Debtor's motion to assume XYZ lease

III. Conventional Filing of Documents.

A. Conventional Filings. The following documents shall be filed conventionally and shall not be filed electronically (except to the extent that the Office of the Clerk elects to do so):

1. Petitions to commence a case under the Bankruptcy Code, complaints initiating adversary proceedings, and schedules and statements required to be filed under section 521(1) of the Bankruptcy Code (11 U.S.C. s 521(1)) shall be filed conventionally.

2. A motion to file documents under seal shall be filed electronically. However, the document(s) to be filed under seal shall be filed conventionally. The order of the Court authorizing the filing of such document(s) under seal shall be filed electronically by the presiding judge and shall indicate that the motion to file documents under seal has been "so ordered" in accordance with Paragraph II.E., above. A copy of the order shall be attached to the document(s) under seal and be delivered to the Clerk or Chief Deputy Clerk of the Court.

3. Appendices and exhibits to motions, memoranda of law, or other documents that are not capable of conversion to a WordPerfect 5.1 or ASCII format shall be filed conventionally and are not required to be scanned or converted into WordPerfect 5.1 or ASCII format. A cover page consisting of the "Notice of Electronic and Conventional Filing" containing the CLAD docket number. The Notice should identify the exhibit(s) and number for the document filed when applicable.

B. Services of Conventional Filings. Pleadings or other documents which are filed conventionally and are not filed electronically shall be served in the manner provided for in, and on those parties entitled to notice in accordance with, the Federal Rules of Bankruptcy Procedure except as otherwise provided by the order of the Court.

C. Docket Numbers. With respect to any document conventionally filed under paragraph III.A.1., above, the Office of the Clerk will obtain a docket number from CLAD. Any pleading or other document filed conventionally under paragraphs III.A.2. and III.A.3., above, shall include the docket number generated by CLAD at the time that the "Notice of Electronic-Conventional Filing" is produced. The letters "A," "B," "C," etc. following the docket number (e.g., 1302-A) shall indicate that a conventional filing is being made in conjunction with an electronic filing. The "Notice of Electronic-Conventional Filing" shall be attached to the document to be filed conventionally with the Office of the Clerk, which will not accept a conventionally filed document that does not have the "Notice of Electronic-Conventional Filing" prefixed thereto.

IV. Technical Requirements.

A. Document Format.

1. All pleadings and other documents which are filed electronically shall be filed in WordPerfect 5.1 format or in ASCII format. If a pleading or other document is filed in the WordPerfect 5.1 format, it shall be set up with the following initial style set up:

[T/B Mar:1"] [Pg Numbering: Top Right] [Just:Left] [Ln Height:0.167"] [Ln Spacing:2] [L/R Mar:1.25",1.25"] [Hyph Off] [W/O Off] [Font: Courier 10cpi]

After the initial style set up, the document may contain format codes for appropriate presentation (e.g., single space and block indent).

2. DO NOT USE THE AUTOMATIC DATE CODE FEATURE IN ANY WORDPERFECT DOCUMENT FILED ELECTRONICALLY.

3. Documents which are filed in the ASCII format will NOT contain page numbers when viewed electronically on CLAD. In addition, when ASCII documents are printed from a word processing software, the pagination will not be uniform. Therefore, it is recommended that all documents filed electronically be in the WordPerfect 5.1 format.

B. Hardware Requirements. To access CLAD, it is necessary to have a computer (i) operating under a DOS operating system and (ii) equipped with a Hayes compatible modem with a speed up to 14,400 baud. Each attorney having access to the CLAD BBS for the purpose of filing and retrieving pleadings and other documents must have a computer equipped with a hard disk drive.

V. Availability of Documents Electronically Filed.

A. CLAD BBS. Documents filed electronically are immediately available for retrieval on the CLAD BBS.

B. CLAD Private Database. Documents filed electronically are also available for retrieval on the CLAD Private Database as follows:

1. Documents which are electronically filed by 7:30 a.m. will be available for viewing on CLAD by 11:00 a.m.;

2. Documents which are electronically filed by 11:00 a.m. will be available for viewing on CLAD by 3:00 p.m.;

3. Documents which are electronically filed by 3:00 p.m. will be available for viewing on CLAD by 5:00 p.m.;

4. Documents which are electronically filed by 5:00 p.m. will be available for viewing on CLAD by 7:00 p.m.;

5. Documents which are filed after 5:00 p.m. will be available for viewing on CLAD by 11:00 a.m. on the next business day.

VI. Public Access to the CLAD Docket.

A. The public will have electronic access to the documents filed in CLAD and the CLAD docket in the Office of the Clerk during the hours of 10 a.m. to 12 noon and 2 p.m. to 4 p.m., Monday through Thursday.

B. Copies of the documents will be available at the copy service in Room 505, Alexander Hamilton Custom House, One Bowling Green, New York, NY during business hours Monday through Friday. The fee for such copy will be made directly to the copy service.

SCHEDULE A-1. SAMPLE CLAD ELECTRONIC NOTICES

NOTICE OF ELECTRONIC FILING

Please take notice that the following pleading or document has been electronically filed by [name of party] in

[case number] [bankruptcy number]

on CLAD for the United States Bankruptcy Court for the Southern District of New York on [filing date] at [filing time]:

[document title]

Docket Number; [docket number]
Related to Docket Number: [related docket number]
Related Main Case: [related main case number]

Document type: [filing type]
Filed by: [filed by]
Receipt Number: [receipt number]
Approved by: [approving attorney id]

Adversary Proceeding Number: [adversary proceeding number]
Adversary Proceeding Name: [adversary proceeding name]

Return Date: [return date] Return Time: [return time]
Objections Due: [objection due date/time]

Signature of Counsel _____

SCHEDULE A-2

NOTICE OF ELECTRONIC-CONVENTIONAL FILING

Please take notice that the following [document type] has been electronically filed by [attorney name] for [party] in:

[main case name] [bankruptcy number]

on CLAD for the United States Bankruptcy Court for the Southern District of New York on [file date] at [file time]:

[title]

Docket Number: [docket number]
Related to Docket Number: [related docket number]
Attorney Bar No: [approving attorney id]

This [document type] is returnable on [hearing date] at [hearing time]. Objections to this [document type] are due [objection date] at [objection time].

In addition, pursuant to the Clerk's "CLAD Administrative Procedures," one or more conventional filing(s) will be made starting with docket number [docket number]-A.

SCHEDULE B. REGISTRATION FORM

Complex Litigation Automated Docket (CLAD)
United States Bankruptcy Court
Southern District of New York

Authorization for Electronic Filing

Registration Information:

Attorney Name _____

Last 4 Digits SSN _____

Firm Name and Address _____

Phone No. _____

Facsimile No. _____

Are you a LEXIS/NEXIS subscriber

( ) Yes ( ) No

Bill Group No. _____

Attorney Signature _____

Password _____

Authorization:

Date _____

Clerk _____

MEAD notice to Clerk and Registrant:

Date _____

MEAD Representative _____

SCHEDULE C. LIST OF ABBREVIATIONS

[TO BE FAXED WHEN SUPPLIED]

Clerk's Office Procedural Handbook U.S. District Court for the Eastern District of Pennsylvania XLI. Electronic Filing and Retrieval of Documents

XLI. ELECTRONIC FILING AND RETRIEVAL OF DOCUMENTS

Electronic filing and retrieval of documents is available for certain documents filed in the Eastern District of Pennsylvania. All civil and criminal documents will be accepted for electronic submission, including complaints, notices of removal and notices of appeal. The legal agency or law firm utilizing electronic filing must first submit an application to the clerk's office which explains the equipment specifications needed to transmit electronically.

The documents electronically transmitted are in lieu of paper submissions. The attorney making the electronic submission should not transmit a document electronically and also submit the same document in paper form. An application is attached and should be submitted to the Clerk's Office (Appendix V). Also attached is a directory of automated services which are available. (Appendix W).

A. Signature Documents. Each attorney with an electronic filing account must submit one original signature document to the Clerk of Court to be appended to each electronic submission. Any electronic document that does not have a signature document on file will be returned to the attorney. In addition, the attorney must submit a Signature Document Authorization Statement with each electronic submission.

The Signature Document Authorization Statement will authorize the Clerk to append the signature document. The Authorization Statement should state: I hereby authorize the Clerk of Court to append my signature document, on file in the Clerk's Office, to this electronic submission.

B. Equipment. The electronic submission of documents requires the use of a terminal, a 2400 baud modem, and a computer capable of processing ASCII or XMODEM or Word Perfect 5.0. At the present time, these are the only acceptable means to transmit documents electronically to the district court.

APPENDIX V. APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS

APPLICATION FOR A GROUP USER ACCOUNT FOR ELECTRONIC SUBMISSION OF CIVIL DOCUMENTS

Purpose:

This application may be completed by any legal agency or law firm wishing to establish a group account whereby attorneys belonging to that agency or firm may make electronic submissions of certain civil and criminal documents to the United States District Court of the Eastern District of Pennsylvania. A submission is defined as a document that would normally be submitted to the court on paper. Electronic submissions consist of machine-readable information that, instead of being typed out on paper using the attorney's word processor, is transmitted to the court computer where it is then printed out for submission to the judge. Those documents that an attorney elects to electronically submit are in lieu of paper submissions and must not be followed up by paper submissions of the same documents to the court. The attorney making the submission will still be required to serve other counsel in the case with paper copies of any electronically submitted

document and take care to ensure that the informational content of the copies served on other counsel is exactly the same as that of the electronic submission. Once this application is approved, attorneys that are members of the agency or firm may use their computer to gain access to a court computer via a dial-in modem.

This document must be executed by an appropriate manager within the applying agency or firm.

Return the completed application to the following address:

Michael E. Kunz
Clerk of Court
United States District Court
for the Eastern District of Pennsylvania
Room 2609
601 Market Street
Philadelphia, PA 19106-1797

1. Date of Application: _____

2. Name and Address of Applicant Agency or Firm: _____
_____
_____

3. Name and Phone Number of Designated System Liaison Within Agency or Firm:
_____

4. Approximate Number of Attorneys Within Agency or Firm: _____

5. Make and Model of Computer System(s) Used by Applicant:
_____
_____

6. Make and Model of Computer Terminal(s) Used by Applicant:
_____
_____

7. Word Processing Software Packages Used by Applicant:
_____
_____

8. Communications Protocols Used by Applicant:
(NOTE: Only ASCII, XMODEM-CHECKSUM, XMODEM-CRC and YMODEM)
_____

The applicant agrees to the following requirements and conditions: Appointment of a Group System Liaison. The agency or firm will appoint a System Liaison whose name and phone number appear in item 3 of this application. This person shall be responsible for activating and deactivating individual user accounts for each attorney employed by the agency or firm desiring to make electronic submissions to the Court.

Individual User Accounts. User accounts will only be established for attorneys that are admitted to practice before the Court. To satisfy the requirements of Rule 11 of the Federal Rules of Civil Procedure, which states in part:

> Every pleading, motion and other paper represented by an attorney shall be signed by at least one attorney of record in the attorney's individual name, whose address shall be stated. [Emphasis added] [FN*]
>
> FN* So in original.

an attorney participating in this pilot project must submit an original signature document (Attachment A) to the Clerk of Court to be referenced to any document electronically filed. In addition, each electronic submission must contain the following statement authorizing the Clerk of Court to append a signature page to that document:

I hereby authorize the Clerk of Court to reference my signature document, on file in the Clerk's office, to this electronic submission.

Signature Documents. It shall be the responsibility of each attorney with an electronic filing account to submit to the Clerk of Court a signature document so that it may be referenced to any electronic submission. Unless an attorney has filed a signature document with the Clerk of Court he cannot file an electronic submission. Attachment A to this application is a copy of the signature document that must be used.

Signature Document Authorization Statement. Each electronic submission must contain the statement that authorizes the Clerk to reference the signature form in order for it to be accepted for filing. Any submission not containing the authorization statement will be rejected.

Acceptable Communication Protocols. The electronic filing system will presently accept files that are transmitted via either ascii, xmodem-checksum, xmodem-crc or ymodem. Only one of these communications protocols may be used.

Acceptable Terminal Types. The following terminal types are presently recognizable by the system: vt100, ansi, and dumb. Users should specify the dumb terminal type if they are unsure as to which terminal they have. Only one of the above terminal types will be specified.

Modem Settings. The court dial-in modem is presently set as follows: 2400 baud, 8-bit, 1 stop, no parity. Data can be transmitted at 1200, 2400 or 9600 baud. User dial-out modems should be set appropriately.

Filing Status Messages. Individual attorneys will be expected to access the electronic filing system periodically to check either private or public messages regarding the status of any electronic submissions. Both acceptance and rejection messages relative to an attorney's electronic submissions will appear under private messages. Information relative to submissions by any attorneys that are accepted for filing within the previous few days will appear under public messages.

Technical Support by Court Personnel. The users will be responsible for making the appropriate settings on their hardware and communications package in order to gain access to the electronic filing system. If a user is unable to gain access and there is reason to believe that the court system is not operational, please call 597-5860 and request to speak to the Electronic Filing System Administrator. Normally, if users get a "no answer" message when attempting to dial in, then either there are no ports available presently (and the user should try again later) or the system is down for some type of maintenance. Routine system backups will be accomplished between the hours of 8:30 am and 9:30 am Monday thru Friday. The system will not be available for use during these hours.

User Fees. A fee structure may be implemented in order to recover any increased personnel, equipment and telephone line costs that are incurred by the Court. Users will be advised at least 60 days in advance of the implementation of any fee system. At that point users will have the options of either agreeing to pay the established fees or of having their electronic filing access services discontinued.

Document Formatting. Presently this system will only accept documents containing standard ascii characters or in WordPerfect 5.0 format (See Attachment B to this application for a list of the standard ascii characters). Most word processing packages have an option whereby the user can convert the word processing formatted file to an ascii file. When this option is used, the word processing system will strip out all special formatting characters and retain only the ascii characters. As a matter of practice, the attorney should review any file that is converted to ascii prior to the electronic submission of the ascii file to the court. The symbol "&" must be used in lieu of the section symbol when referring to a title and section of a code. Title 18, Section 495 of the U.S. Code would be typed as 18 USC & 495. Footnotes must either be treated as end notes or manually inserted on each page. Page breaks (CONTROL-L) must be inserted for each page of the document being submitted. Otherwise, the system will automatically insert a page break every 66 lines.

Attachments, Appendices, Exhibits to Electronic Submissions. Documents with attachments, appendices or exhibits may only be submitted electronically if they may also be included in full as part of the submission document. This means that if a document is transmitted as an ascii file only attachments, appendices or exhibits that consist entirely of ascii text files may be submitted. No document may be electronically submitted that has attachments, appendices or exhibits that consist of graphs, drawings or pictures of any other non-ascii characters.

Affidavits, Depositions and Other Signed Statements. Affidavits, depositions or any other sworn statement signed by any person other than the attorney making a submission may not be electronically transmitted to the court. Certificates of service that are normally signed by the attorney must be included as part of any electronic submission.

Effective Filing Date and Time for Electronically Submitted Documents. The date and time that the document is transmitted will be considered as the "Date Filed" for the document. In most cases, documents will be reviewed within a few hours after they are received on the Court machine. The only exceptions will be documents that are electronically submitted after normal office hours (8:30 am to 5:00 pm EST) Monday thru Friday, documents submitted on weekends and documents submitted on holidays.

Documents submitted during the exception periods will be promptly reviewed on the next court business day.

Files Lost Due to Hardware Malfunction. It is remotely possible that an electronically submitted document may be lost on rare occasions due to a malfunction of the court computer. This problem is only likely to occur if the hard disk on the computer should sustain some damage during the few seconds between the time that a user confirms acceptance of the document for submission and a security copy of the document is printed out in the court. In these instances, users will not receive a document review message and should contact the Electronic Filing System Administrator by calling 597-5860. Any lost documents will then have to be resubmitted. It must be emphasized that this type of problem is extremely rare and may never occur.

The undersigned, as the duly authorized representative of the applicant agency or firm hereby states that he or she has read all of the terms and conditions on this application and promises that steps will be implemented to ensure that all employees will abide by these terms and conditions. The undersigned further affirms that the statements made in this application are true and factual.

_____

(Signature of Applicant's Authorized Representative)

_____

(Title)

_____

(Phone Number)

May 1997.

Attachment A. Signature Document

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

CERTIFICATION OF SIGNATURE
PURSUANT TO F.R.C.P. 11

I hereby authorize the Clerk of Court to reference this signature document to any pleading, motion or other paper electronically filed in order to satisfy the requirements of Rule 11 of the Federal Rules of Civil Procedure and agree to be bound by the provisions thereof.

_____ (Attorney Signature)

PLEASE PRINT:
_____ (Attorney Name)
_____ (Firm Name)
_____ (Address)
_____
_____
_____
_____

Attachment B. ASCII Character Set

ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

0 1 2 3 4 5 6 7 8 9

! @ # $ % & * ( ) - + = ( ) [ ] : ; " ' < > ? , . /

Space Delete