

**GO TO PAGES 17 - 18.....**

NCSC  
KF  
8733  
W35  
1999  
C.3

Electronic Court Documents ;

*An Assessment of Judicial Electronic Document and Data  
Interchange Technology*

by

J. Douglas Walker

*Director of Court Technology Research*

National Center for State Courts



Prepared by the National Center for State Courts,  
with funding from the State Justice Institute

Library  
National Center for State Courts  
300 Newport Ave.  
Williamsburg, VA 23187-8798

Rec'd 1-5-00

© 1999  
National Center for State Courts  
ISBN 0-89656-204-2

This report was developed under grant number SJI-96-06D-B-153 from the State Justice Institute. The points of view expressed are those of the author and do not necessarily represent the official position or policies of the State Justice Institute.

NATIONAL CENTER FOR STATE COURTS  
*Board of Directors*

**E. Norman Veasey**

**Chair**

Chief Justice of Delaware  
Carvel State Office Building  
P.O. Box 1997  
Wilmington, Delaware 19899

**Howard W. Conyers**

***Vice-Chair***

Administrative Director  
Supreme Court of Oklahoma  
1915 North Stiles, Suite 305  
Oklahoma City, Oklahoma 73105

**Gerald W. VandeWalle**

**Chair-Elect**

Chief Justice of North Dakota  
Supreme Court of North Dakota  
State Capitol Building  
600 East Boulevard Avenue  
Bismarck, North Dakota 58505-0530

**Roberto A. Arias**

Judge

Duval County Courthouse  
330 East Bay Street, Room 324  
Jacksonville, Florida 32202

**Byron Attridge**

King & Spalding

191 Peachtree Street, N.E.  
Atlanta, Georgia 30303-1763

**Frank Broccolina**

Deputy State Court Administrator  
Courts of Appeal Building  
361 Rowe Boulevard  
Annapolis, Maryland 21401

**David A. Brock**

***Immediate Past Chair***

Chief Justice  
Supreme Court of New Hampshire  
Frank Rowe Kenison Building  
Concord, New Hampshire 03301

**Kevin S. Burke**

Judge

Hennepin County District Court  
1051-C Government Center  
Minneapolis, Minnesota 55487

**William Cousins**

Justice

Illinois Appellate Court  
160 North LaSalle, Rm. 1905 S  
Chicago, Illinois 60601

**Ann K. Covington**

Justice

Supreme Court of Missouri  
207 West High Street  
Jefferson City, Missouri 65101

**Gordon M. Griller**

Court Administrator

Maricopa County Superior Court  
201 W. Jefferson St., 4th Fl.  
Phoenix, Arizona 85003

**William G. Kelly**

District Court Judge

62-B District Court  
4900 Breton Avenue, S.E.  
Post Office Box 8848 (49518-8848)  
Kentwood, Michigan 49508

**Jack B. Middleton**

McLane, Graf, Rauleron & Middleton  
900 Elm Street  
Manchester, New Hampshire 03105

**Thelma Cummings Moore**

Chief Judge

Superior Court of Fulton County  
Suite T-4905  
185 Central Avenue  
Atlanta, Georgia 30303

**Gayle A. Nachtigal**

Presiding Judge

Circuit Court of Washington County  
Washington County Courthouse  
145 NE Second Avenue  
Hillsboro, Oregon 97124

**Dwight Opperman**  
Key Investment, Inc.  
601 Second Avenue, South  
Suite 5200  
Minneapolis, Minnesota 55402

**Kenneth R. Palmer**  
State Court Administrator  
Florida State Courts System  
Supreme Court Building  
500 South Duval Street  
Tallahassee, Florida 32399-1900

**Louise M. Parent**  
Executive Vice-President and  
General Counsel  
American Express Company  
American Express Tower  
World Financial Center, 51<sup>st</sup> Floor  
New York, New York 10285

**Carroll D. Stevens**  
Associate Dean  
Yale Law School  
127 Wall Street (06511)  
Post Office Box 208215  
New Haven, Connecticut 06520-8215

**Sandra Ann Thompson**  
Judge  
Los Angeles Municipal Court  
South Bay Judicial District  
825 Maple Avenue  
Torrance, California 90503-5058

**Ruth Walsh McIntyre**  
1409 East Prospect  
Seattle, Washington 98112

**William C. Vickrey**  
**Immediate Past Vice-Chair**  
State Court Administrator  
Administrative Office of the Courts  
455 Golden Gate Avenue, Ste. 5622  
San Francisco, California 94102-3660

**Roger K. Warren**  
*ex officio*  
President  
National Center for State Courts  
300 Newport Avenue  
Williamsburg, Virginia 23185

**Robert Wessels**  
Court Manager  
County Criminal Courts at Law  
301 San Jacinto, Room 401  
Houston, Texas 77002-2022

## FOREWORD

This document contains discussions of several advanced technologies and technology issues. There is no universal agreement regarding the details of some of these topics, with different opinions and interpretations often being found among technology industry experts and court technology practitioners. The views expressed here represent the author's findings and conclusions based on a study of the information, issues, technology applications, and experiences of practitioners. These views do not necessarily reflect the opinions or official positions of the National Center for State Courts (NCSC) or the State Justice Institute.

This document also contains information about a number of court technology projects. The information was obtained through research, interviews, discussions, personal observations, and materials furnished by the individuals and organizations involved in these projects. The information presented is believed to be generally accurate, based on the author's understanding of the source material available at the time; however, the author apologizes for any inaccuracies or omissions. The reader is urged to contact the relevant courts or vendors directly to obtain the most recent and complete information about any projects, products, or services mentioned.

The author is indebted to many individuals and organizations for their contributions to this study. Colleagues within NCSC and throughout the courts have provided information, ideas, advice, and assistance in conducting the study and preparing this document. Rather than risk leaving anyone out by attempting to name individual contributors, the author simply wishes to express his gratitude to all who helped make this work possible. He is especially grateful to the court personnel involved in each site visit, who made themselves and their staffs available even when it was not convenient. Their candid discussions of their projects and the issues they encountered were invaluable to this assessment. The author also wishes to thank the State Justice Institute for providing the grant funds to support this work.

# TABLE OF CONTENTS

<b>CHAPTER ONE - <i>Introduction</i></b> .....	<b>1</b>
Project Background.....	1
Purpose and Organization of this Report .....	2
The JEDDI Concept.....	2
<b>CHAPTER TWO – <i>The National Experience</i></b> .....	<b>5</b>
The Evolution of JEDDI.....	5
The Development of Effective Court Rules for JEDDI.....	6
A Summary of Court JEDDI Projects.....	7
Local Court Projects .....	7
State-Level Court Projects.....	9
The Federal Courts Project.....	10
JEDDI Technology Vendors.....	11
<b>CHAPTER THREE – <i>Why JEDDI Is Inevitable</i></b> .....	<b>15</b>
Introduction.....	15
Cost Advantages .....	17
Processing Costs .....	18
Storage and Handling Costs .....	21
Improved Information Processing and Accessibility .....	23
Improved Information Processing .....	23
Improved Information Accessibility.....	25
Public Expectations.....	26
<b>CHAPTER FOUR - <i>The Nature of Electronic Documents and Their Implications for the Judicial System</i></b> .....	<b>29</b>
Types of Electronic Documents.....	29
Image-based Electronic Documents .....	29
Text-based Electronic Documents.....	31
Implications for the Judicial System.....	32
The Coming Transformation of Court Documents .....	32
Early Examples of this Transformation.....	33
Courts Must Prepare for This Change.....	34
<b>CHAPTER FIVE - <i>Format and Transmission Alternatives</i></b> .....	<b>35</b>
Transmission Media and Methods .....	35
Physical Media .....	35
Electronic Transmission .....	36
Alternative Approaches to Electronic Documents.....	37
Dumb Documents.....	37
Electronic Cover Sheet Paired with Dumb Documents .....	38
Intelligent Documents.....	39
Standardized Markup Languages.....	41

SGML .....	41
HTML .....	41
XML .....	43
<b>CHAPTER SIX - Security and Authentication Technologies .....</b>	<b>49</b>
Introduction .....	49
The Challenge of Internet Document Interchange .....	49
General Security Requirements for JEDDI Systems.....	49
Security Issues for Electronic Document Transmission.....	50
Technological Approaches to Security and Authentication.....	51
Something You Know .....	52
Something You Are.....	54
Something You Have.....	55
The Judicial System’s Place on the Security Scale.....	56
Security in Traditional Paper Systems .....	56
Why Electronic Records Should Have Higher Security Requirements than Paper .....	56
The Most Promising Technological Method to Ensure Authenticity and Integrity.....	57
Electronic Signatures.....	58
Digital Signatures .....	59
Cryptography .....	59
Public Key Infrastructure (PKI).....	62
Conclusion .....	65
<b>CHAPTER SEVEN - New Jersey’s JEDDI Project .....</b>	<b>67</b>
Project Background.....	67
Initial Challenges.....	67
Pilot Court Selection.....	67
Selection of Law Firms.....	68
Development and Implementation .....	68
Court Rules Affected .....	69
Major Obstacles .....	73
Interface with Legacy System .....	73
Securing the Support of the Bar .....	73
System Design and Operation.....	74
System Overview.....	74
Quick Filer.....	75
Batch Filer .....	82
Import Function .....	85
Docketing.....	86
Search and Retrieval Function.....	89
Security .....	96
Future Plans .....	97
Primary Lessons Learned.....	97
<b>CHAPTER EIGHT - Utah’s JEDDI Project.....</b>	<b>99</b>
Project Background and Key Issues.....	99
The Internet.....	99
SGML .....	99

Case Type for Pilot.....	100
Digital Signatures .....	100
Broad Vision of Electronic Ecosystem.....	100
Personnel Setbacks and Solutions.....	101
System Design and Operation.....	102
E-Filer Client.....	102
Court Components and Processes.....	103
Flexibility of the Court Side of the Architecture .....	116
Future Plans .....	117
Web-based Filing.....	117
Expanded Scope .....	117
Additional Improvements and Expansion.....	118
Primary Lessons Learned.....	119
<b>CHAPTER NINE - <i>Conclusions</i> .....</b>	<b>121</b>
Growth Factors.....	121
Trends .....	122
Planning for JEDDI Implementation .....	123



# CHAPTER ONE

## *Introduction*

Courts have been pursuing the concept of electronic documents for nearly a decade. The term JEDDI, for Judicial Electronic Document and Data Interchange, was coined several years ago to describe the idea of developing a formal protocol for document and data interchange within the justice community. The JEDDI protocol would be based somewhat upon the commercial sector's rigorous data exchange standard known as Electronic Data Interchange or EDI. Over time, however, the EDI approach generally has been abandoned as impractical for the courts. JEDDI has come to be used to describe the general idea of electronic court documents and the transmission of those electronic documents within the justice community. This concept has proven to be a significant challenge to the judicial system. While a substantial number of courts now can provide some form of electronic access to general if not case-specific information, only a handful of pioneers can claim successful implementation of some type of electronic filing (e-filing) system, much less an extensive JEDDI system.

### Project Background

With funding from the State Justice Institute, the National Center for State Courts (NCSC) began a study to observe the progress of efforts among the state courts to develop and implement JEDDI technology. The study was intended to identify and explore the major issues involved, review a few of the more successful projects, track relevant advances in the technology industry, and develop some conclusions about the best approach to electronic documents to provide some guidance to court managers.

When the grant application for this study was submitted in 1996, there were several promising JEDDI projects being discussed among the court community. Some were still in the planning or design stages, but others reportedly were operational. As research activities got under way and some early site visits were conducted, however, it became obvious that there was much more concept than substance to most of the court projects. While some courts may have started rudimentary experimentation with JEDDI, expansion into working pilot projects was a year or more away. Other courts that had projected an operational phase for their projects within a few more months suffered subsequent setbacks that severely affected their schedules. In addition to the projects undertaken by court staffs alone that did not progress as planned, two major initiatives involving public-private partnerships were discontinued after an initial investment of millions of dollars (one after implementing a working pilot project and the other before any significant implementation occurred). A project of more modest proportions in a Mississippi trial court was scrapped after being overwhelmed by problems, even though the vendor had successfully implemented a system in another state.

Because it was critical to have an adequate pool of operational projects to assess the national experience, NCSC's research project was slowed to permit court JEDDI projects to

progress so that they could provide more meaningful input to the study. NCSC staff continued to track any developments in the technology industry or court efforts. Subsequent staffing and organizational changes at NCSC necessitated additional delays. As a result, the study was extended through 1999. The extended schedule permitted two major state-level projects that had been targeted previously for review to recover from their own setbacks and become operational. These projects, in New Jersey and Utah, were reviewed during the second quarter of 1999. In many aspects these two projects represent a culmination of the state of the art of JEDDI technology implementations.

## **Purpose and Organization of this Report**

This report presents the significant findings and conclusions from NCSC's assessment of JEDDI technology. The chapters that follow will discuss the characteristics and implications of JEDDI, the national experience with its implementation, and important technology issues to be considered. Although many common issues are covered briefly, the report focuses on certain areas while directing the reader to other sources for in-depth coverage of other topics. One notable complementary document is NCSC's *Guidebook for Electronic Court Filing*, which was developed with funding provided by West Group and was published by West Group in 1998. It provides a good overall picture of the many aspects of electronic filing and offers a particularly thorough treatment of court rules pertaining to electronic filing. An electronic version of that document is available on NCSC's Web site: [www.ncsc.dni.us](http://www.ncsc.dni.us) (the complete URL at the time of publication was <http://www.ncsc.dni.us/NCSC/TIS/TIS99/Electr99/EfileWest.htm>).

This report concentrates on key concepts and technology issues critical to successful implementation of JEDDI systems. Chapter Two summarizes the national experience with implementation of JEDDI technology, including a brief description of most of the projects that have been accomplished to date. Chapter Three discusses the compelling rationale for pursuing JEDDI despite the long, hard road traversed by the first generation of practitioners. Chapter Four presents another key concept: the paradigm shift that results from moving from a traditional world based on paper documents to a new world of electronic documents—a movement that totally redefines the nature of a document and reshapes a myriad of associated implications. Chapter Five then covers one of the critical technology topics germane to electronic documents, which is how to handle the format, representation, and transmission of the documents. Chapter Six follows with an in-depth discussion of the technology alternatives to ensure the security and authentication of electronic documents and case records. The two key state-level JEDDI projects in New Jersey and Utah are described in Chapter Seven and Chapter Eight. Chapter Nine ends the report with a short summary of the conclusions drawn from the study, including a view of where JEDDI technology is heading based on trends and recent developments.

## **The JEDDI Concept**

The general concept of judicial electronic document and data interchange is relatively simple: rather than pleadings and other court documents being prepared on paper and physically

stored and handled for all subsequent processes, they are created, transmitted, stored, and maintained in electronic form. The legal process itself remains essentially unchanged, and the information contained in the documents is used for the same purposes as before. What does change are the myriad steps dealing with the documents themselves and the processes needed to record and extract the information they contain.

As with most concepts, the devil is in the details and in the implications that result from putting the concept into actual practice. The adoption and implementation of the JEDDI concept has profound consequences for the way in which the courts and the entire justice community operate, even though the fundamental legal process is not changed. Furthermore, it seems to be less than practical to implement isolated components of the electronic environment that JEDDI embodies, even though a phased conversion from traditional paper-based processing is highly recommended. For JEDDI to be truly effective, a holistic or systemic approach is needed. The holistic vision of an ideal JEDDI implementation encompasses a range of components, including

- Electronic documents
- Electronic case files
- Electronic signatures
- Electronic filing
- Electronic noticing
- Electronic public access
- Integration of case management, document management, electronic filing, and public access systems.

Moreover, for it to succeed and deliver optimal benefits, a JEDDI system has to extend to all major players in the justice community. Needless to say, it is essential to involve representatives from all affected entities from the outset of any JEDDI project. Most early JEDDI projects were pilot efforts concentrating on the electronic filing front end and limited primarily to the exchange between a small number of attorneys (or a division of the prosecutor's office) and a subdivision of the clerk's office. However, the ultimate embodiment of the JEDDI concept will include not only the components listed above, but also all aspects of the judicial process from initial filing to final disposition. The remainder of this report discusses the issues and implications inherent in that broader vision.

## CHAPTER TWO

### *The National Experience*

#### The Evolution of JEDDI

The evolution of the JEDDI concept is a result of both technology advances and a cultural shift within the courts, as court officials and staff adapted to the applications of technology to their daily operations. As computerized case management systems became the rule rather than the exception, court staff came to rely on the electronic version of the case record as the first source of case information. Yet case management databases contained mostly information manually extracted from paper documents filed with the court or originating within the court. Moreover, at the heart of the adjudicatory process, courts continued to rely on the original paper documents as the source of facts and other information. A few court leaders began envisioning how to extend the advantages of technology to include the documents themselves as part of the electronic store of information.

Others were more concerned about moving the source documents more efficiently between the parties and the courts. As fax machines became more commonplace, numerous courts modified their rules to permit attorneys to file briefs by fax, although in many cases an “original” had to follow within a prescribed time period. Unfortunately, except in rare instances, the document was simply printed out on the court’s fax machine and then handled just as any other paper document.

The advent of document imaging systems in the courts proved to be both a boon and a bane for the notion of electronic documents. On the one hand, document imaging permitted an existing paper process to be improved through conversion of incoming paper documents to electronic files. Such files then could be moved around the court electronically and stored on optical disk platters requiring very little physical space and affording rapid retrieval. Moreover, to the extent that judges and other court officials were willing to view document images on a computer screen, this technology solution advanced the idea of depending on an electronic version of case information rather than paper. Indeed, the successful integration of a document imaging system with the case management system seemed to many to be an ideal solution. On the other hand, in some ways document imaging further wedded courts to the notion that paper documents—or at least an electronic picture of those documents—were an inevitable and essential component of case processing and adjudication.

Some progressive leaders, however, recognized the inherent value of text-based electronic documents. Text-based documents are machine-readable as well as readable by humans. That means that computers can perform powerful text-based searching to locate information of particular interest. Moreover, information can be electronically copied and pasted into other documents or into the case management database. Text-based documents offer another major benefit in terms of the relatively modest storage requirement they impose on computer systems. Even with formatting control characters, for example, a word processing

document can be stored digitally in a fraction of the space required for a document image file. Although with the rapid decline in the cost of computer storage technology in recent years this advantage is not as significant as it once was, it is still a consideration. Furthermore, because document files must be moved around frequently within the court community, the difference in file sizes affects the entire technology infrastructure, including network bandwidth and telecommunications efficiency.

Along with the growing acknowledgment of the advantages of text-based electronic documents, there seems to be a growing acceptance of the idea that, for many purposes, the information contained in a document is the essential component, not the document itself. Despite the necessarily conservative nature of the judicial system and the well-entrenched notions of prescribed formats, original documents, and other safeguards of due process, the judicial process is moving a bit more toward substance over form in some areas. In terms of accepting pleadings electronically from law firms, this attitude enables the adaptation of powerful and flexible new technology solutions, such as eXtensible Markup Language (XML), to create “smart” electronic documents. Smart documents, in turn, can automate many of the document tracking, data extraction, and data entry functions now having to be performed manually even in courts with sophisticated case management systems. These concepts and their underlying technologies will be discussed in depth in the chapters that follow.

## **The Development of Effective Court Rules for JEDDI**

The past few years have witnessed tremendous progress in the development or modification of court rules—and sometimes statutes—to address the application of JEDDI technology to court operations. With growing momentum, state legislative committees and task forces on court rules have overhauled obsolete laws and rules that would have prevented or hampered the transition to electronic documents. Much of this work has been very carefully thought out, with great concern for preserving due process while enabling courts to move forward with new methods for conducting their operations. Unfortunately, some revisions have been a bit too specific in prescribing the technologies, formats, and procedures that must be followed. Achieving the proper balance and avoiding undesirable ramifications from the authorizing statutes or rules is a difficult task. As the judicial branch gains experience with the sweeping changes that rapid technology advances are bringing to the courts, the states will draft better and better legislation and rules to govern court procedures.

An exceptionally thorough treatment of the topic of court rules can be found in Chapter 3 of the *Guidebook for Electronic Court Filing*. NCSC staff developed recommendations for rules covering many different aspects of JEDDI technology, along with examples extracted from actual rules and a general discussion of the issues. In addition, the publication contains a comprehensive appendix of sample court rules as well as summaries of rules organized both by state and by topic. Another good source for current information on legislation and other policy matters regarding the broader topic of electronic commerce can be found on the Web site for the law firm of Baker & McKenzie (<http://www.bakerinfo.com/ecommerce>).

## A Summary of Court JEDDI Projects

It seems fair to say that any court that has attempted implementation of a JEDDI system up to this point should be considered a pioneer in this application of technology. Virtually all have had to break new ground to some extent. Despite the compelling simplicity of the concept, no standardized approaches have been established, and many issues remain unresolved. Indeed, some of the fundamental principles still are being debated sharply among both theorists and practitioners, even while consensus is growing concerning other aspects of JEDDI projects.

This section presents a very brief description of most of the state and local court JEDDI projects that have been implemented to date. It also mentions the admirable initiatives undertaken by the federal courts to develop guidelines and working systems. The list does not pretend to be exhaustive, nor are the descriptions guaranteed to be current or accurate in every detail. This list does, however, illustrate the wide variation in the nature and characteristics of the approaches that different courts have taken to develop some type of electronic document exchange system. There has been little coordination among these efforts, as they have been conducted mostly by individual, independent entities scattered around the country. Regardless of the extent to which these practitioners may have been successful, they are to be commended for their efforts and their contributions to the growing pool of knowledge about JEDDI and experience with its practicable implementation. The numerous courts now gathering information or actively planning JEDDI projects, along with the commercial technology vendors that are rapidly gearing up to provide JEDDI products and services, will benefit from the lessons learned through these pioneers.

The projects are listed in no particular order within the categories below. Readers may wish to contact some of these courts and other organizations directly to obtain more information about their JEDDI projects.

### *Local Court Projects*

#### **CLAD (Complex Litigation Automated Docket)**

CLAD, one of the first electronic filing projects, is a commercial system developed by Mead Data Central (now LEXIS-NEXIS) to handle massive, complex insurance coverage cases filed in the Delaware Superior Court for New Castle County. The system became operational in 1991 with the first filing accepted in December. Mead/LEXIS-NEXIS retained ownership and operation of the system, which uses proprietary software to permit registered users to connect with the document database through dial-up communications for filing or viewing documents.

#### **Prince George's County (Maryland) JusticeLink Project**

This public-private partnership between the Circuit Court of Prince George's County and Andersen Consulting was one of the pioneering efforts among state and local e-filing projects. This pilot project handled motor tort and foreclosure cases and used Lotus Notes as an underlying technology for the JusticeLink system. It began in 1995, and the resulting system

began accepting filings in November 1996. Although technically a success, the pilot project ultimately was shut down because it was considered fiscally infeasible for the current market. In 1998, Andersen Consulting entered a joint venture with Lynx Capital Group, a private equity firm in California, to establish JusticeLink, Inc., as an independent company focused on developing and marketing e-filing services. JusticeLink, Inc., recently merged with LAWPlus. The merged company retains the JusticeLink, Inc., name.

### **Shawnee County (Kansas), Third Judicial District Court**

This court has been operating an electronic filing system since October 1998. The system initially accepts civil filings for debt collection cases. It uses e-mail as the transmission medium, employing specially formatted templates and ASCII text in the body of the message rather than attached documents.

### **Orange County (California) Superior Court**

A project has been in operation since about 1996 to permit the family support division of the district attorney's office to file complaints for paternity and other selected case types electronically. Filings that pass validation result in automatic updating of the court's family law database and printing of the summons and complaint for immediate service. In April 1999 the Orange County Superior Court announced that it was entering a public/private partnership with SCT and West Group to provide countywide electronic filing. Pilot projects are expected to be operational in 2000, beginning with the family law division and expanding into the probate and then general civil divisions.

### **LAWPlus and Jefferson County (Texas), Fifty-eighth District Court**

Since late 1996, this court has been operating an e-filing system developed for it by LAWPlus to accept selected civil filings from law firms. In addition, LAWPlus reportedly has contracts in two additional Texas jurisdictions, the U.S. District Court in northern Alabama, and the San Francisco County Superior Court. As of this writing, LAWPlus had just merged with JusticeLink, Inc., a pioneering e-file venture jointly owned by Andersen Consulting and Lynx Internet Ventures Fund, LLC.

### **Pima County (Arizona) Consolidated Justice Court and Law-on-Line, Inc**

Together, the court and Law-on-Line, Inc., created a Web-based public interface called the Virtual Peoples Court. This system includes an electronic filing component, which is unique in that it is aimed at the general public rather than either the private bar or other justice system partners. The Pima County e-filing system is geared toward public filing of small-claims cases. Filers can submit initial complaints, answers, or requests to transfer from small-claims court to the justice court. This system uses an Internet Web browser as the user interface together with e-mail for confirmations, and it includes on-line payment of filing fees via credit cards.

## Arapahoe County (Colorado) and Gros Ventre Systems

In late 1996 the Eighteenth Judicial District Court began a project with Gros Ventre Systems of Denver to develop an electronic filing system. The court had been plagued by a growing caseload and inability to add more clerical staff to handle the backlog. The court has accepted fax filings for several years, and these had grown to constitute nearly half of the total document filings. The public-private partnership developed a Web-based electronic filing system to permit attorneys to connect to a secure Web site and transmit their documents to the clerk's office. The system, named legalFile, became operational in June 1997 as a pilot project involving twelve law firms. By March 1998, over 1,000 documents had been filed electronically. The system has continued to be expanded and improved. Its successful operation was an important factor in Colorado's decision in the spring of 1999 to implement a statewide JEDDI project.

## *State-Level Court Projects*

### New Jersey

The New Jersey Administrative Office of the Courts (AOC) has been developing a JEDDI system during the last few years, which it is now pilot testing in Monmouth County. The system is designed around the concept of a totally electronic court record and reengineered workflow to capitalize on its capabilities. The initial system is being used for retail debt collection cases handled by a limited number of law firms. Although the user interface currently employs a dial-up connection between the law firms and the AOC, a Web-based interface is under development. (Chapter Seven contains a detailed description of New Jersey's project.)

### Utah

The Utah judiciary has been exploring JEDDI issues and technologies for a number of years. Utah was the first state to pass digital signature legislation in 1995. The Utah Administrative Office of the Courts has been planning and developing a JEDDI system since about 1992, experimenting with evolving technology such as SGML (Standard Generalized Markup Language) and XML (eXtensible Markup Language) to create "smart documents" with automatically identifiable data fields. The pilot implementation of Utah's system, which was a joint project between the Third District Court, the AOC, and the Office of the District Attorney for Salt Lake County, started with criminal (fugitive from justice) case filings. Plans call for the system to be expanded to handle civil and small-claims cases. (More information about this project can be found in Chapter Eight.)

### New Mexico

The New Mexico Administrative Office of the Courts has been developing and piloting a Web-based electronic filing system for the last several years. The state is piloting this system, which was based on the early federal court model but has undergone significant alteration, in the Eleventh Judicial District Court. In a commendable spirit of cooperation, the state AOC is



working with the U.S. District and U.S. Bankruptcy courts in New Mexico to develop a system that presents a common interface for New Mexico's attorneys, while meeting the specific requirements for each court. The state's pilot project deals with criminal case filings, but the system will be expanded to other case types. The federal-state team currently is developing a new approach using XML technology to improve operation of the system. This approach will permit the attorneys to connect with each court, using their own or vendor-supplied software.

## **Colorado**

Colorado's administrative office of the courts awarded a contract to JusticeLink in August 1999 to develop and implement a statewide electronic filing solution for civil cases. An initial pilot project was scheduled to begin in November 1999.


## **North Carolina**

The North Carolina Business Court was established in 1996 as a specialized court to handle complex business litigation. In the spring of 1999, the court began a court technology pilot project, capitalizing on the specialized nature of the single-judge court. The technology project involves the AOC, superior court judges, the North Carolina Bar Association's technology committee, and technology consultants. In addition to courtroom technologies, such as presentation technology and videoconferencing, a major focus of the project is electronic documents and electronic filing. A pilot version of an electronic filing and case management system has been developed. Electronic documents can be accepted in several formats, including MS Word, HTML, ASCII text, RTF, and Adobe Portable Document Format (PDF). The system also will accept MS PowerPoint and JPEG graphics files. An objective of the court is to be able to review all documents on a computer monitor and to display them electronically in the courtroom as needed. Court rules covering electronic filing were drafted in November 1999 and will be finalized in early 2000.

## ***The Federal Courts Project***



The federal judiciary has been aggressively pursuing the concept of electronic filing and electronic case files for a number of years. Beginning in 1995, technology staff from the Administrative Office of the U.S. Courts began working with the Northern District Court of Ohio to develop a solution for handling a tremendous volume of filings in maritime asbestos cases. The electronic filing front-end system that resulted from this effort became the basis for a more complete electronic filing system prototype. This prototype system was piloted beginning in late 1996 in the Southern District of New York Bankruptcy Court. With more and more case management components being included in the design, the USAOC began referring to its system as the Case Management/Electronic Case File (CM/ECF) System. With continuous improvements and adaptation for new case types, CM/ECF now has been implemented in nine federal courts (four district courts and five bankruptcy courts) as an expanded pilot project. Through the first half of 1999, it is estimated that the system has been used by over 1,000 attorneys and has processed more than 15,000 cases and 175,000 documents. The USAOC anticipates expanding the system to other federal courts.



The federal system employs a Web browser interface, Web forms, and Adobe PDF files for transmitting filing information between law firms and the courts. Attorneys prepare a document using standard word processing software with the addition of Adobe's Acrobat software, which writes the document out as a PDF file, preserving the formatting produced through word processing. After logging on to the court Web site with an authorized ID and password, the law firm uses interactive Web pages to enter the information needed to specify the case and filing details. The PDF file containing the document itself is then uploaded through the Internet connection to the court's computer. The PDF file is stored in the CM/ECF system and linked to a docket entry that is created in the case record to reflect the filing. The docket entry and the document image are both available immediately for viewing by all parties and the general public via the Web site. In addition, the filing attorney receives an immediate electronic acknowledgment. The system also includes electronic noticing for other parties who participate in the CM/ECF system.

## JEDDI Technology Vendors

As the interest in JEDDI has grown over recent years, a number of commercial technology vendors have emerged to provide JEDDI products. A few are start-up companies concentrating on electronic filing systems. Others are case management system developers who are now adding e-filing front ends to their existing line of products. A third group are more general technology or court services firms that are striking strategic alliances with other vendors to provide comprehensive solutions that include JEDDI technology.

Shown below are vendor profiles, reproduced from NCSC's on-line *Court Technology Vendors List*, for the more prominent commercial vendors of JEDDI systems as of this writing. This selection was not compiled through exhaustive market research or vendor surveys. It is based on available information about court projects, vendor profiles that have been submitted to the *Court Technology Vendors List*, and other informal sources. Moreover, the commercial court technology sector is quite volatile, with existing companies merging or being acquired, other companies dissolving or ceasing to develop JEDDI products, and new corporations forming. Indeed, some of the companies mentioned in the above project descriptions no longer exist, at least in the same form. The *Court Technology Vendors List* (<http://www.ncsc.dni.us/NCSC/VENDOR/Vindex.htm>) is a good source for current information on most companies that provide court technology products and services, including contact information and a description of the products and services they offer. In addition, the *Vendors List* groups subscribed vendors that have indicated some connection with electronic filing technology by specifying "electronic filing products and services" as part of their company profile. Most of these companies are not included in the selected profiles below but may be helpful to courts planning to implement JEDDI technology.

## NATIONAL CENTER FOR STATE COURTS

### Vendor Profile of JUSTICELINK, INC. (formerly LAWPlus, Inc.)

<p><b>Primary Contact</b> Mr. Edward H. Carlson Vice President, Sales &amp; Marketing JusticeLink, Inc. 11482 Luna Road Dallas, TX 75234 (800) 581-1035/Fax (972) 443-9797 e-mail: <a href="mailto:ed.carlson@justicelink.com">ed.carlson@justicelink.com</a> Internet: <a href="http://www.justicelink.com">http://www.justicelink.com</a></p>	<p><b>Alternate Contact</b> Mr. Jeff Jones Marketing Communications Manager JusticeLink, Inc. 11482 Luna Road Dallas, TX 75234 (800) 581-1035/Fax (972) 506-8267 e-mail: <a href="mailto:jeff.jones@justicelink.com">jeff.jones@justicelink.com</a></p>
<p><b>Product(s)/Service(s) Provided to Court</b> JusticeLink, Inc. (formerly LAWPlus, Inc.), enables electronic filing, electronic certified service, and electronic storage of documents generated by multiparty litigation suits. With its revolutionary Internet-based solution, JusticeLink provides a secure and reliable communications link between the court, firms, and others needing to file documents.</p> <p>For <b>judges</b>, JusticeLink provides electronic document management and improved access to case files, allowing the judge to spend more time administering justice. From the bench or chambers, a judge can view entire case files, issue orders, and notify parties, all electronically.</p> <p>For <b>court clerks</b>, JusticeLink reduces physical space requirements of document storage. Attorneys electronically transmit filings to the court clerk, eliminating manual document movement and enabling efficient use of staff.</p> <p>JusticeLink maintains accurate service lists for each case and provides public access to all electronic case documents through computerized search capabilities. JusticeLink helps improve work quality and speed, productivity, and cost-effectiveness for all constituents in the practice of law.</p>	
<p><b>Scope of Business</b> JusticeLink, Inc., is an innovative electronic legal document solutions company servicing the entire legal community and courts nationwide.</p>	

# NATIONAL CENTER FOR STATE COURTS

## Vendor Profile of WADE SYSTEMS INC.

<p><b>Primary Contact</b>  <b>Mr. Bryan K. Mossey</b>  <b>Vice President</b>  <b>Wade Systems Inc.</b>  <b>3705 West Memorial Road, Suite 1409</b>  <b>Oklahoma City, OK 73134</b>  <b>(405) 755-1885/Fax (405) 755-1447</b>  <b>E-mail: <a href="mailto:bkmossey@wadesystems.com">bkmossey@wadesystems.com</a></b>  <b>Internet: <a href="http://www.wadesystems.com">http://www.wadesystems.com</a></b></p>	<p><b>Alternate Contact</b>  <b>Mr. Jay Wade</b>  <b>Chief Developer</b>  <b>Wade Systems Inc.</b>  <b>3705 West Memorial Road, Suite 1409</b>  <b>Oklahoma City, OK 73134</b>  <b>(405) 755-1885/Fax (405) 755-1447</b>  <b>E-mail: <a href="mailto:jaywade@wadesystems.com">jaywade@wadesystems.com</a></b></p>
<p><b>Product(s)/Service(s) Provided to Court</b>  Wade Systems Inc. provides complete case management, document imaging, Internet-based remote public access, and electronic filing for the federal court system.</p>	
<p><b>Computer Environment</b>  Our software is Web-based and requires Windows NT on the server, Windows on the client with a Web browser, and Internet connectivity for remote public access and electronic filing.</p>	
<p><b>Scope of Business</b>  We sell our software solutions nationally to the U.S. Federal Court system and currently support over 50 federal courts around the nation to include the top five largest U.S. Bankruptcy Courts.</p>	

# NATIONAL CENTER FOR STATE COURTS

## Vendor Profile of WEST PUBLISHING CORPORATION d/b/a West Group

<p><b>Primary Contact</b> Mr. Thomas C. Leighton Vice President Government Relations and Contracts West Publishing Corporation 610 Opperman Drive Eagan, MN 55123 (651) 687-5676/Fax (651) 687-5686 E-mail: <a href="mailto:tom.leighton@westgroup.com">tom.leighton@westgroup.com</a> Internet: <a href="http://www.westgroup.com">http://www.westgroup.com</a></p>	<p><b>Alternate Contact</b> Mr. Thomas C. Leighton Vice President Government Relations and Contracts West Publishing Corporation 610 Opperman Drive Eagan, MN 55123 (651) 687-5676/Fax (651) 687-5686 E-mail: <a href="mailto:tom.leighton@westgroup.com">tom.leighton@westgroup.com</a></p>
<p><b>Product(s)/Service(s) Provided to Court</b></p> <p>West Group provides hardbound legal publications including statutes, case reports, and other legal publications.</p> <p>West Group provides:</p> <ul style="list-style-type: none"> <li>• Westlaw, computer-assisted legal research service consisting of over 10,300 databases containing legal and legal-related information</li> <li>• West CD-ROM libraries, including topical and jurisdictional libraries</li> <li>• Private file development for internal document management</li> </ul> <p>Westfile Electronic Court Filing Service, an Internet-based service in development offering tight integration with your court case management systems and providing comprehensive filing services to the attorneys, agencies, and members of the public who interact with your court. Contact Phil Ytterberg, Telephone: (651) 687-4557, E-mail: <a href="mailto:phil.ytterberg@westgroup.com">phil.ytterberg@westgroup.com</a></p> <p><b>FACT Member</b></p>	
<p><b>Computer Environment</b></p> <ul style="list-style-type: none"> <li>• Westmate–Westlaw communications software. Windows versions including stand-alone and networked versions. Other applications are also available.</li> <li>• Westcheck–Electronic citation checking and verification software.</li> <li>• Premise and Folio–West CD-ROM libraries software.</li> </ul>	
<p><b>Scope of Business</b></p> <p>West Group is an international company specializing in service to the entire legal community, including the courts. West Group works with all levels of courts.</p>	

## CHAPTER THREE

### *Why JEDDI Is Inevitable*

#### Introduction

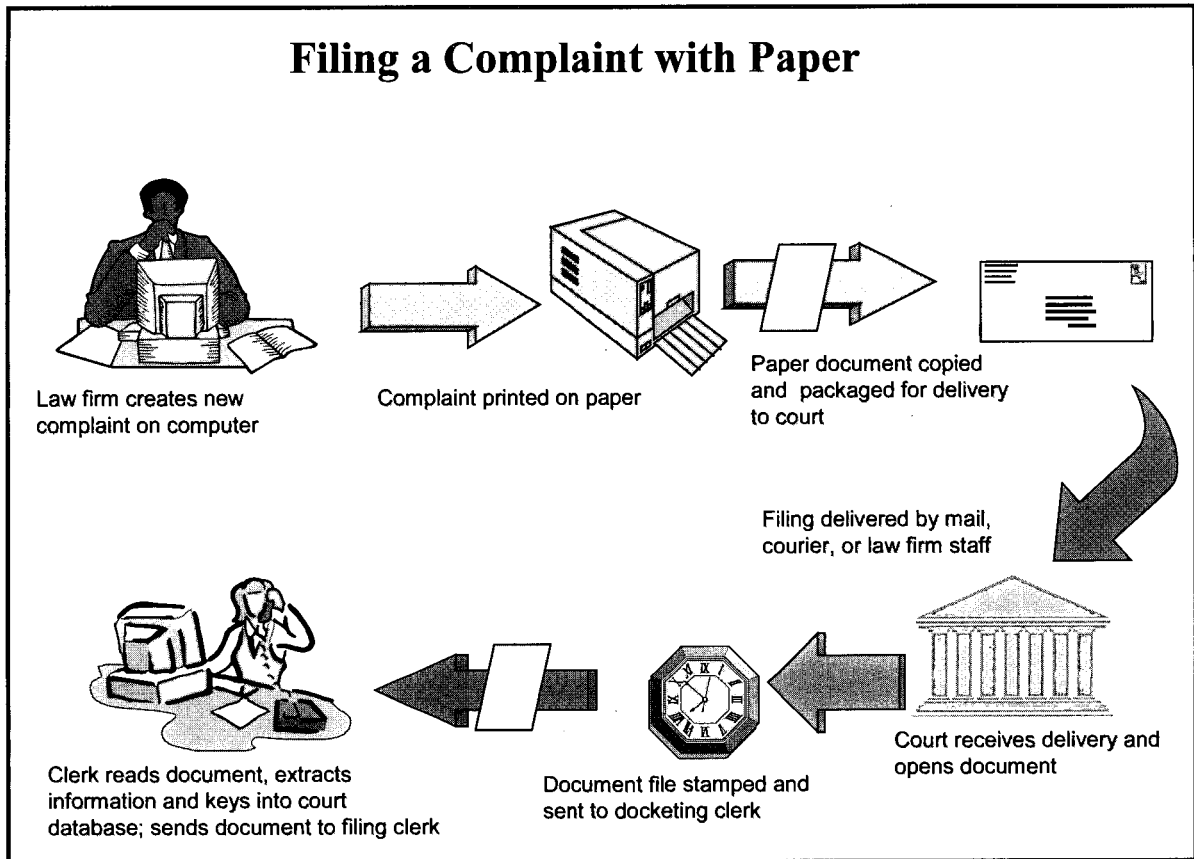
JEDDI has been evolving for almost two decades. Very slowly at first but with increasing speed and outreach, the JEDDI concept has tugged irresistibly at the minds of technologists and court visionaries. With the nearly continuous rise in volume and complexity of the paperwork involved in the judicial process, these progressive thinkers became increasingly convinced that technology and electronic communications could offer a better alternative to the flood of paper forms and documents. As the world of commerce and information services continued its pursuit of new technology solutions to improve the bottom line of business operations, those in the justice system who were watching witnessed example after example of the irrefutable advantages of electronic data interchange in the commercial sector.

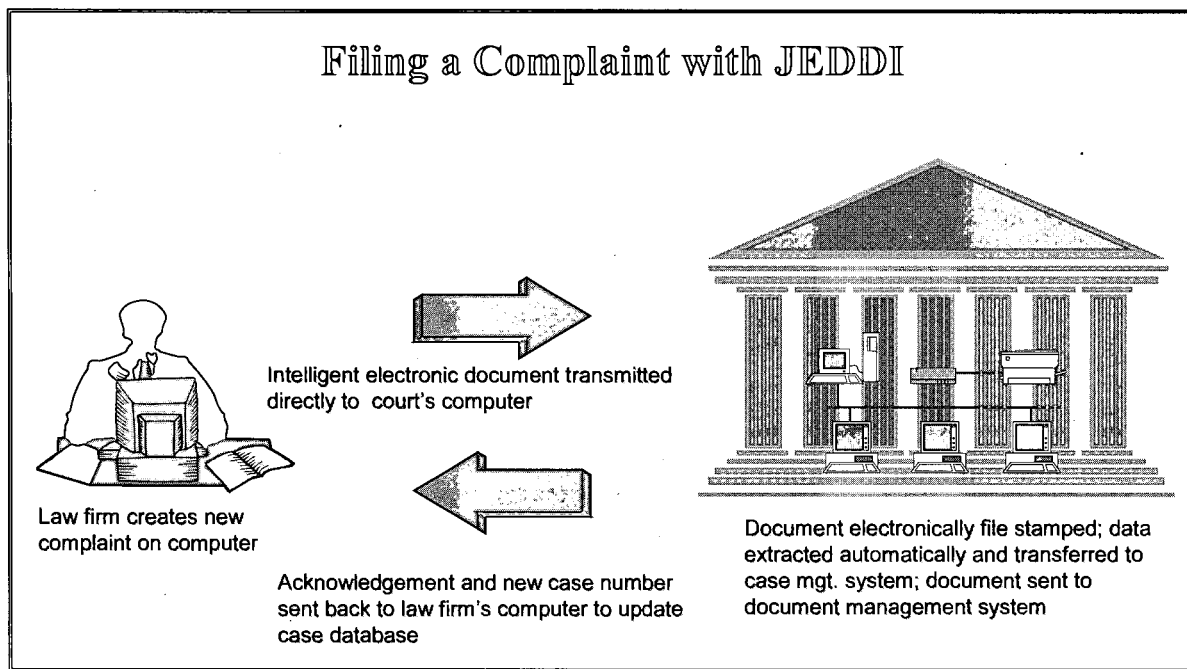
Despite significant impediments stemming from the necessity to protect and preserve the integrity of the legal process, a few courts began exploring the possibility of substituting electronic information exchange for some aspects of the paper flow. Many court officials began discussing the topic among themselves in their own communities and at state and national conferences. In state after state, groundbreaking work began on overhauling obsolete statutes and court rules blocking the introduction of electronic documents. Today, several individual courts and a few state judiciaries have active JEDDI systems in operation or in development. Hundreds more are planning for eventual implementation. Private-sector technology vendors are gearing up to offer JEDDI products and services, and courts are already using a few of their products.

A few skeptics remain unconvinced that paper court documents can be replaced, and numerous pragmatists believe the technology still is too immature to be adopted widely without compromising the quality of justice or endangering due process. At the other extreme, several pioneers, by implementing working systems, have demonstrated their conviction that JEDDI is practical now, despite its evolving nature and lack of standards. Overall, most court practitioners acknowledge that JEDDI is a logical and inevitable next step in the judicial system's growing dependence on technology tools to improve court operations.

Why is JEDDI—in whatever form—so obviously an inevitable step in the progressive application of technology to the courts? Simply put, the advantages this technology offers are far too compelling to ignore. The diagrams that follow illustrate the differences between most existing court operations (using paper files along with their automated case management systems) and a court operation with a JEDDI system in how an initial case filing would be processed. The differences are even more striking when the subsequent processes and activities are examined. The inefficiencies of the paper system and the additional capabilities of the electronic system add up to a compelling rationale for adopting JEDDI (especially an approach that includes electronic filing, electronic case records, and electronic public access). With

practically all court documents now being originated electronically, it is fundamentally illogical to continue converting them to paper for transportation and primary use and then converting them back into some electronic form through manual data entry or imaging. Not only is this approach highly inefficient, but the quality and availability of critical case information suffer greatly as well.





One way to explore the range of benefits JEDDI offers is to lump them into two categories:

- Cost advantages
- Improved information processing and accessibility.

Although these two categories are strongly interrelated, using them makes it somewhat easier to discuss both the justification for pursuing JEDDI and the long-range advantages it offers. The sections below examine these benefits and advantages more closely. The chapter closes with a brief discussion of how our changing society and public expectations are helping to accelerate the adoption of JEDDI.

## Cost Advantages

There are numerous costs associated with a paper-based court information environment. Most of these fall into either *processing costs* or *storage and handling costs*, although there is considerable overlap between these categories as well. Processing costs refer primarily to the expenses involved with retrieving information from paper documents, recording information on paper documents, and conveying paper-based information between individuals or different parts of an organization's operation. Storage and handling costs refer to the expenses associated with the physical storage of paper records, their retrieval for use, and their subsequent refile in the storage location. Both types of costs can be reduced considerably through effective implementation of JEDDI technology and related procedures, even though there are likely to be offsetting startup costs in the early stages of implementation. Moreover, the cost differential between traditional and JEDDI solutions will continue to grow, because the largest cost factor in both processing costs and storage and handling costs consists of human resources and directly related expenses. Whereas these costs will continue upward over time, the cost of technology is



dropping all the time. Court managers who must justify JEDDI primarily on the basis of cost may wish to conduct a cost-benefit analysis to project a risk-adjusted return on investment.

## ***Processing Costs***

Processing court documents involves several steps and consumes a considerable amount of clerical effort. Although some courts have conducted time-and-effort studies with implementation of some new program, organizational restructuring of the clerk's office, or process reengineering, traditional clerical processes have been regarded as an integral and inevitable part of most courts' operations. Yet the human resources costs resulting from these basic processes account for a significant percentage of the total court budget. Moreover, these costs are constantly rising because of inflation-driven salary increases, increased cost of personnel benefits such as insurance, and other personnel-related factors. Unfortunately, rising workloads generally require a corresponding increase in the number of staff positions necessary to process the cases.

### **A Case Study**

In 1997 the Shawnee County Court in Kansas conducted one of the few comparative cost studies that have been done in conjunction with implementation of electronic filing. This study did not attempt to encompass the entire range of costs and cost savings that may be involved in converting from paper to electronic documents. However, it is extremely valuable in pointing out the "raw" personnel savings that can result from the changes in the staff time required for performing the fundamental steps involved in processing filings after an electronic filing system has replaced the paper system.

The study identified nine processing steps involved in the typical filings for the type of case being considered:

1. Accepting the filing and collecting fees
2. Checking the petition for completeness
3. Entering data into the case management system
4. Issuing the summons
5. Signing the summons
6. Cashiering operations for the fees
7. Mailing the receipt
8. Filing the documents
9. Carrying summons to sheriff.

The study then measured the average amount of staff time required at each step for processing 100 *documents* (not cases) in the paper-based system and compared it with the amount of time required for electronic filing. The study found that processing 100 traditional, paper-based documents averaged 9.75 hours. Processing 100 of the same type of documents required only 8.8 minutes of staff time with electronic filing. Put another way, electronic filing

consumed only 1.5 percent of the clerical effort required for traditional paper processing. The eye-opening results are shown in the table below.

### Staff Time Required to Process 100 Documents in Paper-based and Electronic Filing Systems in Shawnee County, Kansas

Process Description	Paper-based Process	Electronic Filing	Staff Time Savings (in Hours) with Electronic Filing
	Staff Time Required (in Hours)	Staff Time Required (in Minutes)	
Case Filed and fees collected	1.00	5.5 minutes	0.93
Petition checked for completeness	0.75	Included above	0.75
Data entry	3.25	3.3 minutes	3.20
Summons issued	1.00	Included above	1.00
Summons signed	1.25	Included above	1.25
Docket fees rung by cashier	1.00	Automatic	1.00
Receipt mailed by attorney	0.25	Automatic	0.25
Documents filed	1.00	Automatic	1.00
Summons carried to sheriff	0.25	Automatic	0.25
<b>Total</b>	<b>9.75 hours</b>	<b>8.8 minutes</b>	<b>9.63 hours</b>

In theory at least, implementing electronic filing would free up approximately 1.2 staff days (9.63 hours) per 100 documents filed in the court. Assuming a typical pattern of 15 to 20 documents per case, electronic filing could save over 14 full-time equivalent (FTE) positions in a court with a caseload of 20,000 cases per year. The calculations for this theoretical savings are as follows:

**E-Filing  
required only  
1.5% of staff  
time required  
for paper**

- 20,000 cases per year X 15 documents per case = 300,000 documents per year
- 300,000 documents per year X 1.2 staff days per 100 documents = 3,600 days
- 3,600 days / 250 working days per year = 14.4 FTE positions.

## **Other Staff-related Savings**

Additional savings in staff time can be realized at other processing stages when a court community implements a JEDDI system. For example, notification of court dates or court rulings can take place automatically through electronic communications. The reduction in transcription errors and subsequent correction activities is another source of staff savings.

Another cost related to manual processing that sometimes is overlooked is that of the facilities to house the personnel and operations. For each staff member required, the court must provide a certain amount of office or work space, furniture and equipment, a parking space, and utilities such as lighting and heating and cooling. With traditional processing, therefore, an increased workload means increased demands on the facilities. Electronic document interchange and automated information processing can delay the need for new construction and slow some of the rising costs of operating current facilities.

## **Viewing Court Staff Savings Realistically**

It is important to recognize three facts regarding this discussion of potential staff savings:

1. There are likely to be one or more new staff positions necessary when a court moves toward JEDDI implementation. For example, additional technical staff may be required to develop, implement, and maintain the new systems and expanded capacity of the court's technology infrastructure.
2. The initial stages of implementation more than likely will include an increase in the actual workload. The learning curve; initial glitches in systems, procedures, and policies; and the need to operate dual processes during the transition all contribute to the temporary workload increase. In addition, many courts elect to convert existing paper files for some or all of their active cases to move more quickly into an all-electronic case environment. Even though they may phase in the conversion so that an individual case is converted only when a new electronic document is filed or some other case event occurs, the conversion process requires extra effort.
3. Finally, history has shown that courts do not lay off clerical staff when new technology increases efficiency. Some positions are diverted to other areas of the operation that are understaffed. Other staff move from routine, labor-intensive tasks to apply their skills and knowledge at a higher level to improve the quality of case information and court services. The savings occur through normal staff attrition and through cost avoidance, as higher volumes of work can be absorbed without commensurate increases in staff.

## **Reduced Processing Costs for Law Firms**

It also is important to note that law firms also can enjoy some degree of savings in processing costs after they convert from paper to electronic documents. Some of the most apparent savings can be achieved on the front end—the document-preparation-and-filing process. A law firm can eliminate many labor-intensive steps associated with filing pleadings on

paper by implementing electronic filing. A study of local law firms in Prince George's County, Md., estimated the cost of preparing a paper pleading for filing by mail at about \$25. This estimate included printing, copying, preparing an envelope, and paying postage. It did not include the substantial additional cost of more direct delivery methods, such as courier service, overnight express delivery, or hand delivery by law firm staff.

### *Storage and Handling Costs*

Paper files consume significant resources even after the documents are filed and processed in the clerk's office. Paper files are both bulky and fragile, requiring special provisions to store and protect them. Courts spend considerable sums each year on housing their files and making them accessible, even though many of these costs are not apparent at first glance. Often it is only when a court outgrows existing facilities that such costs begin to be identified and calculated.

#### **Storage Space**

Storage for files consumes valuable square footage in most courthouses. Files for active cases must be close at hand to minimize delays, yet weight limits and accessibility requirements may dictate how densely files can be housed. New courthouse construction costs average over \$200 per square foot nationally and reach as high as \$300 per square foot for more expansive designs or for buildings in some urban locations. Typical leased space may cost up to \$15 or more per square foot annually. In addition, file rooms must be maintained within temperature and humidity limits, and they must be equipped for fire detection and suppression. Security concerns may impose further square footage or equipment requirements on file storage areas. With such facilities-related costs increasing steadily, it is readily apparent that substantial cost savings or cost avoidance may be realized by replacing paper files with electronic ones.

#### **Equipment and Supplies**

There are additional hard costs associated with paper file storage other than expenses related to the space itself. For example, suitable file cabinets or shelving must be purchased, installed, and maintained. Many courts have expensive and complex mechanized file systems to improve the efficiency of their paper record storage and retrieval. Moreover, all good filing systems require special folders, fasteners, and labeling devices. Bins, racks, trays, and carts are required to organize paper documents and records during different operations and to transport them from location to location. Sufficient photocopying equipment must be bought or leased to ensure that a record can be made available where needed without making the file unavailable to others. Courts purchase reams upon reams of paper annually to accommodate paper-based operations. Finally, many courts have installed microfilming equipment or have contracted with microfilming services to make archival copies of their paper records.

#### **Handling Costs**

On top of the physical storage and other hard costs, personnel costs for handling the paper files account for a surprisingly high percentage of a court's total operational expenses.

File management requires substantial staff time, especially in large general jurisdiction courts handling a high volume of complex cases. Clerical effort is expended routinely on creating physical files, pulling and filing case jackets for court events, adding new documents to the case jackets, maintaining file-indexing systems, purging inactive records and sending them to secondary locations or archiving stations, and tracking the location of files in use throughout the court. Even in a court with a good automated case management system, paper files are needed any time a document must be examined or the case goes to the judge for action. Retrievals and subsequent refiling consume many staff hours each month, as does the actual transportation from one location to another. In addition to costs for routine handling, lost or misplaced files require additional staff time, both for the effort required to track down and retrieve the missing information and for the delays and disruptions caused by the file's unavailability. Although courts usually recover the cost of copying records for outside parties through a copying fee, many hours of staff time are also consumed in making copies required internally. Microfilming operations in many courts also require several staff positions.

### **A Case Study**

The Circuit Court of Prince George's County, Md., conducted an assessment of costs associated with storage and handling of paper records several years ago. The results of that study drive home the point that traditional court procedures based on paper records impose a significant premium on the cost of court operations. The study reflects a court with ten judges handling about 20,000 cases per year. The cost calculations are based on personnel and other costs in Prince George's County at that time (see results below). Perhaps the most surprising aspect of the study's findings is the enormous expense associated with routine "case pulls" necessary to move the case record to where it was needed in the court. In this study, the average case was pulled at least five times per year at a cost of approximately \$4.00 per pull (including all operational costs for retrieval, transportation to and from the destination, and refiling). Electronic case files and related automated procedures essentially eliminate this expense.

**Estimated Annual File Storage and Handling Costs  
Circuit Court of Prince George's County, Md.**

237 file cabinets / 20 year life span	\$1,279.80
1024 sq. feet of storage space @ \$15 per year	\$15,360.00
20,000 folders with fasteners @ \$18.59 per box of 50	\$7,436.00
3.8 million pages of paper @ \$5.29 per ream	\$40,204.00
Lost file costs @ 150 hours per judge (10 judge court)	\$34,095.00
File transportation costs @ 5 pulls per case per year	\$400,000.00
Heating and cooling costs @ \$1.50 per sq. ft per year	\$1,536.00
Copy costs @ 25 copies per case x 5 cents per copy	\$25,000.00
Estimated archiving microfilm cost	\$10,000.00
Paper shredding cost of 2% of pages (76,000) @ \$1.00 per pound	\$1,013.00
<b>Total per year for 20,000 cases, using file cabinets</b>	<b>\$535,923.80</b>
Cost per square foot using file cabinets	\$523.36
Open shelf filing - storage savings (lower cost units)	\$200.00
Open shelf filing - space savings (40% more efficient)	\$68,897.00
Open shelf filing - heating and cooling savings (40% less space)	\$614.00
<b>Total per year for 20,000 cases - open shelf</b>	<b>\$466,212.80</b>
Cost per square foot per year using open shelf (614 sq. feet)	\$759.30

## Improved Information Processing and Accessibility

### *Improved Information Processing*

Many improvements are possible in the processing of court information when a well-designed, comprehensive, and integrated JEDDI system is adopted. A number of labor-intensive manual steps associated with paper records are eliminated, and information flows more quickly to the next step. In a properly designed system, electronic documents facilitate automatic processing for other aspects of the operation that formerly required human intervention and data entry. Although the most dramatic improvements are seen within the clerk's office and other areas of the court, law firms can enjoy similar improvements in their operations, especially if they integrate JEDDI with their internal automated legal systems.

### Reduced Document Handling

A JEDDI system sharply reduces document handling, even leaving out the case pulls. Clerks spend tremendous amounts of time handling paper filings that come across the counter (opening, stamping, logging, routing, etc.) and additional time handling court-originated documents such as orders and judgments. Electronic documents eliminate most of these steps, and automated procedures simplify others. Furthermore, copying documents and court records for different uses nearly disappears. Information retrieval is another operation that requires

much less clerical effort in a JEDDI system. Clerks do not need to handle any paper documents to obtain information from the case record. In the first place, a substantial portion of information retrieval becomes a self-service process, because the electronic records can be made available to both court staff and remote users. Even when the clerks do need to retrieve information, improved text-searching capabilities and automated tools simplify the process and deliver the information almost immediately.

### **Reduced Data Entry**

Manual data entry also is greatly reduced in JEDDI systems. Intelligent electronic documents in a properly designed system permit automatic extraction of data fields to populate the case management database and “trigger” subsequent activities. They are self-docketing in that they carry with them in machine-readable format the information needed to create the appropriate entry in the automated register of actions. This information also enables the documents to be indexed properly and stored in the document management system without human intervention (subject to the court’s administrative rules for review of filings). In addition, totally electronic court records reduce the transcription and data entry steps needed to record court actions and generate orders, judgments, and other documents. Finally, the dual data entry frequently required for tracking files in paper systems disappears completely.

### **Improved Workflow**

Electronic documents and case files permit courts to reengineer their processes and improve workflow significantly. In a traditional court environment, a paper document that requires processing by multiple parties usually goes through a sequence of steps, moving from desktop to desktop and sitting in queues until the individual responsible for the next step can get to it. Many traditional clerk’s offices were arranged physically to reflect or attempt to optimize the paper flow. These sequential steps greatly reduce the availability of a document, especially if it is sitting at the bottom of an in-basket. To make matters worse, often the entire case record must be pulled for reference during certain steps in the processing of a new document. Electronic documents and case records enable courts to avoid such bottlenecks and maintain the availability of records. In addition, workflow can be greatly streamlined through elimination of numerous manual steps and automatic routing of work electronically to the appropriate staff.

While most of the improvements in processing have been discussed in the context of court operations, law firms also can realize numerous improvements in preparing, transporting, and retrieving electronic court documents and case records. Law firms can reap the benefits of automated data entry and improved workflow within their organization, especially when their legal systems are fully integrated with the court’s JEDDI system. For example, electronic noticing and access to the electronic court docket can save many steps in preparing and retrieving information. In addition, however, electronic notices and electronic documents transmitted by the court can be made to trigger automated procedures in the law firm’s system.

## *Improved Information Accessibility*

JEDDI systems—especially those based on intelligent documents and totally electronic case files—can provide tremendous improvements in the tools available to help users locate and retrieve the exact information they need in its most useful form. Information accessibility encompasses several related ideas. In this section these components are categorized as availability, retrievability, and quality.

### **Improved Availability**

When a court adopts electronic documents and case records, its entire file room (at least for active cases) is online. One tremendous advantage of electronic records is that they are available to multiple users simultaneously. One person's use of the case file no longer removes it from circulation or availability to others. Another advantage is that online records can be made available to users on a 24-hour/7-day basis if desired, except for possible brief disruptions for system maintenance. Furthermore, JEDDI systems can make electronic records accessible from anywhere inside or outside the courthouse. This means, for example, that if an unexpected need for a particular case file or document arises during a court session, the electronic record can be retrieved immediately without delaying the proceeding. Perhaps more important, judges and attorneys can access the records from their homes and offices, from other courts in the district or around the state, or from more distant locations while attending conferences or other functions. Moreover, they can get to them any time of day or night, regardless of whether the courthouse is open or their staffs are available to help them by telephone.

Abandoning paper court records has some less obvious advantages of a very practical nature. Lost documents or damaged files that often hamper the availability of information in paper systems are not a problem in properly designed JEDDI systems. Physical wear and tear are eliminated entirely. No amount of retrieval, reading, or copying can damage an electronic file. While spilling coffee, whiteout, or nail polish on a computer may be costly (although current equipment is far less vulnerable than older models), it is trivial compared with the damage such an accident can cause to a paper court file.

### **Improved Retrievability**

Powerful software tools can greatly enhance the ability of users to locate, select, and retrieve the precise information they need for a particular purpose. Furthermore, even if complex search-and-selection criteria slow the speed of retrieval, it is blindingly fast compared with manually retrieving information from paper files. When each text-based document is stored electronically in addition to the information in the case management database, the entire case record becomes text searchable. Context-sensitive search engines using Boolean logic and other techniques can locate specific information buried deeply in the case file (although they are far from perfect and may retrieve irrelevant information). This permits users to find a particular case or document when, for example, they can only remember it by some obscure word or phrase that would never appear in any ordinary case index. Once a desired document is located, the specific phrase, paragraph, or section can be highlighted, and the extract can be electronically copied and pasted into a working document or other application. In addition to locating



information, software tools can sort, prioritize or rank, and format the information in whatever manner the user wants it to be presented.

### **Improved Quality of Information**

JEDDI systems can provide a higher quality of information to court users than is easily attainable with typical case management systems combined with paper case files. Information is enhanced simply by having it all consolidated, with the entire record and all documents available together at any time. Every user can work with a complete set of consistent information. The information in a well-designed JEDDI system also is likely to be more accurate. Electronic documents eliminate many opportunities to introduce transcription errors, improperly index information, misfile documents, or inadvertently obscure information with a stray mark, stain, or misapplied file stamp. Furthermore, the built-in validation and editing routines in the software used to create, transmit, and process intelligent documents can help prevent erroneous, inappropriate, or incomplete information from ever getting into the record. Another key benefit is that the information contained in electronic case documents is available in text form, making it much more usable than either a paper document or an electronic image. For example, targeted pieces of information can be located, extracted, assembled, copied, and pasted as character-based text.

JEDDI systems unlock the potential for court records to include even more information and more-effective forms of information. Hypertext links can permit records to be structured in a drill-down arrangement supporting both a hierarchical and tangential method of presenting information. In addition to giving the viewer instant (but optional) access to related information in other sections of the document or relevant information in other documents in the same case record, links can provide direct access to external sources cited in the document, if permitted by court rules. As powerful as text—especially in hypertext constructs—can be, the inclusion of rich multimedia components, such as full-color graphics and audio and video material, can greatly improve the quality of the information that can be conveyed to the user. (Chapter Four discusses this aspect of electronic documents in more detail.)

### **Public Expectations**

Another reason that JEDDI is inevitable is the sweeping movement toward a “wired society.” The Internet has opened the floodgates for electronic interchange as no technology in the past could ever do. From simple swapping of e-mail notes to online shopping, banking, and filing of income tax returns, individuals routinely turn to electronic communications to obtain information or to provide information needed by others. The dramatically lower threshold for affordable technology, ready availability of Internet service providers, and explosion of Web sites of all descriptions have combined to create among the general public the expectation that information from all sources will be available online. If ordinary citizens can sit at a home computer and look up legislative bills under consideration, download tax forms from the IRS, take out a home mortgage, and select and purchase the week’s groceries to be delivered to the doorstep, why should they tolerate a court system that requires them to drive downtown, find a parking place, and stand in line at the clerk’s counter to obtain public court information?

Indeed, progressive courts already have used the Internet extensively to answer the need for better public service. Hundreds of courts have Web sites that provide electronic public access to information ranging from static items such as court hours and location to dynamic information such as calendars and indexes. A few courts are linking their Web sites to their case management databases, permitting viewers to retrieve case-specific information such as registers of actions and names of parties and their attorneys. The availability of case information, in turn, is fueling the appetite for remote access to complete case records and documents.

Expectations for the justice system encompass more than just benefits to individual users within the court system. Increasingly, the general public has come to expect courts not only to provide improved public service and reduce delay, but also to operate more efficiently in general through the application of current methodologies and technology. Citizens are surrounded by technology in their own workplaces, in their daily interaction with both commercial and government organizations, and even when simply ordering a lunchtime hamburger from a fast-food restaurant. Despite the traditional nature of the judicial process, they expect the business side of courts to operate smoothly and cost-effectively, with appropriate use of technology tools and systems to stretch tax dollars as far as possible. The pressure from all of these public expectations can be a significant force in the growing JEDDI movement.

## CHAPTER FOUR

### *The Nature of Electronic Documents and Their Implications for the Judicial System*

There is much more to the concept of electronic documents than perhaps first meets the eye. While assessing the substantial gains in efficiency and improved service that JEDDI promises, judicial leaders also must consider the characteristics of electronic documents and the significant change in thinking that their adoption implies. Moving to an electronic format redefines entirely the nature of a “document” as it has been known for the last five centuries. Freedom from the constraints of the printed page makes the notion of paper size, page length, page limits, book and page number, bindings, and other specifications somewhat meaningless. Moreover, while paper documents retain the same appearance to all readers, electronic documents can be displayed differently to different readers for different purposes. An even more profound truth is that electronic documents do not have to present information sequentially or in only one order. Instead, they can permit a viewer to navigate through the information they contain (or reference) in a variety of ways.

#### Types of Electronic Documents

The implications of the JEDDI concept depend upon the definition of an electronic document that is being applied. JEDDI systems that have been installed or are under development today use a variety of electronic representations and technical approaches to package and transmit information between entities in the judicial system. In the broad sense, electronic documents may be word processing files (with or without templates attached), plain ASCII text files, fax files, image files (in a variety of formats), HTML Web files, XML files, or proprietary formats, such as Adobe PDF, which specifies a protocol for accurately preserving original format and content while providing limited text capabilities. Perhaps the two major categories into which most electronic document schemes fall are image-based and text-based documents.

#### *Image-based Electronic Documents*

Technically, an electronic document can be simply an electronic representation of a physical paper document. In fact, an electronic document can consist of a computer file storing a set of digital images—each one an exact picture of the corresponding page in the original paper document. When accessed through the appropriate software, the digital file can faithfully reproduce on a computer screen not only the image of the printed text but handwritten signatures, stray marks, staple holes, stains, and smudges, as well. The electronic document can be read on the computer monitor or printed out on paper.

Filing via facsimile transmission is a crude example of an application of this type of electronic document. While the quality of a faxed document is poor, reflecting both loss of detail and frequent introduction of extraneous marks, the fax technology does attempt to reproduce the appearance of the original document. Document imaging systems serving as components of a JEDDI system generally produce much higher quality images than fax technology, although sometimes compatibility issues must be resolved between the equipment used in law firms and the system in place in the court. With a proper system design and appropriate hardware and software, document imaging systems can deliver surprisingly good results, especially when large-screen, high-resolution computer monitors are used. Documents printed from such systems are sometimes hard to distinguish from the originals.

It is interesting to note that, although they are based on similar technologies, facsimile transmission and imaging systems initially were implemented for somewhat opposite purposes. Fax transmission was used to move a paper document electronically between a law firm or other outside location and the court, with it once again being printed as a paper document at the receiving end. On the other hand, the primary motivation for implementing most court imaging systems was to convert paper documents that had been delivered through traditional methods into their electronic representation for purposes of storage and access. Nevertheless, except for the potential to convert an image file to text through OCR (optical character recognition) technology, both fax and imaging systems serve mainly to create a digital picture of a paper document (yes, it is quite possible to generate either a fax or high-quality image file directly from an electronic text file such as a word processing document).

The narrow definition of an electronic document as a digital image gives rise to two questions. On the one hand, how important is it always to preserve all of these bits of information about the appearance and physical characteristics of a document? On the other hand, what other valuable capabilities might other types of electronic documents have?

Few would argue that when it comes to evidence and exhibits, it can be very important to reproduce all of the characteristics of the original if that evidence or exhibit is to be stored and displayed electronically. But what is sacrosanct about the exact format and surface appearance of ordinary pleadings filed by a recognized attorney as an official case document? The purpose of the pleading is to convey information clearly and completely to the court and other parties. So long as that information can be authenticated as having come from the attorney who is indicated as the filer, and the information itself is unaltered, courts should be interested in the most effective methods for transporting that information among parties and conveying its meaning clearly. In that sense, electronic documents can do a much better job if they are not simply pictures of paper documents, but instead are text-based files.

For the immediate future, image-based documents will be a necessity for many courts. Specialized JEDDI systems that deal with a single case type or a single filing entity may have no need for images. Likewise, courts may avoid document imaging by running a dual system that maintains paper files for existing documents and for filings from parties that do not participate in the electronic system (although such an approach is not advisable). Overall, however, imaging systems will continue to have a very important role in most JEDDI implementations. In the first

place, they permit existing case documents in active cases to be converted to some form of electronic document. This step enables the court to make the transition to completely electronic case files, whereby all contents of the traditional file folder are maintained and accessed in electronic form. Second, document imaging systems allow future exhibits that exist only on paper to be captured electronically. Another important consideration is the need to accommodate *pro per* filers who do not have the ability to use the electronic system. Although public workstations and kiosks are potential solutions that may permit the general public to file electronically, most courts would view a requirement to do so as an unreasonable burden. In all likelihood, document imaging systems will be around for several more years.

### *Text-based Electronic Documents*

Text-based electronic documents generally are files containing standard ASCII code representing characters (as opposed to digital bitmaps representing images). In addition to the words in the document, the file can include control characters and electronic “tags” to specify formats or other instructions the computer system can use to determine how to display or interpret the text. This representation permits the construction of electronic documents that are sometimes called “smart” or “intelligent” documents. Such documents are far more than merely the electronic equivalent of an ordinary paper document. They can contain information that is both more accessible and more flexibly organized than is possible with a paper document. In addition, that information is machine readable, able to be identified readily and extracted automatically by the court’s computer upon receipt of the document. When the efficiency of the process itself is factored into the equation, the power of electronic documents becomes even more obvious.

Indeed, the potential capabilities of text-based electronic documents have far-reaching implications. Electronic documents provide the opportunity to organize and display information very effectively. There is seldom any single, specific order in which a comprehensive set of information must be approached by a party seeking to understand that information. As educational psychologists have proven, different people have different methods by which they acquire and assimilate information effectively. Paper documents force the reader to proceed sequentially. Although there is some ability to skim ahead and read thoroughly only those sections that are of greatest interest, even the skimming process requires sequential reading of the information, however superficially.

Universities and research labs began developing and experimenting with improved methods for constructing and navigating computerized text files some thirty years ago, applying the term “hypertext” to these non-sequential constructs. It was not until the recent advent of the Internet and the World Wide Web, however, that the general public was introduced directly to this radically different way of organizing and accessing information. With HTML documents, viewers of a Web page seldom read information sequentially throughout the Web document. Instead, they take advantage of navigation features that permit them to jump around to different points in the page, to different pages, or even to other Web sites. Hypertext linkages not only draw attention to potentially important pieces of information, but also provide the viewer with an almost instantaneous method for retrieving additional information about a particular topic that is

highlighted. Yet if the topic is not of immediate interest, the viewer is not forced to read through it.

Tapping this ability to structure data in a hierarchical fashion is often referred to as a “drill-down” approach. Beginning with a high-level summary of a given set of information, such a structure permits the reader to select the most appropriate order for pursuing more in-depth information about each particular topic that is represented in the overview. From a secondary level of detail, the reader then can choose to proceed into further and further levels of detail, until either no further information is desired or no further information is available. This structure, when combined with hypertext’s ability to let the reader/viewer explore tangential information threads as desired, can make a document meet a variety of needs. Perhaps the closest approximation to this concept in a paper document is a combination of the table of contents, a subject index, and footnotes on individual pages. However, these paper-based mechanisms cannot begin to approach the power and effectiveness provided by the electronic medium.

## **Implications for the Judicial System**

The judicial system is just on the threshold of realizing the powerful implications that accompany a move into the world of electronic documents. Early implementations of JEDDI systems have taken a very conservative approach to electronic documents. Whether image, PDF, or text based, most seek to preserve the appearance and format of what the attorney creates. Moreover, most retain the characteristics of traditional paper-based court documents, conforming to margin, page length, font, line spacing, page numbering, and other specifications developed by the courts, often many years ago. Such constraints are reasonable and necessary for paper documents to ensure their readability and control their size. However, these same constraints are somewhat artificial when applied to electronic documents.

Electronic documents free us from the limitations of an 8 ½ by 11-inch, two-dimensional, sequential medium. Consider, for example, how meaningless are the concepts of page length and number of pages for HTML documents viewed through a Web browser. A Web page can be of virtually any length, and the viewer easily can scroll seamlessly up or down its entire content. Only when the Web page is printed on paper do length and number materialize. Moreover, left and right margins are more a function of the browser characteristics and PC settings than of the document itself, unless the author chooses to specify, for example, table boundaries to control the appearance. Even then it is the viewer’s browser that determines exactly how it will look. When courts begin making full use of available technology for working with electronic documents, many existing standards will not be applicable.

## ***The Coming Transformation of Court Documents***

As the judicial system becomes more comfortable with JEDDI and begins to tap more deeply into the advantages that electronic documents offer, the nature of court documents will undergo a significant transformation. Future pleadings may be in the form of intelligent documents consisting of “packages” of electronic files. Such documents will be capable of

automatic processing by the court's computer, spawning automatic docketing and database updates, electronic noticing, and workflow routines to an extent not possible with current systems. Further, the documents likely will be capable of presenting information to readers using hypertext techniques and navigation tools. Through such tools and multidimensional layouts, the document can permit each viewer to access the content of the brief in the most individually effective manner. In addition to using the navigation capabilities, viewers routinely will "zoom in" on certain portions of the document and apply electronic highlighting to selected sections of text.

Comprehension of the facts and position being presented in the brief can be heightened further by including multimedia-rich information, such as diagrams, photographs, digitized audio recordings, and even video clips. Indeed, all exhibits other than physical objects could be included in the package as electronic images, text files, or multimedia files. Each exhibit could be hyperlinked to every place in the brief that contained a reference to that exhibit, making it simple to view the exhibit being discussed in the section. Suppose, for instance, that one section describes a complex procedure. By clicking on a highlighted hypertext link or a graphical button icon, the judge or other reader could view a narrated video clip illustrating the procedure. Similarly, clicking on a transcribed passage might play a digital recording of the speaker saying the words. Depending upon the court rules, hypertext links would not necessarily be limited to sources included in the package. For example, exhibits could be stored electronically in a designated location on the court's server and referenced there by links embedded in briefs and other documents in the case. Furthermore, case law cited in the brief could be referenced by a hyperlink to an external Web site or legal research database.

### *Early Examples of this Transformation*

The judicial system already has begun the transition to multimedia electronic briefs. Federal court cases have led the way with appellate briefs filed on CD-ROM. The first "cyberbrief" filed in the U.S. Supreme Court was submitted on CD-ROM in October 1996 by Schnader Harrison Segal & Lewis LLP. This brief was filed on behalf of the American Association of University Professors and twenty-four other organizations as "friends of the court," supporting the position of the appellee, the American Civil Liberties Union, in the famous case addressing the constitutionality of the Communications Decency Act. Although this brief did not include hypertext links to case law, it broke new ground in demonstrating how effective electronic briefs containing multimedia material can be in conveying information to the court. The brief contained hypertext links to display exhibits consisting not only of text references but also numerous color images of photographs. Even more striking was the inclusion of audio files and full-motion video clips. Finally, the brief included links to external Web sites that were listed as exhibits in the brief.

In July 1997 the U.S. Court of Appeals for the Federal Circuit accepted a brief on CD-ROM that was filed in the appeal of a patent case. Briefs on CD-ROM had been filed earlier in this court, but were not accepted because appropriate procedures were not followed. The CD-ROM brief used HTML and Web browser software to present the material. Hypertext links provided the ability to navigate throughout the brief and display referenced text.

### ***Courts Must Prepare for This Change***

Moving from the familiar world of paper-based documents into this brave new world of electronic documents does not mean that courts no longer will impose standards for their submission. Although paper size, number of pages, and other physical standards no longer apply, there must be rules to control electronic documents as well. For example, courts may have to impose limits on the number of words or characters that a brief may contain. They may have to develop some restrictions on the hypertext constructs to ensure that they enhance, rather than diminish, the document's readability. It may be necessary to limit the number of external linked references, or to provide secondary sources in case a link is no longer valid because the external Web site has changed. In addition, courts will have to determine what kind of multimedia material can be included and how they will allow that material to be linked and accessed by the viewer.

Clearly, the concept of electronic documents—when examined without imposing the confines of traditional judicial operations—will be one of the most powerful ever to affect the judicial system. The resulting changes in the practice of how briefs are filed, recorded, and read will require careful thought and, in all likelihood, many years to work out completely. The potential benefits, however, are tremendous. Substantial operational efficiencies can be gained through automated processing of the information contained in electronic documents and the elimination of physical document handling. Perhaps more important, these new approaches also can enhance the quality of justice by improving access to information and empowering judges and other parties to assimilate and comprehend critical case information more easily and completely.



## CHAPTER FIVE

### *Format and Transmission Alternatives*

A fundamental question arises in making the transition from paper to electronic documents: how should electronic documents be transported or transmitted between parties? The answer is neither singular nor simple. As technology continues to evolve, moreover, the answer also must evolve.

#### Transmission Media and Methods

Electronic documents can be moved from one location to another through a variety of methods that include physical media as well as electronic communications technology.

#### *Physical Media*

Early efforts to use electronic documents usually involved exchanging information by floppy disk. For example, a law firm might draft an order as a word processing document and submit it on a floppy disk for the court to edit, print, and sign. When the Northern District of Ohio piloted electronic filing, it permitted attorneys to submit their briefs on floppy disk if they could not connect with the Internet to submit them online. More recently, the CD-ROM has been used to submit lengthy electronic briefs to courts, especially when the brief contains hyperlinks or multimedia information. With a capacity of 650 megabytes, CD-ROMs permit a very high volume of information to be exchanged, copied, and retrieved by multiple parties at a very low cost and with nominal storage requirements.

The downside to using physical media to exchange electronic documents, of course, is that the physical disk or other device must be transported between locations, just as paper documents must be delivered. In addition, accessing the data requires human intervention after the storage device arrives at its destination. Consequently, many of the disadvantages of the paper system remain, even though the document itself retains its electronic format throughout the exchange. For example, with electronic documents on disk, there still is a significant time lag between preparation of the document by a law firm and its receipt by the court. Delivery remains limited to court business hours. Even if it arrives before the court closes and is file-stamped, the disk may not be loaded into the court's system until the next business day, at the earliest. Service of process remains a problem. Finally, clerical effort is required to handle the physical media, even though it is much less than that required for paper.

## ***Electronic Transmission***

### **Fax**

Electronic transmission of documents can be accomplished through a variety of methods. Facsimile transmission was one of the first methods used to move documents electronically, and it is still frequently used for many purposes. Unfortunately, the most common practice continues to be that of printing a document, placing it on a standard fax machine, and transmitting it to a fax machine at a second location, where it is printed out as an inferior copy of the original. This paper-to-electronic-to-paper exchange circumvents most of the disadvantages of physically transporting either paper or disks; however, it offers none of the benefits of electronic documents. The process improves somewhat if the originator faxes the document directly from his or her computer, or if the recipient receives the document through a fax server or fax modem and stores it electronically, albeit as a low-resolution image file.

### **Direct Dial-up Telecommunications**

A second method of electronic transmission involves computer-to-computer exchange through a direct dial-up connection. Many electronic public access systems still use this method to deliver documents or information from the court database to subscribers. Some electronic filing systems rely on this method to permit attorneys to connect directly with the court's computer to file briefs online. This approach offers the advantages of both electronic documents and electronic transportation of those documents. Moreover, it may provide enhanced security for those transmissions when compared with transmitting over a public network such as the Internet. The chief disadvantages are that the court is required to maintain a bank of modems and phone lines and a proprietary communications method must be established between the court and all participating parties. An attorney who practices in multiple courts might be required to buy, maintain, and learn to use a different communications software package for each such system. An alternative to direct dial-up connectivity is using a commercial, third-party provider for electronic filing and information retrieval. Under this scenario, the attorney subscribes to the service, which provides the law firm with a direct dial-up telephone connection (or even a dedicated line for high-volume users) for filing and retrieving information. The service then connects with the court through a high-speed communication line or an Internet interface, passes the electronic document to the court's case management and document management systems, and retrieves information from the database and document servers for its subscribers.

### **Electronic Mail via the Internet**

Undoubtedly, the most ubiquitous form of general electronic interchange today is electronic mail. E-mail has been around for many years, locally on networks in individual commercial and government organizations, through subscriber services such as America Online, and, more recently, on the vast global network known as the Internet. An incredibly useful tool, e-mail delivers millions of messages to desktops daily, ranging from simple and informal notes between individuals to mission-critical files containing text, graphics, software programs, and audio and video files. Similarly, e-mail has been used by most of the early JEDDI projects to one extent or another. E-mail transmission over the Internet permits a variety of mail programs

to be used by different organizations in the justice community with a relatively high rate of success in exchanging messages, providing that certain basic standards are observed. E-mail messages can carry documents and other files as attachments, subject to the size limitations imposed by e-mail gateways at each end of the connection. The software is easy to use and already familiar to most JEDDI participants because it is used for many other purposes.

### World Wide Web

The World Wide Web arguably has done more to connect courts with their constituents than any other technology advance in history. Court Web sites have sprung up like wildflowers as the Internet has continued its phenomenal growth. Tens of millions of individuals in this country alone log on daily, using their Web browsers routinely as the point of access to information related to every aspect of their lives, from in-depth research needed in their jobs to the current weather report and traffic conditions. Many do online banking, shop for goods and services, and file their tax returns through the Internet. They have come to expect courts to provide information through this venue as well. Many courts have obliged by posting general information, such as location, contact information, and an explanation of where citizens should go for specific needs. Some courts then made available information that changed daily, such as court calendars. A growing number are now beginning to post case-specific information for public access, such as indexes, registers of actions, and even individual case documents.

Indeed, the Web provides that Holy Grail long sought by information system developers—a universal, user-friendly, two-way interface. It has enabled court technology managers to provide information from their automated systems to internal court users, outside agencies, and the general public without much concern for what hardware platform or operating system they use. Moreover, a Web interface can be developed relatively easily for both legacy court systems and those built using the latest database and client-server technology. The interactive nature of the Web makes it a natural choice for electronic filing and related JEDDI initiatives. In addition to ease of navigation, text-searching capabilities, and other benefits of an interactive interface, the Web permits users to organize, format, and transmit data to the court by filling out online forms, uploading documents, and performing other actions through their Web browsers.

## Alternative Approaches to Electronic Documents

Given the widespread availability and ease of use of the Internet through e-mail and the World Wide Web, what are the possible approaches to implementing a JEDDI system? One major distinction is between “dumb” documents and “intelligent” or “smart” documents.

### *Dumb Documents*

Dumb documents are ordinary electronic documents, such as a simple text file, a rich-text format (RTF) file containing only text and formatting commands, a word-processing file (which contains powerful formatting commands in a proprietary protocol), or an image file (e.g., a fax file, high-resolution image file, or a PDF file). These documents are referred to as dumb because

alone they cannot tell the computer how to interpret them or what to do with them. Perhaps an image file is the “dumbest” kind of document, as essentially it provides only a picture of the text contained in the document (although Adobe PDF files permit text to be recognized through proprietary software). Even though a text document is machine readable, in the sense that the computer can recognize text characters and can search for selected words, the computer that receives the document has no way of knowing what text is significant. For example, the computer could not tell whether a filing was a petition or a motion, nor could it determine the attorney who filed it or the case for which it was filed. In other words, the document contains no instructions to tell the computer how to extract information from the text.

A JEDDI system constructed with only electronic mail and dumb documents would offer few of the potential benefits discussed in this report. In such a system, the user in the law firm would probably send an e-mail message to a designated address at the court and attach the word processing document to it. The message may contain text to explain what the attachment is, to what case it belongs, who is filing the document, and other necessary information. Designated court staff would have to read the e-mail to determine what to do with the document. Assuming the attachment was submitted in a compatible word processing format, the staff would then have to open and read the attachment. Staff would have to send a responding e-mail to the attorney acknowledging the filing or explaining any deficiencies if the filing were not acceptable. Staff would have to enter data from the e-mail manually into the court’s case management system. Finally, the document itself would have to be indexed and stored in the document management system (or printed and filed physically if the court does not have a DMS). These steps are labor-intensive and prone to introduction of many of the same errors as in the paper process.

### ***Electronic Cover Sheet Paired with Dumb Documents***

The next level of sophistication in JEDDI systems is designed to address the limitations of dumb documents. This approach is sometimes characterized as the combination of “pseudo-EDI” with dumb documents. It relies on some form of electronic cover sheet that is prepared by the filer to accompany the document. The cover sheet provides a simplistic form of EDI by following a strict format that permits the receiving computer to locate and extract pertinent information from it. The cover sheet can be implemented in a variety of ways.

#### **Formatted E-mail Text**

At its simplest, a cover sheet may be just a strictly formatted e-mail message that contains data labels on prescribed lines followed by the data fields associated with each label. In a given system, for instance, the design may specify that the first line in the body of the message must contain the text “Case Number:” followed by the text representing the identifier for the case for which the attached document is being filed. In this example, let’s suppose the second line was reserved for the bar number of the attorney of record. The third line might contain a code designating what type of document was being filed (e.g., “305” to indicate a motion for continuance). The court’s computer could parse the e-mail message to locate the data labels and then extract the corresponding data to drive the automated functions needed to populate the database and process the attached document.

## Word Processing Template and Macro

A variation on this approach would be to use a word processing template and macro to build the electronic cover sheet as a word processing document. The macro would simplify development of the cover sheet by supplying the data labels in the appropriate location in the cover sheet document and walking the user through filling in the required information. The cover sheet then would be attached to a simple e-mail message along with the brief itself. The court's computer would parse the cover sheet document rather than the body of the e-mail message to extract the necessary data.

## Web Forms

Most Internet Web-based JEDDI systems rely on Web forms to collect the cover data that must accompany the dumb documents. Web forms are very powerful and easy to use. They may employ a simple fill-in-the-blanks approach or may lead the user through the process with a set of interactive prompts. Either way, the scripting language generally used to develop such forms can perform validation checks and other audits to help ensure a complete and error-free submission of the required information. Part of the process includes the user specifying the path and file name for the document that has been created and stored on the user's system. When the cover sheet, or Web form, is submitted, the accompanying document file is uploaded to the court's (or third-party service's) Web site at the same time. The federal courts use this general model in their pilot electronic filing projects. The dumb document originates in the law firm as an ordinary word processing document that is then saved as an Adobe PDF file on the firm's computer. The attorney or designated law firm staff next fills out the Web form using both free-text entries and selections from drop-down boxes on the Web page. The PDF file is uploaded to the court's Web site when the form is submitted.

## *Intelligent Documents*

"Intelligent documents" is a term coined to describe electronic documents in which the instructions for identifying and interpreting the documents' content are embedded directly in the documents themselves. Obviously, all parties must adhere to a standard technique or coding scheme for this approach to be successful. The software used by the document's author must apply the technique to the document before it is transmitted, either while the document is being created or as a separate step in the process. The recipient's software then uses the same technique in reverse, so to speak, to automate the identification and handling of the document. Such processing includes locating and extracting the pertinent data fields, indexing the document to link it with the appropriate case, and routing it to the appropriate storage location or personnel for review. Numerous techniques can be used to create intelligent documents. Most of these involve one or more of the following: significant positioning, field labeling, or data tagging.

## Positional Field Identification

Perhaps one of the simplest approaches (at least conceptually) is to use positional field identification. Participants in the system agree to a fixed format in which character position in the electronic document is significant. This approach is somewhat analogous to using a set of

preprinted court forms for submission of information to be read by staff. A preprinted form not only helps ensure that no required information is inadvertently omitted, but also enables the reader to locate each piece of information immediately. Although fields on a court form usually are labeled, clerks who handle them know precisely where on the page to look for each item even if the label were obliterated. Imaging systems that include optical character recognition (OCR) often depend upon forms to ensure that information is positioned properly on the page so that the system can locate and scan each field.

A JEDDI system with documents based on positional field identification would include software that built the document file with key data fields in prescribed positions in the document. For example, the case number might always begin in the first-character position on the second line of the document. The filing date might always be placed in the twentieth-character position on the same line and be formatted as MM/DD/YYYY. Even though fields such as the case title could be of variable length, they would have to begin in a certain location—say, the first position on the fourth line. With lengthy free-text fields requiring a variable number of lines, this scheme would have to include additional logic that either recognizes special end-of-field characters or interprets two consecutive blank lines as the end of a multiline field. It is easy to see how an apparently simple positional scheme can become complex for all but the simplest of documents. Moreover, a positional scheme imposes very rigid constraints on the author's ability to organize and present information.

### **Field Labeling**

A more powerful and flexible scheme uses text labels to identify fields of information within the electronic document. For example, the case number might be preceded by the label "Case Number," followed by a colon. The originator's software would insert this label in the document, and the recipient's software would search for it. Once the label was located, the software would assume that the characters immediately following the label represent the case number. Similarly, the filing date for the document might contain the label "Filing Date:" immediately ahead of the date itself. By using data labels, the system is no longer dependent upon exact positioning of information in the document. For example, even if the filing date appeared on the third line rather than the second line in the original document, the receiving computer would recognize it, providing it retained the proper label.

A potential problem with data labels in a lengthy text document arises immediately: how to distinguish labels from information fields. The words "case number," for example, easily could appear several times in the body of a document. The system must be able to recognize the identifying label reliably. One solution would be to adopt a hybrid system using both positioning and labels. Such a system could be designed in a variety of ways. The pilot electronic filing project implemented in Toronto uses a powerful set of specialized word processing templates to create electronic court documents. The templates guide the user in the law firm through entry of the required information for a specific type of filing. The user then appends the details of the brief, and the software generates the complete document. The selected template ensures that the needed data fields appear in the prescribed locations in the document and inserts field labels. When the document is received by the e-filing front end of the court's case management system,

the software is programmed to locate the data fields based upon the document type and the template.

### Data Tagging

The technique for creating smart documents that is becoming most widely adopted for electronic commerce is to use the convention of a special format for standardized data labels called “tags.” For example, the label “case number” could be distinguishable from ordinary content text by surrounding it with specific characters so that it would appear as “<case number>.” In every instance of a document that included case number as a significant data field, this special tag would be used to identify the case number field. Such a formalized tagging scheme eliminates the need for positional identification. No matter how data fields might be scattered throughout a document, the use of tags ensures a system’s ability to recognize and extract data from the document automatically.

## Standardized Markup Languages

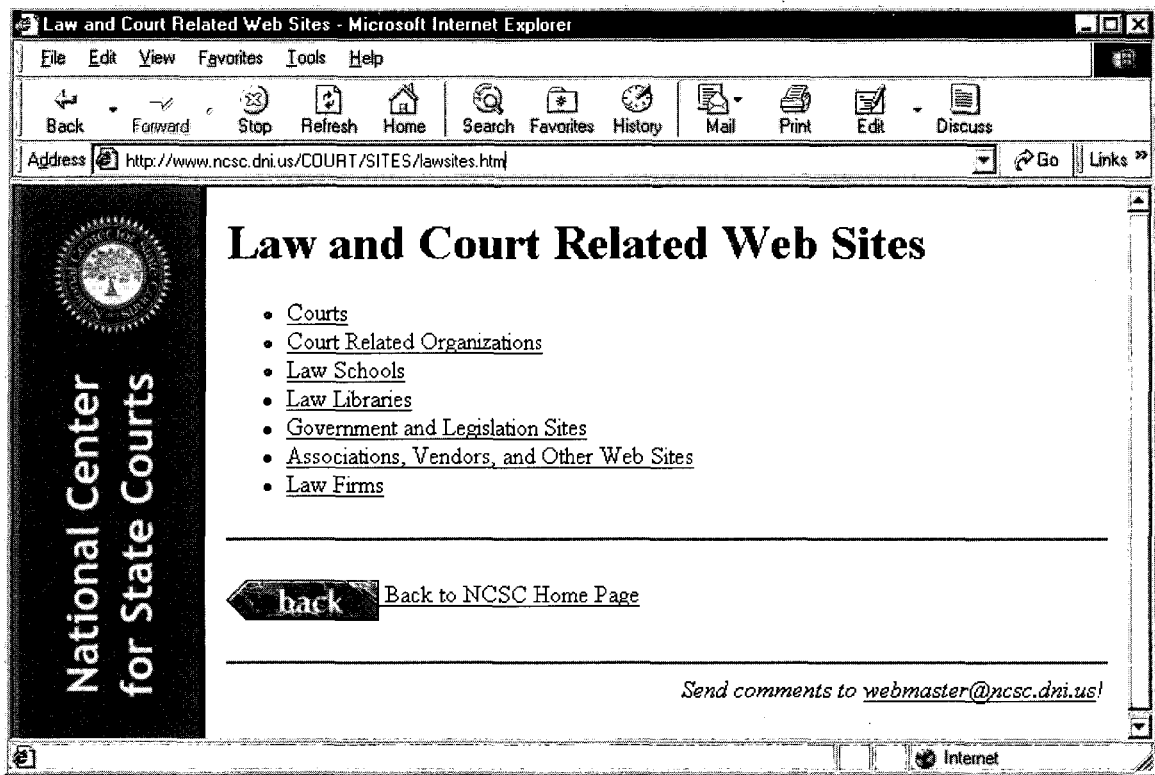
### *SGML*

A standardized language that uses tags to identify and describe the content of an electronic text document is called a markup language. The formal specification of markup languages is accomplished through Standard Generalized Markup Language (SGML). SGML is an ISO (International Standards Organization) specification that determines how a markup language should be defined and what rules documents must follow if they employ a particular markup language. SGML itself is a very broad and powerful language. Unfortunately, because it is so broad in scope, its direct application has been too complex for most purposes, although (like EDI) it has been used by many large corporations in high-volume applications. Several years ago, Utah’s judiciary conducted some preliminary exploration of SGML as a potential vehicle for development of a JEDDI system.

### *HTML*

The most widespread example of a markup language, without a doubt, is Hypertext Markup Language (HTML)—the language of the World Wide Web. HTML is a special markup language defined by SGML for describing the format of Web documents. HTML uses tags to specify how a Web page is to be displayed by the user’s browser software. The tags identify the boundaries of each component of the document (e.g., title, heading, paragraph), and the rules that apply to the HTML specification determine how that component is to be formatted for display (e.g., centered, larger font). The tags themselves are not displayed in the browser window, even though they are contained in the document as ordinary ASCII text. The browser software follows the HTML conventions to recognize the tags as formatting commands instead of content. By selecting “View/Source” on the browser menu bar, the user can view the actual Web document “behind the scenes” complete with tags.

An example of a simple Web page from NCSC's Web site is shown below as it would be displayed through a browser.



Shown next is the HTML source code for this Web page. It is this "electronic document" that is transmitted over the Internet to the viewer's computer. The Web browser software can interpret the standard formatting tags seen below in the brackets (< >) to determine how to display the page.



```

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
<html>

<head>
<meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1">
<meta name="GENERATOR" content="Microsoft FrontPage 2.0">
<title>Law and Court Related Web Sites</title>
</head>

<body background=".../backgrnd.gif">

<table border="0" width="100%">
<tr>
<td valign="top" width="5%"><p></p>
</td>
<td valign="top" width="95%"><h1>Law and Court Related
Web Sites</h1>
<ul>
<li><a href="courts.htm">Courts</a> </li>
<li><a href="orgs.htm">Court Related Organizations</a>
</li>
<li><a href="schools.htm">Law Schools</a> </li>
<li><a href="libs.htm">Law Libraries</a> </li>
<li><a href="govs.htm">Government and Legislation
Sites</a> </li>
<li><a href="assoc.htm">Associations, Vendors, and
Other Web Sites</a> </li>
<li><a href="firms.htm">Law Firms</a> </li>
</ul>
<hr noshade>
<p><a href=".../ncsc.htm"> Back
to NCSC Home Page</a> </p>
<hr noshade>
<div align="right"><address>
Send comments to <a
href="mailto:webmaster@ncsc.dni.us">webmaster@ncsc.dni.us</a>!
</address>
</div></td>
</tr>
</table>
</body>
</html>

```

## XML

As powerful as HTML is in instructing a computer how to display a Web page, it is of no help in defining the meaning of the information contained on the page. A different markup language is needed to describe what a document contains. The language that has evolved in recent years for this purpose is called Extensible Markup Language (XML). Whereas HTML is concerned with the viewing of information, XML provides a standard method for working with data. It is “extensible” in the sense that the tagging scheme is somewhat open-ended and can be

defined to suit a variety of different purposes involving the exchange of information electronically.

XML can be thought of as a much simpler version of SGML. XML permits standardized data exchange using the Hypertext Transport Protocol (HTTP) over the Internet. Just as Web document authors can use HTML to tag a word or phrase to be displayed in bold or italic characters, they can use XML to tag structured data to indicate that a particular phrase represents the description of a retail catalog item, the name of the manufacturer, or the street address of a defendant. Adopting a data-tagging scheme to complement a formatting scheme adds powerful capabilities for processing electronic documents.

### **Benefits of XML**

Tagging the data content of a Web document through the use of XML can enable a search engine to locate that information more accurately. For instance, a search for books written by a particular author, such as Hemingway, could be instructed to retrieve only those Web pages on which Hemingway's name appeared after the "<author>" data tag. The search engine would skip over extraneous occurrences of the same name in other documents, including occurrences in which the name appeared after the "<subject>" tag, as in the case of a biography of Hemingway. Perhaps more important, XML can enable the automatic extraction and processing of relevant data once the data have been located and retrieved. In addition, XML permits the same set of data to be viewed differently by different users. In this context, different users are permitted to view different fields out of the entire document. Because individual fields are recognized, for example, court software displaying an electronic brief could show court staff all data, while blocking out address information in the view accessible by the general public.

#### **Benefits of Tagging Data Through XML**

- Improved searching
- Automatic recognition and extraction of information
- Multiple data views

electronic filing system to extract the party information from the XML document and update the appropriate fields in the case management database.

Business and industry sectors are turning their attention to the issue of XML standards and DTDs. In the short run, individual companies or groups of companies, together with some of the related organizations with which they regularly exchange information, are devising different schemata. Industry analysts predict that much of what develops will evolve into more widespread standards and that other parts of early tagging schemes can be modified to fit the evolving standards. In the meantime, users who can agree on an interim set of standards for a particular purpose can take advantage of what XML has to offer. In addition to these industry-specific developments, organizations such as XML.ORG and an industry consortium called the Organization for the Advancement of Structured Information Standards (OASIS) are hoping to improve coordination of such efforts (and perhaps position themselves to become a value-added service hub) by serving as a repository for XML schemas. Standards of a more general nature are also being advanced through strategic initiatives such as the OBI (Open Buying on the Internet) Consortium, commerceXML (cXML), e-Concert from RosettaNet (a consortium of computer manufacturers and resellers that is developing XML standards and building an XML-based electronic trading network), and Microsoft's BizTalk Framework.

### Growth and Future of XML

As courts consider the potential benefits of this still quite new technology, how can court technology planners be sure that XML will mature to become the predominant methodology for exchanging information? The answer lies in the almost universal recognition of XML as a logical and viable technology solution. Industry analysts point out that XML shares the characteristics of other Internet-based technology solutions that have become universally adopted. These technologies bridge the gap between disparate systems, leaving developers and user organizations free from the concern over what technology platforms and software products are in use by the different entities needing to exchange information. Examples of these successful technology solutions include TCP/IP for networks, the Java programming language, and Web browsers for presenting the contents of electronic documents. XML fills the need for a platform-independent method to transfer the data in electronic documents.

The proof of this recognition is the widespread incorporation of XML across the entire technology industry and its pursuit by major technology users as a practical solution. Consider, for example, just a fraction of the developments occurring as this report was being finished.

- Microsoft's latest browser, Internet Explorer 5.0, was released with full support for the World Wide Web Consortium (W3C) XML standard. Moreover, it includes an XML parser that can work in other applications besides the browser. (Internet Explorer 4.0 included more limited support for XML.)
- Lotus is including support for XML in Release 5 of its Domino Application Server, providing an XML-based application development environment for users and allowing information to be viewed as an XML document. Lotus considers XML to be "the common language of business-to-business e-commerce."

## Example of XML Structure

Shown below is a simple illustration of how the significant data in an electronic document can be tagged for automatic recognition by a software application. As the example shows, XML not only can designate data fields, but also can indicate something about the way the data are structured through the use of nested tags to indicate a hierarchy. Moreover, the tagged document remains readable by users even in its “raw” form.

```
<books>
  <book isbn="0684803356">
    <title>For Whom the Bell Tolls</title>
    <author>Ernest Hemingway</author>
  </book>
</books>
```

In order for XML documents to be exchanged between different entities, the standards governing the syntax and structure of the document must be rigidly followed. Standards include basic rules for constructing XML documents, such as the following:

- ✓ The document must have a “root node” (a unique first element).
- ✓ All data elements must have an end tag (indicated by “/” before the tag name).
- ✓ Nested elements must not overlap.
- ✓ Attribute values (e.g., the ISBN number in the example) must be enclosed within quotation marks.

## XML Standards

XML is extremely powerful because it allows developers to define an unlimited set of data tags to suit their particular needs. The downside is that there is no standard set of tags predefined for any industry, business, or government applications. It is up to each set of players to develop a standard approach.

Document Type Definitions (DTDs) are used to specify formally the characteristics of a particular type of XML document. A DTD defines the valid set of tag names and attribute names. It states which data fields are mandatory and which are optional. It also may indicate which fields can occur multiple times in the document and provide a range of other specifications. In effect, the DTD sets the standards for a particular type of XML document. If two or more organizations that need to exchange data adopt the same DTD, they can use the corresponding XML document to transmit the data between their disparate computer systems. The identification of the DTD being used for the document is specified at the beginning of the document so that the receiving system will be able to recognize the type of document and correctly interpret the data tags it contains. The business application software systems in both organizations can interact automatically with the electronic documents through another standard called Document Object Model (DOM). For example, the legal software in a law firm could be programmed to extract party information from its client database and insert it into the XML document. The court’s case management software subsequently would interface with the

- The number of commercial projects making practical use of XML is mushrooming. For example, IDG Books Worldwide is converting its top books in the “For Dummies” series to XML through a contract with Advanced Data Engineering. Advanced Data Engineering also is under contract with Web MD (an extensive Internet-based healthcare network that connects physicians, hospitals, and consumers to Web-based health-related information and resources) to convert Reader’s Digest books on nutrition and healthy cooking to XML.
- Arlington County, Va., is planning to use Sequoia Software Corporation’s XML Portal Server to provide both local agencies and the general public with quick and easy access to land record documents through the Internet. XML enables the server to work more effectively with data from disparate sources. It will provide powerful search capabilities for locating specific information from among millions of deeds, wills, judgments, and financial documents stored in different county repositories.
- The Mortgage Bankers Association of America (MBA), with a membership of over 3,100 organizations and companies in the mortgage lending field, has been working on XML standards for the mortgage industry since early 1998. In May 1999 it established a formal XML Workgroup, of which Fannie Mae is a member. MBA’s XML Workgroup developed a pilot XML standard, which was submitted to the Eighty-sixth Annual Convention in October 1999 for review.
- The AICPA (American Institute of Certified Public Accountants) is developing XML standards for financial statements. The resulting XFRML (XML-based Financial Reporting Markup Language) will provide the financial community with a standards-based method to prepare and publish financial reports in a variety of formats and to exchange and analyze the information they contain. The XFRML working group comprises several key organizations, including Arthur Andersen LLP; Deloitte & Touche LLP; Ernst & Young LLP; KPMG LLP; PricewaterhouseCoopers LLP; FRx Software Corporation; Great Plains; e-content (a division of Interleaf, Inc.); FreeEDGAR.com, Inc.; EDGAR Online, Inc.; The Woodburn Group; and Microsoft Corporation.

Even if XML eventually is supplanted by another electronic document exchange methodology, it is highly likely to be an evolutionary or transformational process rather than a total scrapping of XML. Consequently, information systems built with XML can evolve with the standard. Moreover, XML documents will be able to be rolled forward into the latest viewers, just as today’s Web browsers can view Web documents constructed with the first generation of HTML. XML as a standard is still in its infancy—yet XML is being pursued and adopted by nearly every major organization that wishes to engage in e-commerce, as well as by major technology providers. Momentum of this magnitude invariably establishes a technology solution as an accepted approach or practice, regardless of whether all details and refinements concerning its application have been worked out and despite the existence of possible alternative approaches.

### **XML Standards for JEDDI Projects**

It is important for the justice system to begin addressing XML standards to realize the tremendous potential benefits that this technology offers. Pioneering work in the practical

implementation of XML for JEDDI projects is being accomplished in Utah and New Mexico, and other courts and commercial court technology providers are exploring the technology. In Utah the AOC has developed preliminary DTDs for court documents and is using them in a criminal JEDDI system operating in the Third District Court. These standards can be spread throughout the state as the JEDDI system expands, potentially enabling the entire state court system to use a standard set of XML documents in the near future. Yet the Utah AOC recognizes the desirability of national standards and would prefer to adapt its systems to those standards, once they are developed. To date, such efforts in all courts have been following an individual approach to setting up DTDs and developing other conventions for the use of XML. Fortunately, however, a concerted effort to address these issues is now in its formative stage.

The National Center for State Courts is working with the Joint Technology Committee (JTC) of the Conference of State Court Administrators (COSCA) and the National Association for Court Management (NACM) to develop national court technology standards. The National Consortium for Court Automation Standards, operating with oversight by the JTC and staffing by NCSC, currently is focusing on functional standards for case management systems. However, it is undertaking a court XML standards initiative, as well, working in cooperation with Legal XML, a nonprofit organization consisting of volunteers from private industry, nonprofit organizations, government, and academia, which is sponsored by Georgia State University (see [www.legalxml.org](http://www.legalxml.org)). In addition NCSC has conducted a project to compile data exchange requirements and definitions as a preliminary step toward identifying XML DTD requirements for courts. Courts planning JEDDI implementations should monitor these activities closely and participate in the standards development efforts whenever possible.

## CHAPTER SIX

# *Security and Authentication Technologies*

### Introduction

In almost any discussion of electronic documents and JEDDI systems, the topics of security and authentication issues and methods are sure to arise. Understandably, court leaders and attorneys are quite concerned about maintaining the integrity of electronic documents in the absence of traditional paper originals, handwritten signatures, and embossed seals. Fortunately, many of these same issues also affect the commercial world, which has been well out in front of the courts in the pursuit of electronic commerce and information interchange. Banking, insurance, and other industries have invested countless hours and millions of dollars addressing security needs.

### *The Challenge of Internet Document Interchange*

Initially, most commercial transactions were accomplished via secure, private networks and direct high-speed telecommunications between organizations. However, the phenomenal global expansion of the Internet has changed the playing field dramatically, establishing the Internet as the information highway of choice. Organizations all the way from mom and pop enterprises to Fortune 100 corporations are turning to the Internet for transmission of critical business documents and for transactions collectively worth billions of dollars. *But the Internet is a public, unregulated, and inherently unsecured network.* Ensuring the security of corporate-to-corporate exchanges is enough of a challenge, but it pales by comparison with the challenge of conducting electronic transactions with millions of individual consumers.

Courts already are finding the Internet invaluable for exchanging information by e-mail, conducting legal research, locating a variety of other information helpful to their staffs or operations, and making information available to the public. The Internet also is the most practical and useful communications infrastructure for JEDDI systems. Consequently, it is logical for courts to follow current developments in e-commerce security closely and to position themselves to benefit from the techniques and standards that are emerging in the commercial sector.

### *General Security Requirements for JEDDI Systems*

Information system security is a massive field with vast resources of knowledge, technology tools, and practices. It is not the purpose of this chapter to address general system and data security issues for courts, even though many of these common issues apply equally

strongly to implementations of JEDDI technology. In fact, it is essential that all aspects of sound system and data security principles be applied faithfully to JEDDI systems. For example, disaster recovery plans, good backup procedures including off-site storage, comprehensive system logging and audit functions, redundant or fault-tolerant servers, robust Internet firewalls, stringent anti-virus measures, and other standard techniques are critical to establish a firm technology foundation for JEDDI. If a computer system goes down for an hour or two today because of a component failure or breach of access security, most courts can continue to operate to a certain extent, because they have the paper case records available for court proceedings. With totally electronic records, a court is much more likely to grind to a halt if a computer failure or damage from a system intrusion cannot be remedied almost immediately.

General security issues are well covered in other publications and general industry resources. This chapter will focus on the specific security issues pertaining to the electronic exchange of documents between persons and organizations. Most of these issues revolve around the need to establish the *authenticity* of users (senders and recipients) and documents through some effective method of *authentication*.

### ***Security Issues for Electronic Document Transmission***

Being able to rely on the integrity and authenticity of court documents is fundamental to the judicial process. To be legally acceptable, documents must satisfy several conditions, regardless of whether they are in paper or in electronic form:

- **Authenticity:** there must be some method for the recipient to identify the actual sender as the same one indicated by the document as the individual authorized to send the document on behalf of an organization.
- **Integrity:** there must be some method for the recipient to determine that the document is intact and has not been altered since it was sent.
- **Nonrepudiation:** there must be some method to ensure that the sender cannot falsely claim that he or she did not send the document at all or that the contents are different from what was sent.

In the world of paper, these conditions have been satisfied through a variety of accepted techniques or practices. Preprinted letterhead, watermarks, embossed seals, handwritten signatures in permanent ink, and sealed envelopes are all intended to help ensure the integrity and authenticity of a message or document. Even though letterhead can be imitated, signatures can be forged, and envelopes can be resealed, these conventions are sufficient to generate the level of trust needed for paper transactions. Certain assumptions are made regarding the authenticity and integrity of documents meeting the accepted standards, with the force of law and its associated penalties for fraudulent activities undergirding the entire process.

In the world of electronic documents, a similar kind of system is needed to establish the level of trust required to conduct transactions or exchange information between parties at opposite ends of the wire. The first challenge—and the one that has received the most attention in the security field—is to establish the authenticity of the sender of data or documents. It is of



paramount importance for a JEDDI system to provide a means to ensure that only authorized, identifiable users can create and transmit electronic documents.

## Technological Approaches to Security and Authentication

Courts may use a wide range of methods and technologies either individually or in combination to achieve different levels of security or to fit different purposes. These techniques can be grouped into three fundamental categories sometimes identified informally as

- “something you know”
- “something you are”
- “something you have.”

The table shown below summarizes the characteristics of each approach, and the sections that follow discuss the technologies in detail.

<b>Technological Approaches to Security and Authentication</b>			
<b>Approach</b>	<b>Technologies</b>	<b>Advantages</b>	<b>Disadvantages and Limitations</b>
<b><i>Something you know</i></b>	User ID and password	--Simple to implement --Widely supported --Familiar and easy to use	--Limited security --Effective use requires strict policies and frequent password replacement
<b><i>Something you are</i></b>	Biometrics (retinal scan, fingerprint, voiceprint, etc.)	--High security --Limited liability for loss or theft	--Expensive --Less portable (requires specialized readers) --Privacy concerns
<b><i>Something you have</i></b>	Hardware token	--High degree of security --Supported by numerous applications	--Expensive --Cumbersome to use --Subject to loss or theft
	Smart card	--Simple to use	--Immature --Relatively expensive --Limited support --Subject to loss or theft
	Digital certificate	--Good security --Good for partner transactions	--No universal methods and authorities yet --Limited application support

### ***Something You Know***

The “something you know” approach is the one most familiar to most people. It requires the user to know a “secret” piece of information that must be supplied to gain access to certain information or to a computer system. Unique user IDs and passwords constitute the most common manifestation of this approach. Another example is the personal identification number, or PIN, required to access an individual’s bank account through an ATM or online banking system. Although passwords and similar techniques offer one of the lowest levels of security, they are extremely widespread. They are very simple to implement and convenient to use (at least until one reaches the point where numerous sets of IDs, PINs, and passwords have to be

memorized to access a host of different systems or applications). This technique is adequate for many purposes and can be combined with other methods for greatly increased security levels.

Certain policies and principles should be followed if a court or other organization really wants to minimize the security risk associated with relying primarily on password technology. Security experts suggest that guidelines should include these points:

- Passwords for Windows NT or 2000 systems should be either seven or fourteen characters long.
- Passwords for Unix systems should be at least eight characters long.
- Passwords should include at least two alphanumeric and two special characters (such as !, @, #, \$, %, &, or \*).
- Passwords should have no relationship to user name or login ID (e.g., password should not be a variation on user name).
- Passwords should not be obvious words or characters (e.g., “password,” “secret,” “123456789,” or “\*\*\*\*\*”).
- Passwords should be changed at least every ninety days.
- New password should differ from old password by more than one character.
- Passwords should not be easy to guess from knowledge about user such as
  - nickname
  - birth date
  - Social Security number
  - telephone numbers
  - position, job title, or relevant term (e.g., “techie” or “gavel”)
  - name of spouse or child

Many of these policies are difficult, if not impossible, to enforce in most systems. Obviously, the extent to which such guidelines should be adopted depends upon several factors, including

- the nature of the application (e.g., logging into system administrator functions versus logging into an inquiry-only program)
- the degree of perceived risk (e.g., remote dial-up access points versus logging into a desktop system in a locked office)
- the value of the information being protected (e.g., sensitive case documents versus the court calendar)
- the appropriate balance between limiting risk to the organization and imposing an excessive burden on staff that discourages compliance

Courts should seek to develop a reasonable set of policies and procedures covering the various password-protected systems in use. Once these policies and procedures are available, court managers should publicize their existence, educate users about how important they are, and encourage compliance.

In addition to their general use in computer applications, user IDs and passwords are the most prevalent forms of security employed in the limited number of JEDDI systems in existence

today. In the federal systems and some local court projects, login IDs and passwords are employed in conjunction with Netscape's Secure Sockets Layer (SSL) technology to control access to the court's JEDDI Web site and to authenticate users. Although SSL provides a secure connection by encrypting the transmissions sent over the open Internet, the identity of the attorney connected to the Web site is authenticated by only the user ID and password. In the current climate of predominantly pilot projects, with a modest universe of attorneys and limited numbers of transactions, this degree of security probably is quite adequate. As courts expand their JEDDI systems, however, they should consider moving up to more-robust security measures. Certainly, their long-range plans should include adopting appropriate technology that incorporates systems and standards developed to support electronic commerce over the Internet.

### ***Something You Are***

"Something you are" refers mainly to the approach of using biometrics technology to enhance security. The "something" in this case is usually a part of the human body or is related to the body in a unique way. The most common example of this approach is the use of fingerprints to establish the identity of a user. A fingerprint reader at the access point can be linked to a database of authorized users and used to access control software. When there is a match between the fingerprint image taken from the individual requesting access and a fingerprint record for an authorized user stored in the security database, the retrieved identity is passed on to the access control software, which logs the user in for the session. Other examples of biometrics security technology include palm-print systems, retinal scanning systems, and voice recognition systems.

If they are well designed, these systems can offer a high degree of security because of the unique, built-in characteristics of each user. One major drawback is the expense of readers and other technology components. A related disadvantage prevents this approach from being practical for most JEDDI applications. The technology is much less portable than other methods, so the user most often has to be at the site where the reader or scanner is located to access the system. Another disadvantage is that this approach can be somewhat intrusive and may infringe upon the user's privacy.

Voice recognition systems (not to be confused with speech recognition systems) are somewhat less intrusive and can be more portable, as well. For example, voice recognition systems can operate with ordinary telephone voice input for some purposes. Unfortunately, they are difficult to make highly discretionary (selective) when distinguishing speakers and, at the same time, tolerant of background noises or slight variations in the speaker's voice caused by hoarseness or emotional state. Voice recognition systems also may be more susceptible to human or technological impersonation. Finally, although they are still in the early stages of refinement, face recognition systems are becoming more practical, as well. Continuous improvements in computational power, price-performance ratios, and peripheral technology advances are making all types of systems based on biometrics much more powerful, reliable, and cost-effective to implement for general security purposes. It remains to be seen whether some devices can be made sufficiently inexpensive and portable to be practical in a JEDDI environment with many remote users.

## *Something You Have*

The “something you have” approach generally provides a much higher degree of security than the simple ID and password combination. It requires the user to possess a unique security device (which may be physical or mathematical in nature) issued by an authorized entity to gain access to a particular system. Technologies in this category include devices such as tokens and smart cards as well as digital certificates.

Tokens are microprocessor-based, handheld devices that either generate or retrieve from on-board storage the complex passwords required to enter a secured computer system or Web site. Some generate one-time passwords on the fly, while others retrieve a password from a set stored in the device itself, perhaps on the basis of the current date or time. The password produced will be synchronized with the host system and may be designed to let the bearer who was issued that particular token access a prescribed set of systems, databases, or records within a database. The passwords can be far more complex than would be practical for a user to memorize; moreover, they may change on a daily, hourly, or per-use basis.

The devices are available in a number of physical configurations and degrees of sophistication. Some are card-based and require a card reader to use. Others may be pocket keyholders or keyfobs and require a special reader attached to the PC. Still other token-based products operate by having users plug the device (sometimes called a *dongle*) into their computer’s printer port, serial port, or USB port. Upon a request for access, the server (host) system queries the client (user) system to see if the token is present. If it is there, the token transmits the proper password or authorization code to the host system, which then lets the user into the Web site or system. In most systems the token itself is protected by a permanent Personal Identification Number (PIN), which the user must first enter into the computer before the token will issue the password. The PIN adds a further layer of security, especially in the case of theft or loss of the token.

An alternative type of hardware token does not attach to the user’s computer at all. Instead, it contains a small display window and keypad, much like a credit card calculator. When a password is needed, the user keys the PIN directly into the device. If the PIN is correct, the token then displays the appropriate password for the user to key into the computer. Some products add a deeper layer of security by using the Challenge/Response mechanism described in the Secure Sign-on Standard (ANSI X9.26). When the user requests access through his or her PC, the host computer issues a digital challenge (e.g., a seven-digit number). The user activates the token by entering the PIN and then keys into the token the challenge number. The token responds by displaying the corresponding password or code, which the user can enter into the computer for transmission to the host computer or network. As the final level of security, the token actually calculates the response from the challenge, using a cryptographic key stored inside the token. The matching key for that user is stored on the host system.

Smart cards are a refined form of hardware token. They contain an on-board microprocessor and memory and perform the functions described above, even though they may

be as small and nearly as thin as a credit card. Generally speaking, smart cards do not contain a display or keypad; instead, they interact directly with a computer through a smart card reader. The reader may be attached to a computer port or may be designed to fit the PCMCIA card slot on a laptop. Smart cards being produced today are capable of incorporating biometric security and may house the user's digital certificate as well. Digital certificates will be discussed below in the context of digital signatures and public key infrastructure (PKI) technology.

## **The Judicial System's Place on the Security Scale**

The most secure systems, of course, are protected by a combination of these three approaches, sometimes with multiple sets of techniques within a particular category. The Department of Defense, certain federal security agencies, and a few corporations in highly competitive industries subject to aggressive corporate espionage have implemented elaborate security systems that are extremely difficult to penetrate. One rule of thumb sometimes applied to far less robust security systems than these is to design them to withstand a team of hackers applying 1,000 computers to the problem for at least two weeks. While such a level of security may be justified in protecting national security information, defense secrets, or multibillion dollar industrial secrets, it is hardly necessary for the protection of court documents and records.

### ***Security in Traditional Paper Systems***

Court records have never been afforded a particularly high level of direct security. The paper records with which courts have operated for hundreds of years are inherently insecure. They are subject to damage or destruction through fire, flood, and other accidental events, as well as through deliberate acts of vandalism or theft. They are subject to loss through a variety of incidents, including being picked up inadvertently along with other material in the attorney workroom, falling off a clerk's desk into the wastebasket, or being blown out the window on a blustery spring day. More insidiously, paper records are subject to falsification, and handwritten signatures can be forged. Yet loss, damage, and falsification of court records rarely have presented more than a minor annoyance. The primary reason is that the justice system is adversarial in nature and contains built-in checks and balances. Opposing parties tend to scrutinize records closely. Moreover, there are multiple copies of court records in most cases: the court has at least one set, opposing attorneys each have a set, and sometimes the parties themselves have a set. Consequently, it is relatively easy to reconstruct a lost file or to compare records to determine authenticity.

### ***Why Electronic Records Should Have Higher Security Requirements than Paper***

Regardless of the fragility of paper-based systems, however, electronic document systems should indeed be required to provide higher levels of security than is possible with paper. There are several reasons why this is true. In the first place, it is so easy to provide at least minimally

improved security through technology that it would be ludicrous not to do so. In the second place, without giving too much credence to the paranoia that sometimes follows a news report of an isolated hacker attack, there actually is a somewhat higher level of risk associated with electronic records. This is especially true if those record systems are accessible from outside the courthouse through dial-up or Internet telecommunications. Many more people have practical access to electronic records and, consequently, have the opportunity to attempt illegal or unauthorized actions. Potential attackers also can operate more surreptitiously through electronic access, and they can apply sophisticated software tools to the task. Finally, the small percentage of the population who engage in hacking activities usually do so for the challenge and thrill of this technological “game,” regardless of whether they have any direct interest in a particular record. For this group, a JEDDI system presents a potential target that a paper system does not. While there has been little evidence to suggest that existing automated court systems make appealing targets for hacking, this mild risk is further justification to make certain that adequate security measures are implemented.

Another reason to err on the side of caution is that electronic records discourage the practice of maintaining multiple copies (an acknowledged necessity with paper in order for all parties to have ready access to the information). A fundamental principle of information systems is to avoid redundancy of data entry and storage. Because an electronic record is accessible to multiple users at any time, there is no need to store a second copy (excluding backup and archived copies, of course). It is more effective and practical for all case participants to work from the same set of files. In reality, of course, this is not always the situation, especially during the early stages of case development. Attorneys do generally keep their own set of files containing not only the documents they originated but also those received from the opposing party and the court. Increasingly, though, these files are likely to be regarded as temporary working files.

The final reason may be the key issue, at least at this point in the JEDDI movement. It is essential to establish a sufficient level of confidence and trust in the entire system. For JEDDI to succeed, everyone in the system—attorneys and prosecutors, judges, clerks, and litigants—must feel comfortable with the security of all processes and transactions and the integrity of all documents and records. Particularly during the early stages of transition from a paper environment, a breach of security can seriously undermine confidence in the technology and support for the effort, making it more difficult to abandon reliance on the paper record. Ideally, therefore, the security should be sufficient not only to allay fears concerning potential dangers, but to discourage any actual attempts at fraud or corruption of documents and records as well.

### The Most Promising Technological Method to Ensure Authenticity and Integrity

A primary rule of business is to know with whom you are conducting business. The Internet makes it inherently difficult to know who really is on the other end of the wire. Yet widespread adoption of electronic documents requires the establishment of an adequate level of trust between parties who are not face-to-face and who may be personally unknown to each other. More specifically, courts need to know that they are accepting a valid document from a

valid attorney; conversely, attorneys need to know that they are submitting their document directly to the intended, authorized court recipient or other counsel, as well as feel confident that documents they receive are being sent by the court or other legitimate party. With all their faults and limitations, handwritten signatures, together with supporting techniques such as letterhead and sealed envelopes, have been sufficient to bridge the trust gap in paper systems. What is most likely to establish the threshold level of trust in the electronic world?

### ***Electronic Signatures***

Some form of electronic signature would seem to be a natural component of a solution to establish the required level of trust for a JEDDI system. One school of thought was to digitize the handwritten signature of a document's author. Perhaps the most simplistic example of this approach is a faxed document. The document may have been printed, signed by hand, and then sent via a fax machine to the court. Alternatively, the sender may have composed the document on a word processor, using a letterhead template, and then appended an image file of a previously scanned signature before faxing the finished document directly from the computer. If a court has moved beyond fax filing and accepts word processing document files directly as an e-mail attachment or by way of uploading to a Web site, then the image of the signature can be embedded in the document. The same can hold true of a PDF file created from a word processing document containing a graphic of a handwritten signature.

In all these cases, the image approach does not do very much to ensure authenticity. A signature image can be copied from a previous document and applied to a bogus one with very little effort. It really is no more of an assurance of the authorized sender than is the name in the letterhead. The attempt to retain the comfort level provided by a handwritten signature has led to some very creative technology. It has become commonplace, for example, to see delivery services, such as Federal Express and United Parcel Service, have the recipient of a delivery sign an electronic receipt by way of a digitized writing pad. This practice is quite adequate for acknowledging receipt of a package, because it almost exactly replicates the paper process. The receipt is still signed in the presence of the delivery person. The electronic version is simply more convenient and efficient to process. Some proponents of electronic signatures have suggested that this type of electronic pad input be used in JEDDI systems.

An even more elaborate approach was developed by a technology company several years ago. The company built a device consisting of a digitized signing pad on one end of the line and an electromechanical writing mechanism on the other. The idea was to get an "original" signature affixed to the recipient's copy of the document. The printed document was inserted into the writer under the computer-controlled pen. Then, as the author signed the electronic pad at the far end of the wire, the digitized pen strokes were captured and transmitted to the writer unit, where they were faithfully recreated in ink through the plotter-like action of the writing arm. While the ingenuity of this device has to be admired, the approach really is not very practical for a JEDDI system, nor does it ensure authenticity to any great degree.



## *Digital Signatures*

In addition to failing to provide adequate assurance of authenticity, electronic signatures based on images of handwriting do almost nothing to guarantee the integrity of an electronic document or to establish nonrepudiation. The type of electronic signature that provides the needed level of security and practicality is called a *digital signature*. Digital signatures are quite different from “digitized signatures” and have no relationship whatsoever with handwritten signatures. Instead they are based on a mathematical encoding methodology known as *cryptography*. Digital signatures can provide a very high level of security. They make it possible to determine not only who sent a document, but also whether the document has been tampered with after it was signed.

## *Cryptography*

Cryptography has been around for a very long time in one form or another. The principle involves using a reproducible scheme or methodology to transform the elements of an original message into an encoded or *encrypted* version that disguises the appearance or meaning. The encrypted message can be interpreted only if the transformational method (or *key*) is known. Reversing the transformation to recreate the original message is known as *decrypting*.

Suppose, for a very simplistic example, that two friends wanted to exchange e-mail messages that could not be read at a glance by anyone looking over the recipient’s shoulder. They might agree on a simple method of disguising the text by systematically transforming the alphabet so that each letter was offset from its original position in the alphabet by three places. The scheme might include wrapping the last three characters back to the beginning of the alphabet. Julius Caesar reportedly used this type of scheme to send messages securely to his trusted acquaintances when he did not trust the messenger. The algorithm could be represented by the following steps:

1. Add three to the number representing the position of the letter in the alphabet.
2. If the result exceeds 26, subtract 26 from it.
3. Replace the original letter with the letter occupying the alphabetic position indicated by the calculated number.

The table that follows shows the result of the substitution scheme.

Using this simple scheme, the original text of the message would be replaced with the encoded text before the message was sent. The new message would appear to be gobbledygook to the casual viewer. For example, the timeworn phrase, "Have a nice day," would become "Kdyh d qlfh gdb" (which one is sometimes tempted to vocalize after encountering the umpteenth robotic well-wisher during the course of a day!).

Cryptography involving computerized information and electronic communication is, of course, much more complex and powerful than the alphabet example above. Because the entire message or document is in electronic form, sophisticated mathematical algorithms can be used to encrypt the entire message—not simply transform each letter individually. The resulting encrypted document is both more totally obscure and far more difficult to decrypt. Yet the same principles apply as in the simple example. Both the sender and the recipient (but no one else) can interpret the message and recreate the original text, because they share the same critical knowledge of the encoding or encrypting scheme. In essence, they each have the identical key.

Original Letter	Alphabetic Position	Calculated Position	New Letter
A	1	4	D
B	2	5	E
C	3	6	F
D	4	7	G
E	5	8	H
F	6	9	I
G	7	10	J
H	8	11	K
I	9	12	L
J	10	13	M
K	11	14	N
L	12	15	O
M	13	16	P
N	14	17	Q
O	15	18	R
P	16	19	S
Q	17	20	T
R	18	21	U
S	19	22	V
T	20	23	W
U	21	24	X
V	22	25	Y
W	23	26	Z
X	24	1	A
Y	25	2	B
Z	26	3	C

### Private Key Cryptography

Cryptography involving identical keys on each end is called *symmetrical cryptography*. It is also referred to as *private key cryptography* because there is only a single key, which must be held in secret between the two parties. Although symmetrical cryptography works quite well for many purposes in a contained universe of message exchanges, it is not effective for more widespread exchanges. Because each pair of senders and receivers needs a unique key, the technique would quickly become unmanageable as the number of potential senders and receivers that might be paired up for a given transaction increases. First of all, it would be necessary for an individual to generate, catalog, and store a unique key each time a document needed to be exchanged with a new party. But the real challenge is the fact that the secret key also would have to be transmitted to the other party securely, creating a kind of security "Catch-22."

### Public Key Cryptography

The solution that was developed in the mid-1970s to answer the need for widespread secure electronic interchanges is called *public key cryptography* or *asymmetrical cryptography*.

It involves a pair of keys rather than a single, shared key. One key is a private key and the other is a public key. The private key absolutely must be kept secret by the individual user to which it is assigned. Sharing it with anyone would forfeit that user's guaranteed authenticity. However, the public key may be freely disseminated to anyone with whom that individual wishes to exchange information. In fact, the public key can be publicly posted so that anyone can obtain it as needed.

The private key and public key are mathematically related to each other; yet it is not possible to calculate the private key from the public key (the process is deemed "computationally infeasible"). Distribution of the public key in no way endangers the security of the private key. Moreover, a message encrypted by the public key can be decrypted only by the corresponding private key. The public key cannot be used to decrypt the message that was encrypted by that same key.

### *Encryption for Privacy*

Public key cryptography can be used to ensure both privacy and integrity of an electronic message or document and the authenticity of the sender. To protect the message itself, the sender first obtains the recipient's public key. The sender then uses that public key to encrypt the message (which is sometimes referred to as *clear text* in its original, unencrypted form) before transmitting it. The recipient in turn uses his or her private key to decrypt the message or document, restoring it to its original form. No one other than the designated recipient can read the encrypted message, including the sender.

Although public key cryptography can be used to encrypt entire messages, it usually is not in practice. Because public key encryption algorithms operate on very large numbers (e.g., more than 1,000 bits or 400 decimal digits), they are relatively difficult to compute, consuming a lot of time because they require substantial computer processor resources. For that reason they most often are used to encrypt a one-time symmetric message key, which in turn is actually used to encrypt the message itself. The encrypted message key is then transmitted with the encrypted message. The recipient uses the public key to decrypt the message key, which is then used in a much faster computation to decrypt the message.

### *Encryption for Authentication*

While there will be electronic court documents that must be kept private, at least during certain stages in some cases (especially criminal and juvenile cases), most court documents are a matter of public record. The most crucial aspect of security for transmission of the majority of court documents is authentication of the sender and the message. Authentication of the sender, as well as that of the message itself, is established through the use of a digital signature. When the sender wishes to sign a message digitally, the sender's computer performs a mathematical operation involving both the sender's private key and the message itself. First the original message is put through a hashing algorithm that generates a fixed-length code usually called a *message digest*, which is much smaller than the message but has a unique mathematical relationship to it. Then the message digest and the sender's private key are used together in an

encryption computation. The result of this second computation is a digital signature, which is attached to the message and sent along with it.

### ***Digital Signature Use***

The digital signature is unique to both the private key and the message. If the same sender uses the same private key to sign a second message, the new digital signature will be different from the one accompanying the first message. A primary advantage of computing the digital signature from the hashed message digest is that the considerably smaller digest permits the complex computation to be performed much faster, while preserving the unique relationship of the resulting signature to the original message. When viewed, a digital signature looks like a garbled string of characters similar to the following example:

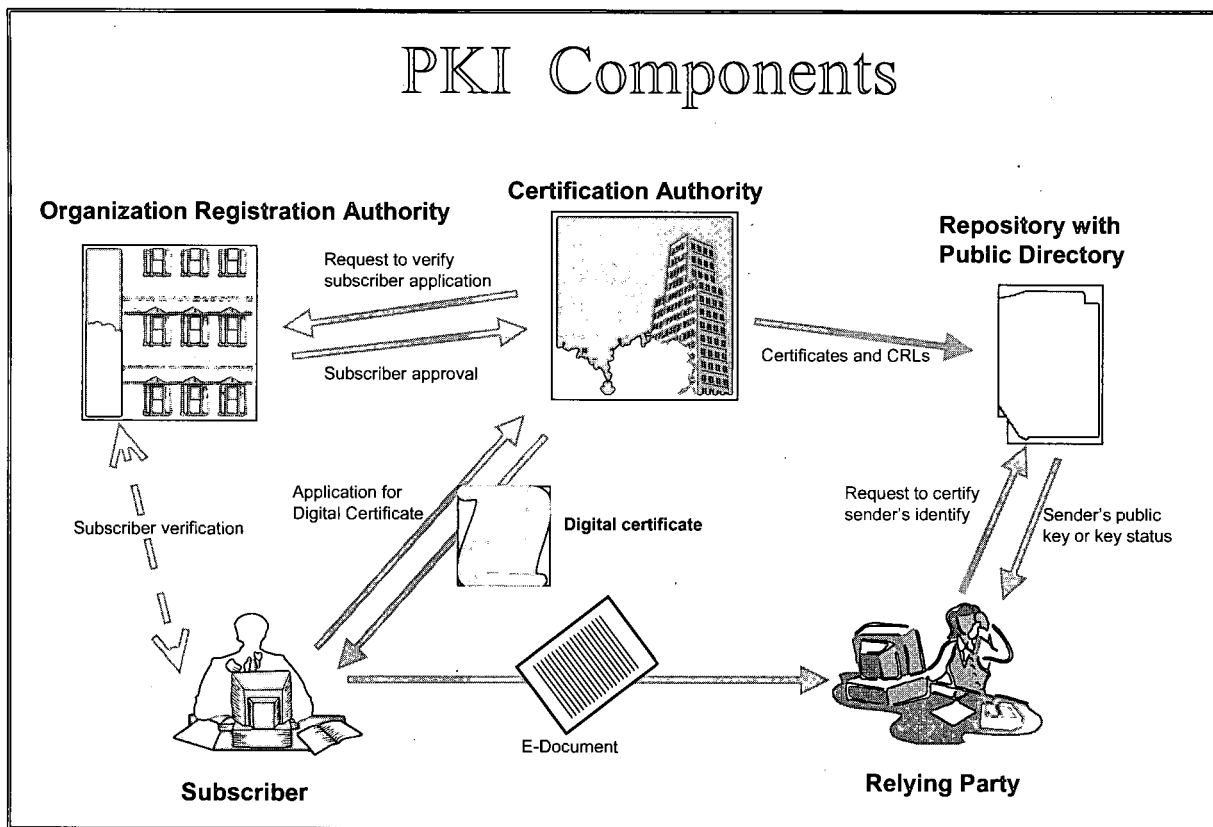
```
idkflkmejsdaoiB441klklk08+kadlkdflioe993+1alkfdlasd4ksrlk41ksafj81kadflk61ardlfj+kd  
akljfl61adfldfjl+adfsdfddf+
```

To verify the signature, the recipient performs a computation involving the message, the digital signature that was attached to it, and the sender's public key (retrieved from a public directory). In essence, the recipient passes the (clear text) message through the hashing algorithm to produce a message digest. Next, the digital signature and the public key are processed by a computation using the public key algorithm. The result of this computation then is compared with the message digest produced in the first step. If the result is correct according to the prescribed mathematical relationship, the signature is verified as genuine, and both the sender and the message are authenticated. If the computed result does not meet this test, then either the signature is fraudulent or the message may have been altered after signing.

Digital signatures, then, elegantly solve the problem of transmitting documents securely regardless of the security of the network through which they are transmitted. Because the Internet is the best and most logical telecommunications infrastructure to use for widespread electronic document interchange, this solution is crucial to establish the level of trust required to use the Internet effectively. Clearly, digital signatures are of paramount importance in the long-range security strategy for a JEDDI system.

## **Public Key Infrastructure (PKI)**

Despite the powerful capabilities that digital signatures and public key cryptography can provide, a few more pieces are needed to tap into their full potential for establishing trust in electronic interchange. Then all the pieces of technology, policies, and procedures need to be put together into a system. The organization of public key cryptography components in a structured system to support electronic document interchange is called a *public key infrastructure (PKI)*. The figure that follows illustrates the components in a PKI.



One important issue is how to establish a reliable method to tie people together with their public keys. Using readily available digital signature software products, individuals and organizations can easily create their own public/private key pairs, sign documents digitally, and circulate their public keys to be used for verification. However, there is nothing to prevent them from claiming any identity they wish for the digital signature they create. Confidence in a transaction or document interchange depends upon knowing for certain that the public key being used really belongs to the party it represents. Unless the user of the public key knows the owner personally, some trusted authority is needed to vouch for the authenticity of the key before the digital signature can be trusted to authenticate the sender. By way of analogy, if every driver could issue his or her own driver's license, no one would trust its validity except those who personally knew the driver. Because licenses are issued by the state department of motor vehicles, an authority that is certifying it has sufficiently verified the identity of the holder, they are regarded as a trusted means of authenticating the driver.

In a PKI, this role is called a *certification authority (CA)*. A CA vouches for the relationship between the identity of a *subscriber* and the subscriber's public key. Typically, subscribers request certification by supplying some base information about themselves (e.g., name, address, e-mail address, name of organization, and sometimes other facts). After the CA verifies the information, a public/private key pair is generated (by either the CA's computer or the subscriber's computer). The private key goes to the subscriber, and the CA issues a *digital certificate*. The certificate contains the subscriber's public key and is signed by the CA's private key to authenticate it. It also contains some of the base information identifying the subscriber

and may indicate the level of certification assigned to the subscriber. The current industry standard specification for digital certificate formats is known as X.503. The CA sends the digital certificate to the subscriber, and may also send it to a repository or certificate distribution system if desired.

Digital certificates can be disseminated by the sender through e-mail or posted on a Web site. For effective widespread use of digital signatures, however, digital certificates must be easily accessible to any user who needs a party's public key to authenticate a document (or to encrypt a private message to send to that party). Even if the public key is in hand, there needs to be a method to ensure that the certification is still valid. For these reasons a PKI includes an online certificate repository that can easily be accessed by the public at any time. Certificates are stored and organized in a directory server for easy retrieval. People who use a public key issued by a CA to exchange messages or documents securely with its owner are called *relying parties*, as they must trust the CA that issued the certificate to verify the subscriber's public key.

CAs not only issue digital certificates but must maintain their validity, as well. If a false identity or fraudulent use of a digital signature is discovered, a subscriber reports a stolen private key, or the subscriber simply wants to cancel a certificate, the CA must revoke that certificate. The CA then adds this information to a *certificate revocation list (CRL)*, which also is stored on the directory server. Therefore, when a relying party seeks to establish trust in a digital signature, the repository can authenticate the public key for certificates that have been issued by a trusted CA and have neither expired nor been revoked.

CAs do not necessarily need direct knowledge of a certificate subscriber to authenticate the subscriber's identity for certification. For some applicants, CAs may depend upon an *organization registration authority (ORA)* to verify the validity of the subscriber's base information. An ORA is a trusted entity that may have more direct knowledge of the individual or can investigate the facts needed for validation. Once it has sufficiently established the credentials of the subscriber, the ORA sends its approval to the CA, which then issues the certificate on the basis of its trust in the ORA.

PKIs offer the potential to permit widespread electronic interchanges to take place through reliance on extended, indirect trust rather than on direct trust. With direct trust, the recipient of an electronic document either knows the sender personally or at least knows the certifier of the sender's private key, who does know the sender. With extended indirect trust, the recipient knows a certifier who knows a certifier and so on, until the last certifier in the chain knows the sender and certifies the sender's private key. The whole basis of this chain of trust is that (1) some trusted authority has directly verified the identification and authenticity of the key-pair owner, and (2) the private key, once generated along with the matching, certified public key, has been kept absolutely secure by the owner. If the private key has been compromised in any way or the issuing authority has been found to be untrustworthy, the entire chain collapses. Making such universal, widespread interchange (i.e., beyond a relatively contained community of organizations and individuals) practical will require the continued development of firm standards and protocols to which different CAs must adhere. While there is some distance yet to go, progress toward this goal has been accelerating sharply during the past two years.

It is possible for a court system to develop its own in-house PKI and take on the role of a certifier of key pairs issued to attorneys, judges, and others needing to exchange court documents. Software products, such as those from Entrust, Baltimore Technologies, and Xcert, permit this approach. Yet setting up and operating a PKI is a fairly complex and expensive endeavor. A handful of well-known commercial CAs can provide outsourcing for this service, usually at a much lower cost and with far fewer headaches for court managers and their technology staffs. Other alternatives include establishing a national certifying authority to handle digital certificates for all participating state and local courts. A national-level approach could greatly simplify the issue of standards and compatibility. This issue ultimately may be of great importance in several areas, including transmission of documents between attorneys and the multiple state, local, and federal courts before which many of them practice; interchange between courts and different local, state, and federal agencies; and state-to-state interchange of court orders and other documents.

## Conclusion

The security of systems, data, and documents is of paramount importance to courts in their movement toward JEDDI implementations. Once a court makes the transition to electronic documents and case records, the integrity, authenticity, and (sometimes) privacy of those documents and records must be ensured through adequate safeguards. User IDs and passwords will continue to be a prevalent first-level mechanism to control access to systems and information. Courts should take the necessary steps to maximize their effectiveness throughout the network. For full-scale JEDDI environments, however, a more powerful and flexible form of security is needed if courts are to realize the potential offered by a holistic approach to information interchange in the justice community.

Court operations undoubtedly will include conducting more and more processes, procedures, and transactions over the Internet through a variety of entry points. In addition to attorneys filing electronic briefs, judges will be signing electronic orders, law enforcement officers will be signing and sending electronic arrest reports and other statements, prosecutors will be reviewing and signing charging documents, and social service agencies will be signing and sending electronic reports to the court. Rather than relying on a secure logon from inside a tightly monitored local area network, this business will be conducted from anywhere at anytime. For example, attorneys may file a brief immediately after interviewing a client or witness during a weekend in another city. Judges may review and sign documents from their homes or while attending a distant conference. More than likely, these individuals will be transmitting their documents over the public, unsecured Internet—perhaps even using their personal Internet Service Provider to access the Internet. Therefore, it is imperative to adopt a security solution designed to permit secure, authenticated transmission over an untrustworthy network.

Public key cryptography, digital signatures, and PKI technology hold the promise of the best global solution to manage risk and establish the trust needed for conducting court business in this new electronic environment. In some ways the concept of PKI is analogous to the Internet, which existed for over twenty years before it suddenly burst into almost every corner of our culture. PKI has been evolving since the early 1970s. Yet it is only within the last two years

that standards have been developed to the point needed to begin generating widespread adoption of the technology and methodologies. Pressured largely by the automobile industry and other large commercial enterprises, standards bodies and vendors have formulated nearly fifty standards and protocols to define and govern PKI technology. Incorporation of PKI components in mainstream technology such as Microsoft Windows 2000, which will provide native support for digital certificates, will help simplify its implementation within an organization.

The movement toward PKI is accelerating all the time, even though adoption of the technology is still in its infancy. Forrester Research, an information technology consulting and market research company in Cambridge, Mass., recently conducted a survey of approximately 2,500 commercial corporations with respect to their approach to security and authentication. The study revealed that 98 percent of these organizations maintain user ID and password methods for authentication of users. However, about half of the respondents were planning to implement digital certificate technology within the next two years, indicating a strong commitment to a substantial shift in their security strategies.

In addition to the widespread pursuit of PKI technology in the commercial sector, the federal government is moving forward with its own initiatives. In a keynote address given in October 1999, Richard Guida, chairman of the federal government's PKI steering committee, said that PKI technology would be deployed in several government agencies. In addition to secure interagency exchanges, the technology will be used to enable the public to interact securely over the Internet with government agencies. Guida urged both government and private entities to move forward with implementation, under the belief that the use of PKI technology will push solutions to obstacles such as the need to synchronize directories from different certificate authorities. This kind of pressure from both the public and private sectors will force the industry to work out the standards and compromises needed to permit a global solution for secure electronic interchange, regardless of which organizations are exchanging information or who the certifying authorities are. Courts need to position themselves to take advantage of this solution.

There is no universally prescribed approach to security of court information systems. Nor is it a simple matter to determine the best strategy for a particular court. A generally accepted principle of security practices is that the investment in security measures—the dollars, time, effort, and user inconvenience required—should be proportionate to the anticipated risk that must be managed. In developing a security strategy, courts should weigh carefully the risks involved in different aspects of a JEDDI implementation. While it is prudent to err on the side of caution to minimize concerns and potential objections to moving into electronic records, courts need not implement security analogous to using a howitzer for a flyswatter. Nor should courts fall into the trap of security paralysis by delaying pursuit of JEDDI until the perfect method is developed to ensure security and authenticity of all document interchange. A balanced approach is called for that includes improving policies and techniques for password-based protection of all systems, taking advantage of built-in browser-based security for Web access, and planning for inclusion of PKI technology as JEDDI projects expand beyond initial pilot implementations.



## CHAPTER SEVEN

### *New Jersey's JEDDI Project*

#### Project Background

The New Jersey Administrative Office of the Courts (AOC) began preliminary planning for a JEDDI project in late 1995. The idea for an electronic filing project germinated through discussions between the managers of the technology and the civil practice divisions. They proposed the concept to the chief justice and the assignment judges. The chief justice strongly supported the idea and, with the agreement of the assignment judges, directed the AOC to move forward with the project. A new technology project team was formed with a senior member of the staff appointed to direct the project.

#### Characteristics of New Jersey's JEDDI Project

- Civil case pilot project
- Totally electronic case record through e-filing and imaging
- Remote application execution and file upload via dial-up connection to PC on AOC WAN
- Semi-automated interface to CMS
- Web interface and Internet e-mail under development

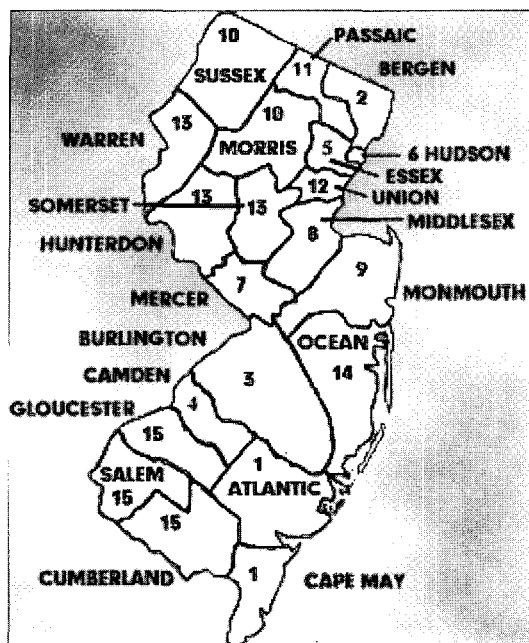
#### *Initial Challenges*

With the help of others at the AOC, the team began research into electronic filing issues and JEDDI technology. They faced many challenges, including uncertainty of the issues, absence of any proven model to follow, and no clear vision of how to move the electronic folder throughout the courthouse. Two specific issues facing the team were (1) what format would be appropriate for the electronic documents, and (2) how the integrity of the documents could be maintained. Furthermore, a major constraint imposed upon the team was the necessity to avoid any significant effect on the existing statewide automated case management system (ACMS). It would be impractical to modify this legacy system to any extent to integrate an electronic front end with it; consequently, all of the interfacing would have to be accomplished through the new electronic filing module.

#### *Pilot Court Selection*

As they completed their preliminary research, the team began considering an appropriate county for a civil case pilot project. Monmouth County was identified as an excellent choice for several reasons. The court leadership and personnel were regarded as being forward thinking and willing to undergo the difficulties associated with a new approach. The administrative judge enthusiastically volunteered his court to cooperate with the AOC in a pilot project. In addition, the court had a well-functioning local area network in place already. The Superior Court of

Monmouth County handles a medium-level, but growing caseload with a substantial number of retail debt collection cases involving not more than ten thousand dollars. The AOC staff and court leaders felt that filings for such cases in the superior court's special civil part would be an ideal basis for the pilot project.



After Monmouth County was chosen during the spring of 1996, the team recognized the importance of involving the law firms early in the project to study their operations, obtain their input for the system requirements, and educate them about how the new processes would work. Members of the team visited ten of the higher-volume filers of collection cases of less than \$10,000 in the Special Civil Part of the Superior Court of Monmouth County. The purpose of these visits was both to look at their operations and to assess their suitability for participation in the pilot project. Some firms immediately asked to participate, others were willing to participate once they understood the project better, and a third group resisted the idea of electronic filing.

### *Selection of Law Firms*

The project leaders sought a range of characteristics across several firms. They wanted a mix of large and small firms. They wanted some firms that were well versed in technology. An important qualification was good management and organization of the practice. Ultimately, five of these firms were selected for initial active participation in the pilot project. One was a solo practitioner, one had two partners, and two had a large volume of filings, even though they did not have a large number of attorneys. Other reasons for selecting a particular firm included a particularly high-technology operation, active participation in the local bar, and the fact that at least one client already was passing electronic files to the law firm.

### *Development and Implementation*

The technology team analyzed the workflow and operations of the court and the law firms and developed a conceptual design for the system. After reviewing the design with the court and attorneys, the team developed the first version of the software, naming it "Judiciary Electronic Filing and Imaging System" (JEFIS). The system was implemented in August 1998 for testing in parallel with the existing paper system. Corrections and refinements were made during this testing until the system was operating to everyone's satisfaction. The recommendation was made to go live with the electronic filing procedures effective March 1, 1999. As of that date, the electronic file would become the official one. Papers not filed

electronically were to be scanned to create a document image file so that the entire case file would become electronic. No more paper records were to be maintained for these cases.

## Court Rules Affected

New Jersey had approximately twenty court rules that had to be addressed to permit courts to accept electronic filing. In late 1996, the New Jersey Supreme Court prepared a single, comprehensive order that relaxed some of these rules and supplemented others, paving the way for implementation of electronic filing. The order was issued and made effective January 1, 1997. Specifically, it was issued to permit the establishment and operation of the pilot project in the Monmouth County Superior Court. The administrative director of the New Jersey courts issued a notice to the bar informing them of the pilot project and the supreme court's new order. The notice and the court rule are shown below.



### NOTICE TO THE BAR

#### *Re: Monmouth County Special Civil Part Electronic Filing/Imaging Pilot Project*

Effective January 1, 1997 the Supreme Court has relaxed or supplemented 20 court rules to permit the establishment of a pilot project this Spring in the Monmouth County Special Civil Part to test the use of electronic filing and imaging technology for documents filed with the court. The pilot project will involve only civil actions that are within the \$10,000 monetary limit of the Special Civil Part. Tenancy actions and small claims will not be included in the pilot. Initially, attorneys selected by the Assignment Judge will file pleadings and other papers electronically. The paper filings of other selected attorneys and pro se litigants will be scanned electronically and stored as images in the pilot project's computers. These computers are capable of managing documents in both electronic text and image formats and they will be used to process, store and retrieve all papers normally kept in a paper case file jacket, such as court orders, affidavits, summonses and writs. In the meantime, the current paper processing operation will continue in the Monmouth County Special Civil Part for cases that are not part of the pilot project. The number of cases in the pilot project will gradually be expanded so that all Special Civil filings in Monmouth County (except tenancy and small claims) are either received electronically or scanned and stored as digital electronic images. At this point, the pilot project will be evaluated to determine the next steps in utilizing this technology. Questions or comments should be directed to Robert D. Pitt, Chief of Special Civil Part Services at the Administrative Office of the Courts. The text of the order follows.

James J. Ciancia  
Administrative Director of the Courts  
Dated: January 7, 1997

## SUPREME COURT OF NEW JERSEY

Whereas the Supreme Court's Judiciary Information Systems Policy Committee has proposed the establishment of a pilot project to test the use of electronic filing and imaging technology in the courts of this State;

Pursuant to N.J. Const. (1947), Art. VI, §2, par. 3, it is ORDERED that the Rules of Court be relaxed and supplemented, as set forth below, to permit the establishment and operation of a pilot project in the Special Civil Part of the Superior Court, Law Division, Monmouth County, in which attorneys selected by the Assignment Judge will electronically file pleadings and other papers, while the filings of other selected attorneys and *pro se* litigants will be scanned electronically, and computers capable of electronically managing documents and images of documents will be used to process, store, and retrieve pleadings and other papers, including court orders, process and judgments, in civil actions where the amount in controversy does not exceed \$10,000 and the actions are filed in that court pursuant to Rule 6:1-2(a)(1):

1. Rule 1:4-4(c) is relaxed to permit an attorney participating in the pilot project who files an affidavit or certification electronically to use a facsimile of the original signature regardless of the affiant's availability, and the original signature of an affiant who is an attorney may be typed or digitized if the affiant is the individual attorney who is filing the document electronically; however, the remaining requirements of the rule remain in effect.
2. Rule 1:4-5 is relaxed to permit the use of the individual attorney's typed or digitized signature on all documents filed electronically that would otherwise require the attorney's handwritten signature.
3. Rule 1:4-8 is supplemented to impose its obligations upon an attorney who uses a typed or digitized signature on a document that is filed electronically.
4. Rule 1:4-9 is relaxed to permit attorneys participating in the pilot project to file all pleadings and other papers in an electronic format prescribed by the Administrative Office of the Courts which will produce, as needed, printed paper copies that meet the requirements of the rule. Pleadings and papers subsequent to the complaint may be filed electronically only in those cases which were commenced by the electronic filing of the complaint.
5. Rule 1:5-2 is relaxed to permit attorneys participating in the pilot project to serve one another electronically through the pilot project's computer system, if it provides this service, with copies of all papers referred to in Rule 1:5-1.
6. Rule 1:5-3 is supplemented to permit the use of the individual attorney's typed or digitized signature in lieu of a handwritten signature on a certification of service appended to a document filed electronically by the attorney.

7. Rule 1:5-6(b) is supplemented to the effect that documents transmitted electronically to the court after 4:00 p.m. shall be deemed received on the next court day.
8. Rule 1:13-4 is supplemented to provide that the papers transferred to another court or agency may be printed paper copies of the documents that have been filed or stored electronically by the court.
9. Rule 1:37-2 is supplemented to permit the printed reproduction of the court's seal on all papers required by the Rules of Court to contain a seal.
10. Rule 4:42-1(e) is relaxed to permit the judge to electronically affix a facsimile of the judge's signature to an order or judgment, to permit the submission of the form of order or judgment electronically by an attorney participating in the pilot project and to require the submission of only the original of the form of order or judgment by all other participants in the pilot project. The rule is further relaxed and supplemented to dispense with the requirement that a self-addressed, stamped envelope be submitted by the participating attorney or party submitting the form of order and to require, in lieu thereof, prepayment of the postage to send a copy of the order.
11. Rules 6:1-1(d) and 6:12-2 are relaxed to permit the electronic filing of all papers by transmission to the Special Civil Part in Monmouth County or to the Administrative Office of the Courts in Trenton, as required by the pilot project.
12. Rule 6:2-2(a) is relaxed and supplemented to dispense with filing the summons and copies of the complaint and participants in the pilot project shall file an original complaint, either electronically or on paper, together with such electronic data or a paper form containing such information as the Assignment Judge may require for the pilot project to produce the summons.
13. Rule 6:2-3(d)(1) is relaxed to permit the clerk to transmit the required information by electronic means.
14. Rule 6:2-4 is supplemented to permit the Monmouth County Special Civil Part Clerk or designee to electronically affix a facsimile of the clerk's signature to all process issued by the court in pilot project cases.
15. Rule 6:3-3(a) is supplemented to permit the Assignment Judge to require the submission with the moving papers of prescribed information in electronic form or on a paper form in pilot project cases.
16. Rule 6:3-3(c)(4) is relaxed and supplemented to permit the clerk to send notice of a hearing by electronic means rather than mail, to an attorney who has filed pleadings electronically in the case.
17. Rule 6:7 is supplemented to permit the Monmouth County Special Civil Part Clerk or designee to electronically affix a facsimile of the clerk's signature to all process for the enforcement of judgments. Rule 6:7 is further supplemented to permit the judge to electronically affix a facsimile of the judge's signature where necessary for the enforcement of judgments.

18. Rule 6:7-1(a) is supplemented to permit requests for the issuance of writs of execution and other process for the enforcement of judgments to be made electronically by attorneys who have filed their pleadings in the case electronically.
19. Rules 6:8 and 6:9 are supplemented to permit the Monmouth County Special Civil Part Clerk or designee to electronically affix a facsimile of the clerk's signature to all process requiring the clerk's signature. Rules 6:8 and 6:9 are further supplemented to permit the judge to electronically affix a facsimile of the judge's signature to the orders, writs, warrants or judgments that require the judge's signature.
20. Rule 6:12-2 is further supplemented to dispense with the requirement that a self-addressed, stamped envelope accompany requests for information or the return of papers regarding pilot project cases and to require, in lieu thereof, prepayment of the postage necessary for mailing the paper.

It is further ORDERED that the terms of this Order become effective January 1, 1997 and remain in effect until further Order of the Court.

For the Court,  
Deborah T. Poritz  
Chief Justice

## Major Obstacles

The project team encountered several obstacles in their attempt to develop and implement a successful JEDDI system. Among these were typical problems resulting from staff turnover at the AOC and local court, the need to learn new technology skills, and the frustration of dealing with new releases of operating systems that must be adjusted to during the course of application software development and implementation (e.g., moving from Windows 3.1 to Windows 95, and then to Windows 98). Two obstacles were particularly challenging: one a technical issue and the other a human issue.

### *Interface with Legacy System*

A major objective of the JEDDI project was to integrate electronic docking, electronic filing, and an electronic case jacket. Such integration requires a number of application interfaces between existing hardware and software components for the docketing and case management functions, as well as new hardware and application software developed to provide the JEDDI capabilities. New Jersey was one of the earlier states to develop a statewide case management system, which has evolved through the years to provide more and more features and functions. The powerful, but venerable Automated Case Management System (ACMS) resides on the mainframe computer in Trenton. Unfortunately, the complex, legacy system was a poor candidate for adaptation to JEDDI technology. Consequently, the requirements for the electronic filing front end had to be based on the precise data elements needed for input to that system and the data formats that it could handle effectively. Laboring under this constraint, the team designed JEFIS so that data flows through it almost transparently and into ACMS. Specifically, an ASCII file created in JEFIS updates ACMS and generates a summons, almost as if the data had originated through standard ACMS keyboard data entry.

### *Securing the Support of the Bar*

Convincing some of the law firms to participate in the electronic filing project was a real challenge. One of the problems is that law firms often have a specialized workflow involving a large staff devoted to paperwork. Changing over to an electronic process requires a significant reengineering of staff roles with consequential training demands and other personnel issues. A few of the firms in Monmouth County seemed to be almost wedded to the paper environment. Turning around some well-entrenched practices proved to be a substantial accomplishment.

Another problem the team encountered was that many law firms that were making use of automation were not really up to date with their technology. Some had minimal or outdated hardware and software, and showed little interest in upgrading. Fortunately, the technology requirements for the law firms to participate in the JEDDI project were fairly modest by today's standards:

- Pentium processor
- ReachOut remote access software
- Desktop document scanner
- Microsoft Word (97 or lower) or WordPerfect (8 or lower).

The total technology investment required is approximately \$2,000 for a small firm. This is a nominal amount when compared with the less tangible costs involved in changing office procedures and workflow.

Faced with this resistance, AOC staff and the administrative judge made appearances at state and local bar association functions and committee meetings to generate support for the project. The major purpose of these appearances was to inform the attorneys about the project and explain the potential benefits for their practices. A deliberate effort was made to limit other types of publicity for the project in the early stages to avoid building false expectations for either the end results or the pace of development. These efforts were largely successful, and the general support from the bar has been good. As the pilot project began operating successfully, interest in it began spreading among the law firms.

The project team also had to be careful to avoid becoming too involved in supporting the law firms in the selection and operation of their computers, scanners, and communications equipment. The range of skills and knowledge among the law firms is considerable. The AOC has encouraged the law firms to become technically self-reliant, dealing with hardware and software problems themselves, whether through training of their own staff or through securing outside commercial technology support services. The AOC staff is available to answer any questions about the electronic filing procedures and system, of course, and can assist the law firms in troubleshooting general problems.

## **System Design and Operation**

### ***System Overview***

JEFIS, New Jersey's JEDDI system, is designed as a hybrid text and imaging system. It permits attorneys to prepare, in effect, an electronic cover sheet for new complaints through a Windows-based application containing data entry forms. Along with the electronic cover sheet, law firms submit the complaint itself as a word processing document, and they have the option to attach a TIF file containing the scanned image of any exhibits. The electronic cover sheet is used in a clerk's office application to feed case initiation information to ACMS on the AOC's mainframe computer, thereby eliminating manual data entry. However, no electronic cover sheet is prepared for subsequent documents filed for the same case.

JEFIS converts the word processing document constituting the complaint into an image file, to which the images of exhibits are appended. The image file is then stored in an electronic case jacket in the document image database for subsequent court activities. Subsequent filings in the case also are submitted as word processing documents with optional TIF image attachments, but no electronic cover sheets. The court scans in paper documents and stores them in the image



database. All electronic case documents filed after the initial filing of the complaint require docketing through standard data entry functions in the clerk’s office. Similarly, all paper filings—including complaints—require manual docketing after scanning. Regardless of the manner of filing, then, all case documents wind up as document image files, which are linked to ACMS through docket entries. JEFIS uses Watermark imaging software and includes workflow functions as well as specific features that permit judges to retrieve, review, annotate, and sign documents electronically. No paper files are kept for these cases.

The major components of the system are the law firms’ electronic filing interface applications, the clerks’ docketing functions, and the courts’ retrieval and annotation functions. The electronic filing user interface comes in two varieties: “Quick Filer” and “Batch Filer.” Quick Filer enables the user to prepare a single case filing, including the electronic cover sheet for a new complaint. The Batch Filer application provides a more efficient method for larger law firms to transmit a number of a certain type of document for several different cases at the same time. The filing programs are written in Microsoft Visual Basic. E-mail, workflow functions, and automated application interfaces fuse all the components into a smoothly operating, totally electronic system.

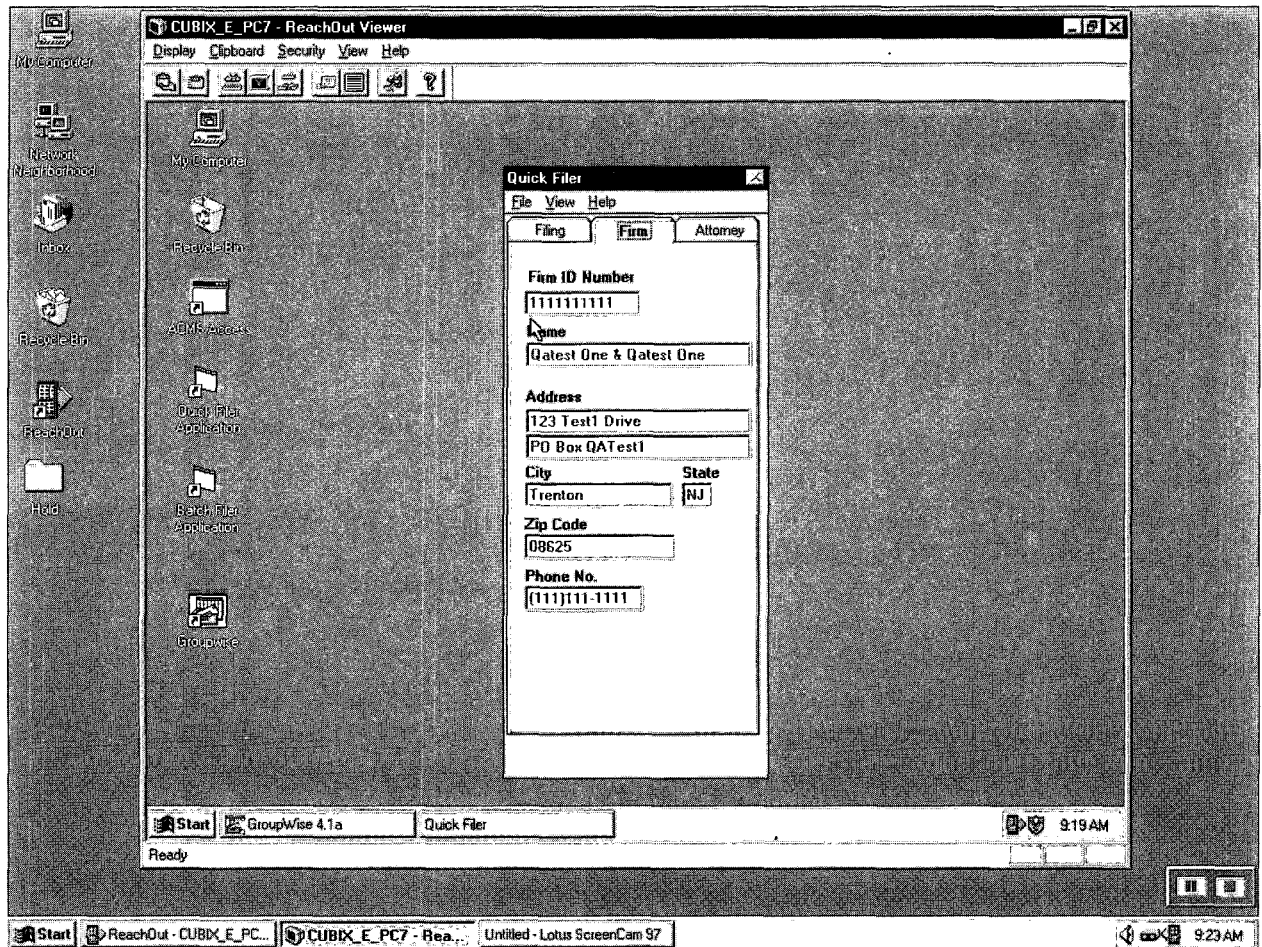
The AOC took an interesting approach with the user interface. The project team decided not to install the applications in the law firms themselves. Instead, Quick Filer and Batch Filer reside on PCs (actually on PC cards) at the AOC in Trenton. Loaded on the PCs in the law firms is ReachOut, a commercial remote-access software package from Stac, Inc. ReachOut enables the attorneys to establish a modem-to-modem connection to the AOC via a toll-free number. Once logged on, the attorney can execute Quick Filer or Batch Filer remotely, controlling the application just as if it were running on the local computer. The PCs at the AOC are connected to the judiciary’s statewide wide area network (WAN). Consequently, documents filed electronically through either Filer application are sent to the local court through the Groupwise e-mail system that runs on the WAN. Through the same dial-up connection and ReachOut, the law firms can access ACMS to look up and display information from the case database. The current pilot system permits eight concurrent dial-up connections.

### *Quick Filer*

Quick Filer is the interactive application designed for the initial filing of new cases. Before logging on to JEFIS, the law firm first prepares the complaint as a standard word processing document. If the attorney plans to attach any exhibits to the complaint, the staff scans those on a desktop scanner, creating a TIF image file. Once all the files for the case have been created and saved in a directory on the local PC, the attorney or designated staff runs the ReachOut software to dial up and log on to the AOC computer. From the desktop on the host PC, the user double-clicks the Quick Filer icon to launch the program and then follows the general sequence of steps shown below (along with illustrations of the Quick Filer screens displaying test data).

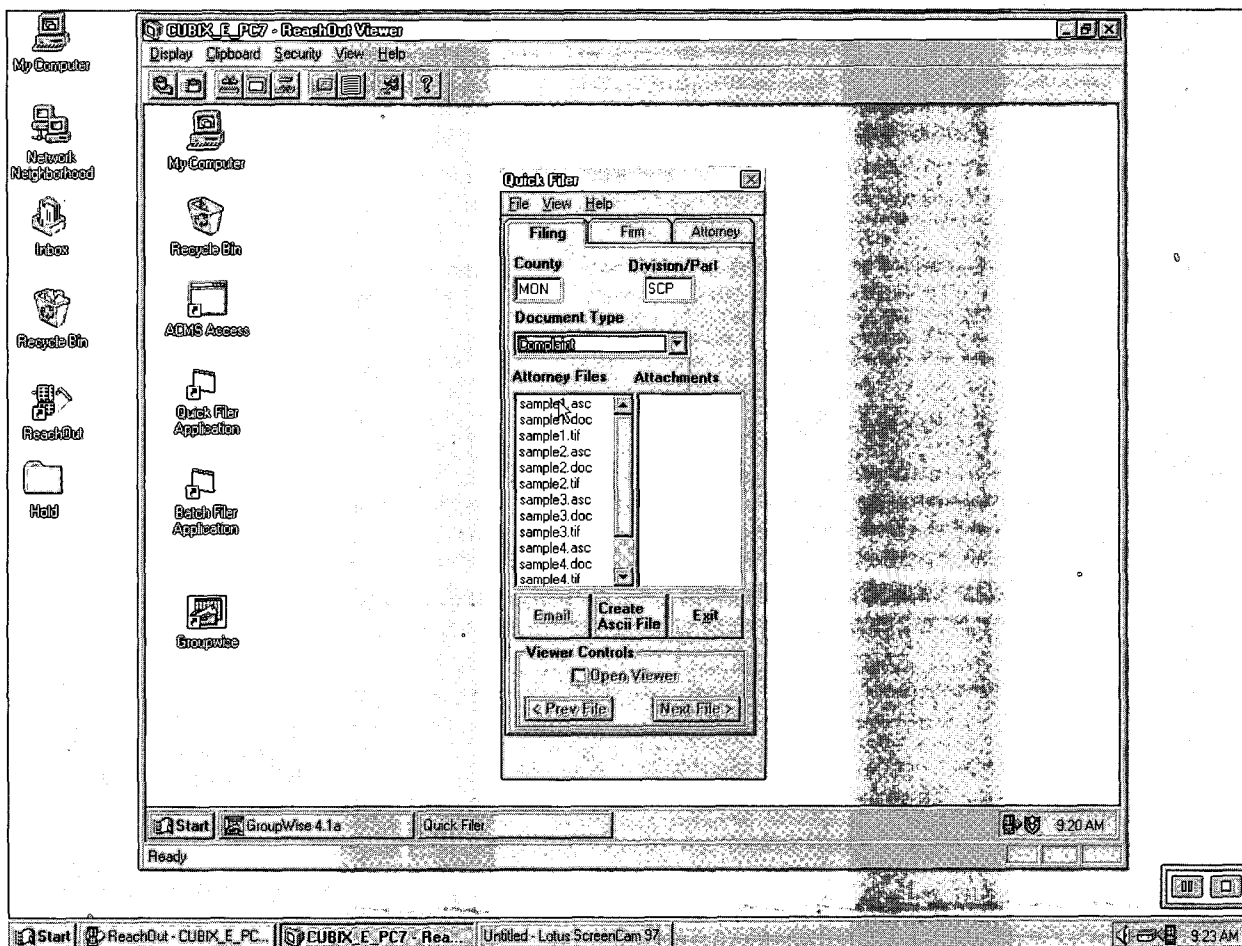
### Step 1.

The user enters or verifies the identifying information for the law firm and attorney.



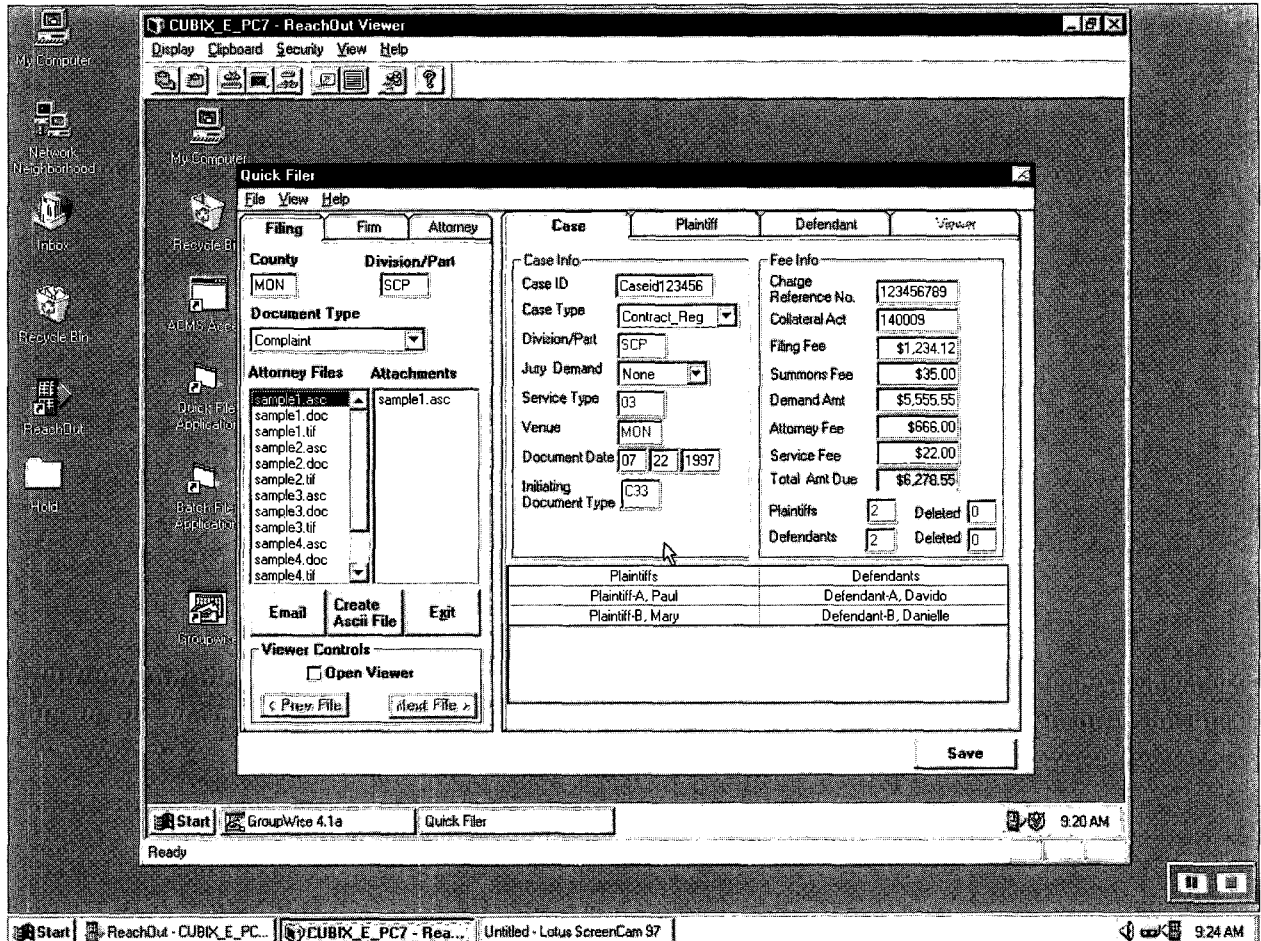
Step 2.

The user clicks on the “Filing” tab and selects the type of document to be filed (e.g., complaint) from a drop-down box of document types.



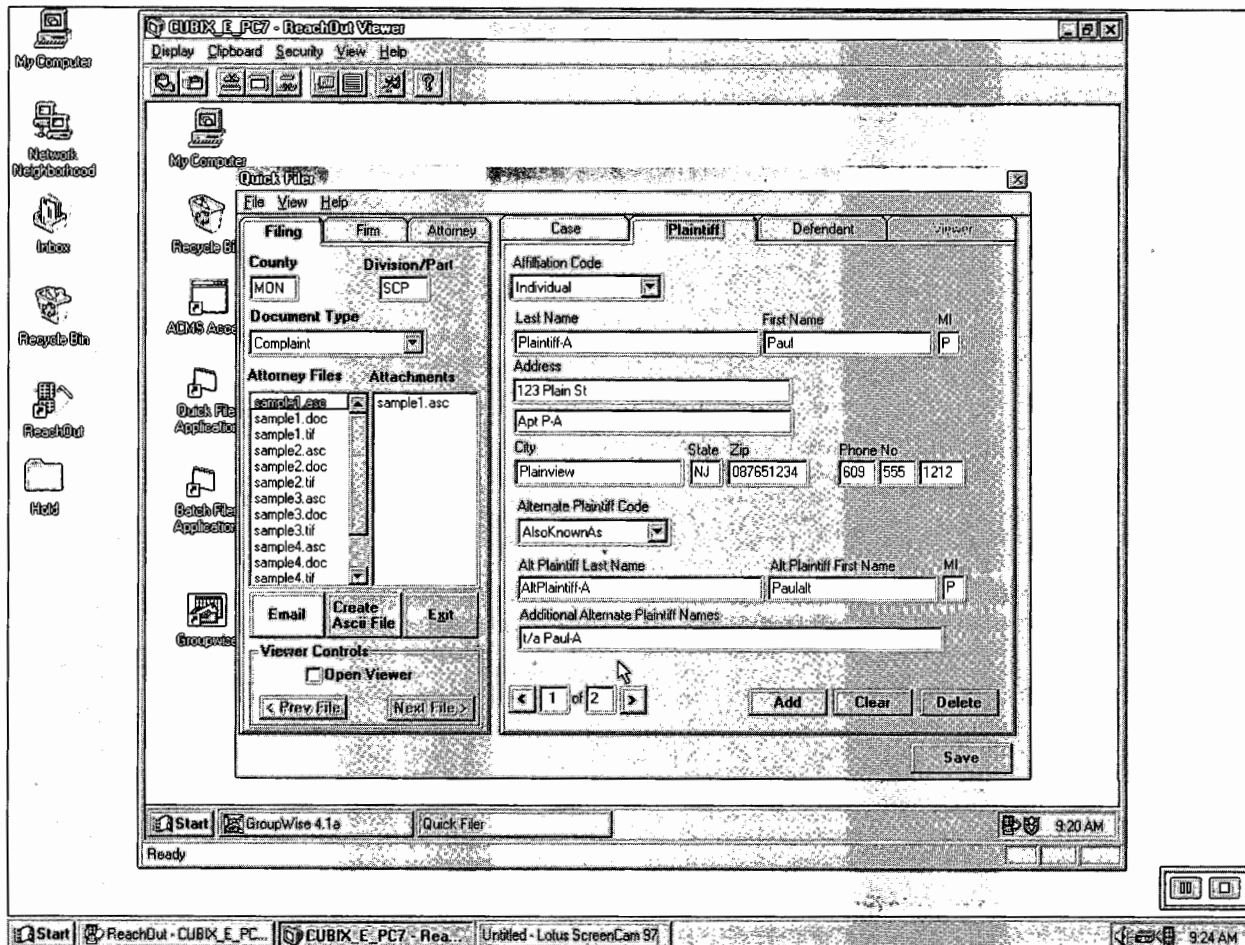
### Step 3.

On the basis of the information in the complaint to be filed, the user goes through the data entry form windows, entering basic case information required by the program.



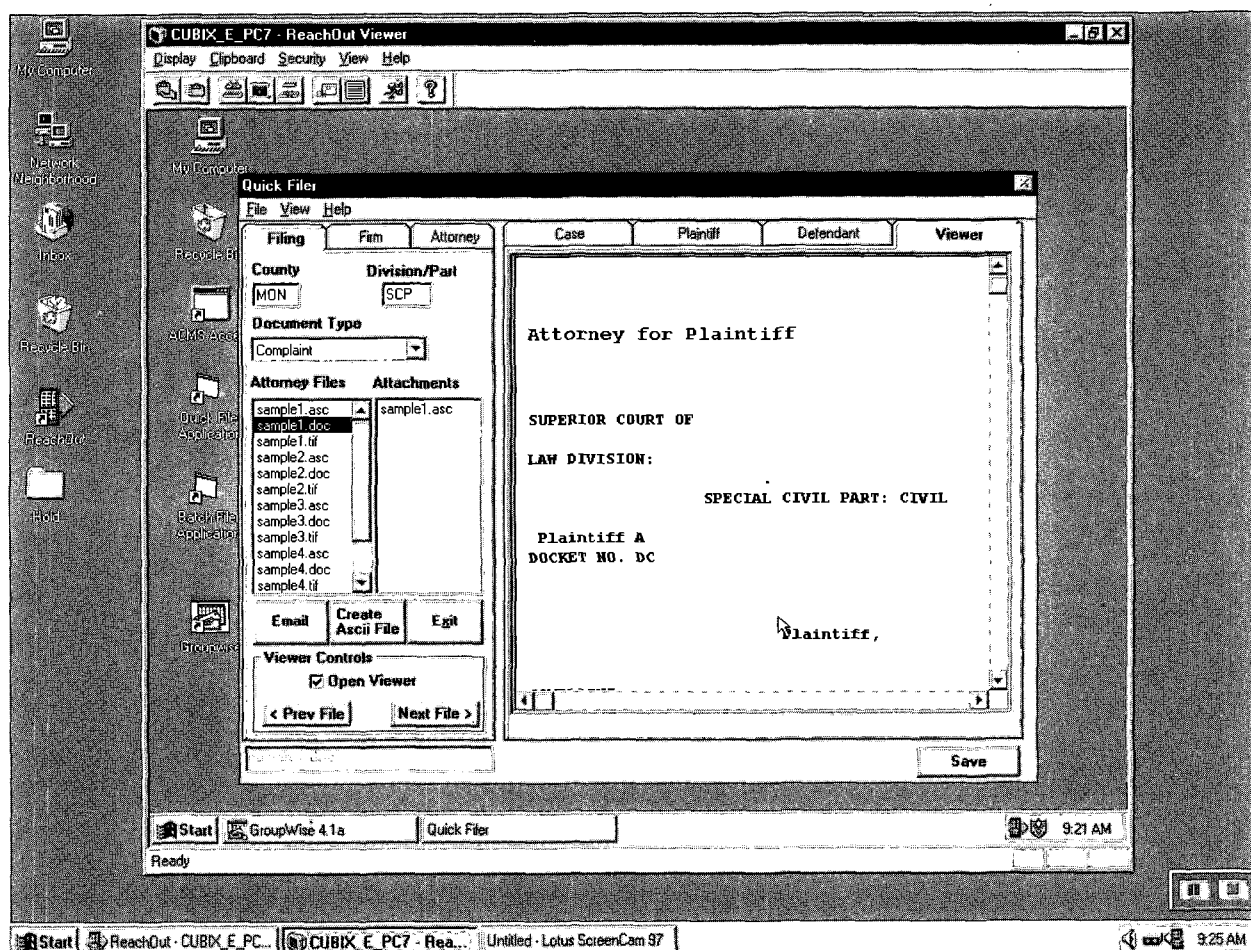
## Step 4.

The user enters information about case parties, filling in all the required fields on the party forms.



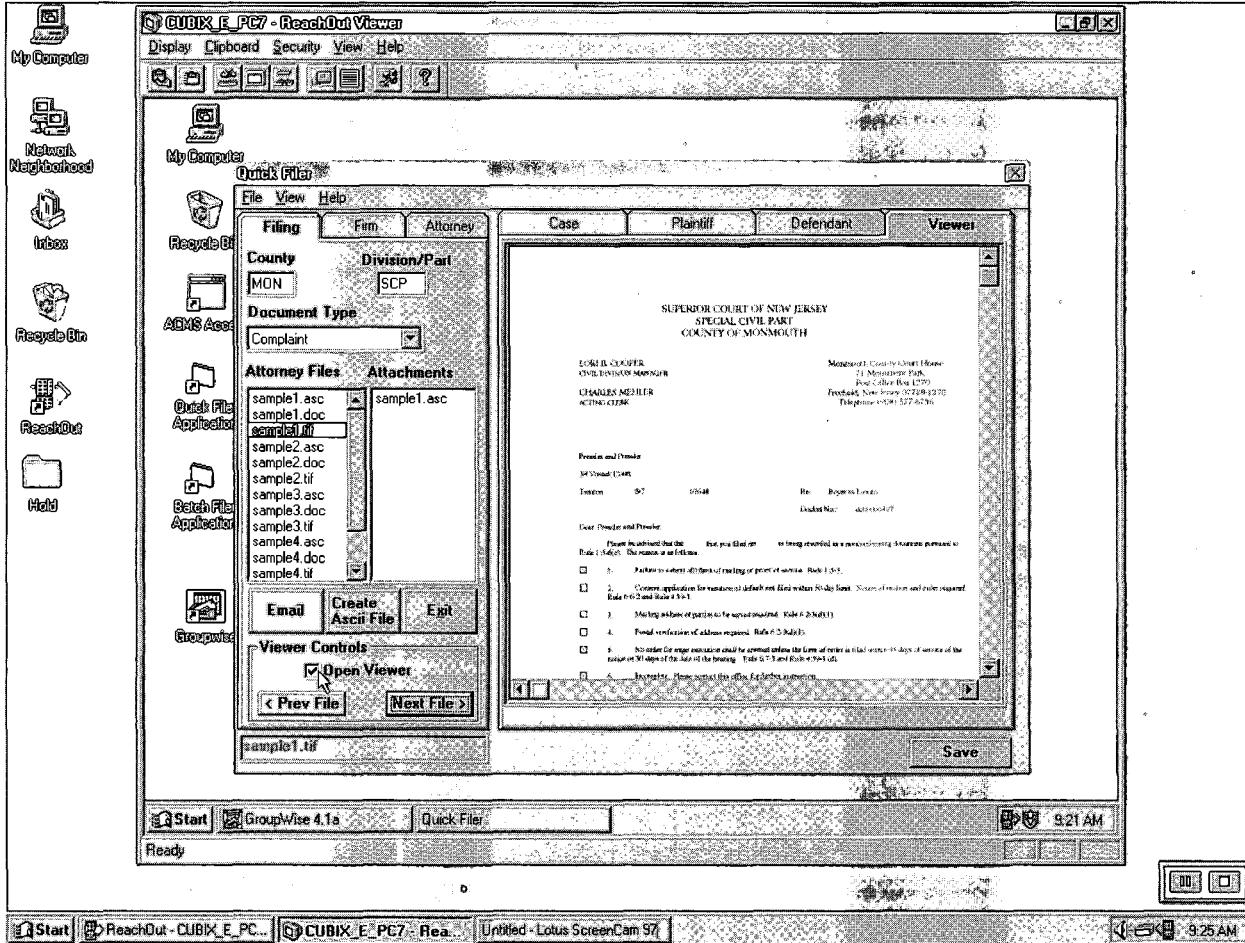
## Step 5.

When all data fields have been entered and validated by the program, Quick Filer generates an ASCII text file containing the data (with filename extension ASC). The user then uploads the word processing document file (with DOC extension) and can review it through the Quick Filer Viewer window.



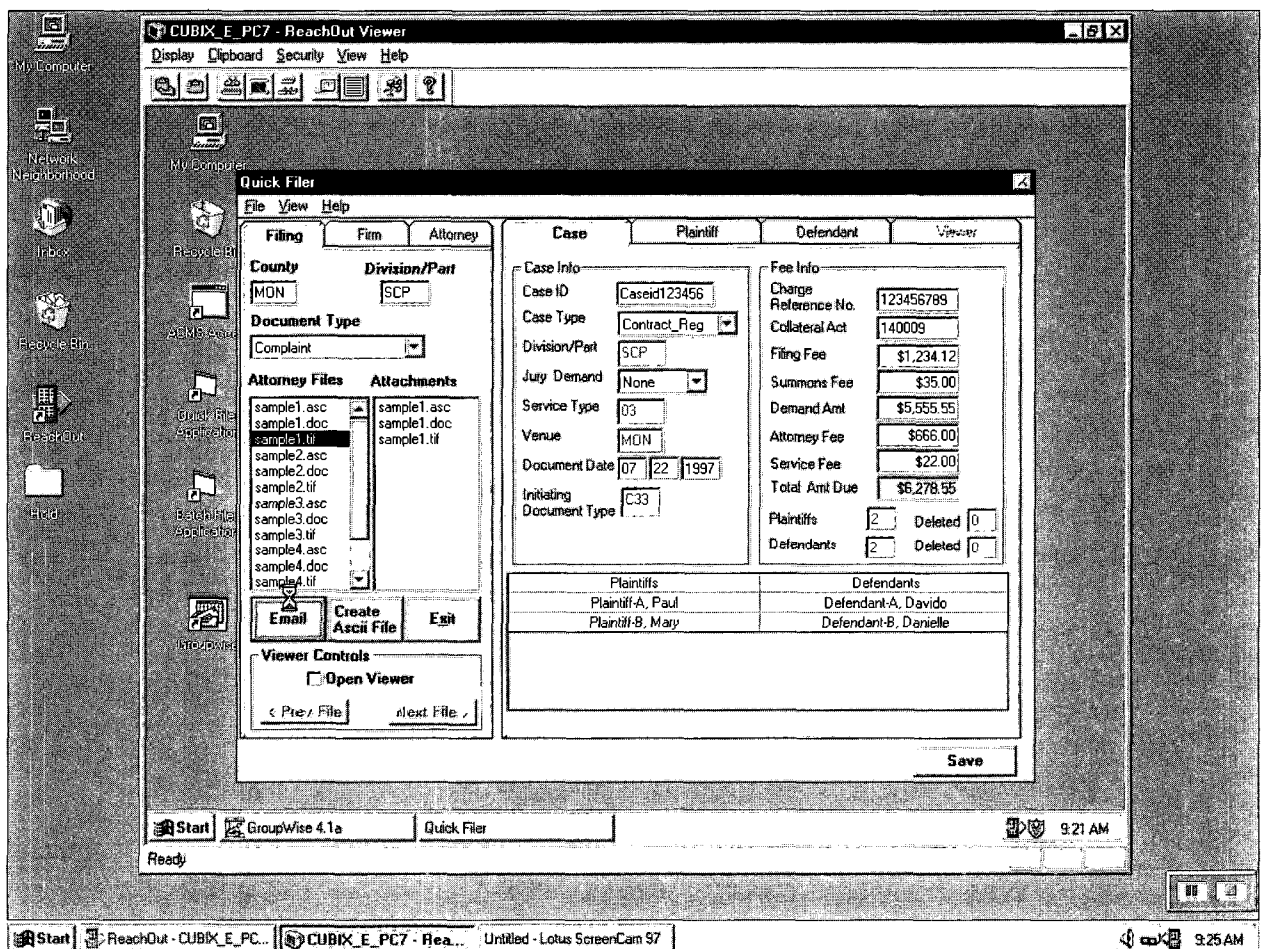
Step 6.

If there are any scanned exhibits to accompany the complaint document, the user uploads the TIF files created by the scanner in the law firm. The images also can be viewed through the Quick Filer Viewer.



## Step 7.

When the user is satisfied with the preparations of the filing materials, he or she uses the mouse to drag the designated file names into the Attachments window and then clicks on the E-mail button. Quick Filer validates the filing and reports any errors to the user for correction. If the files are valid, Quick Filer opens an interface with Groupwise and e-mails the set of files to the designated court. The system archives a copy of the e-mail message and then deletes the files from the hard drive on the AOC's PC.



## Batch Filer

The Batch Filer application provides an efficient way for a law firm to submit to the court a larger number of documents at a time. Essentially, it handles the last step in the Quick Filer application; however, instead of the user dragging a specific set of electronic document file names into the Attachments window, Batch Filer processes all files in the batch that the user has



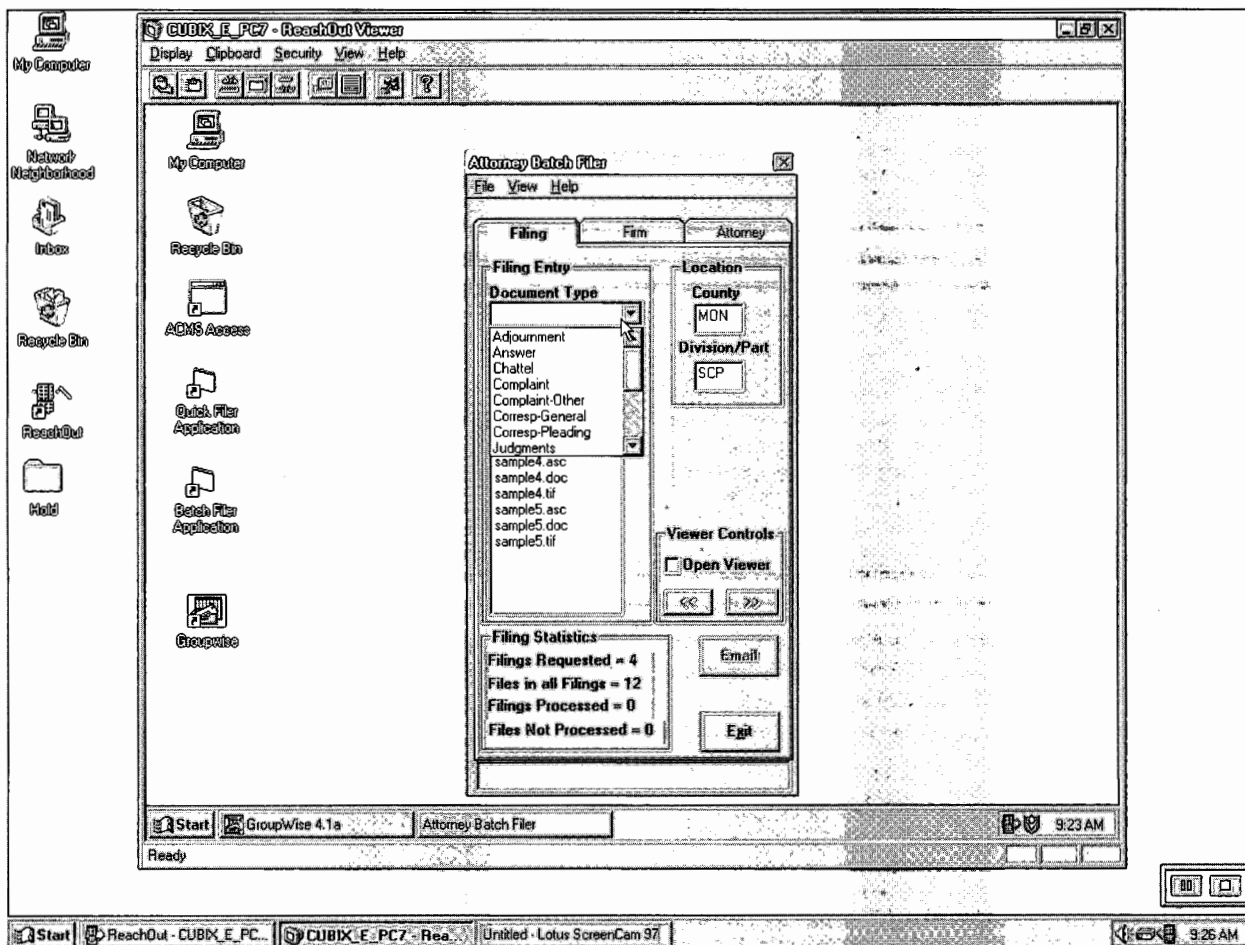
built up on the AOC’s PC. Only like documents can be batched together. The steps required for Batch Filer are much simpler than those for Quick Filer.

### Step 1.

The user goes through the same process of verifying attorney and firm information, identifying the filer as was shown for Quick Filer.

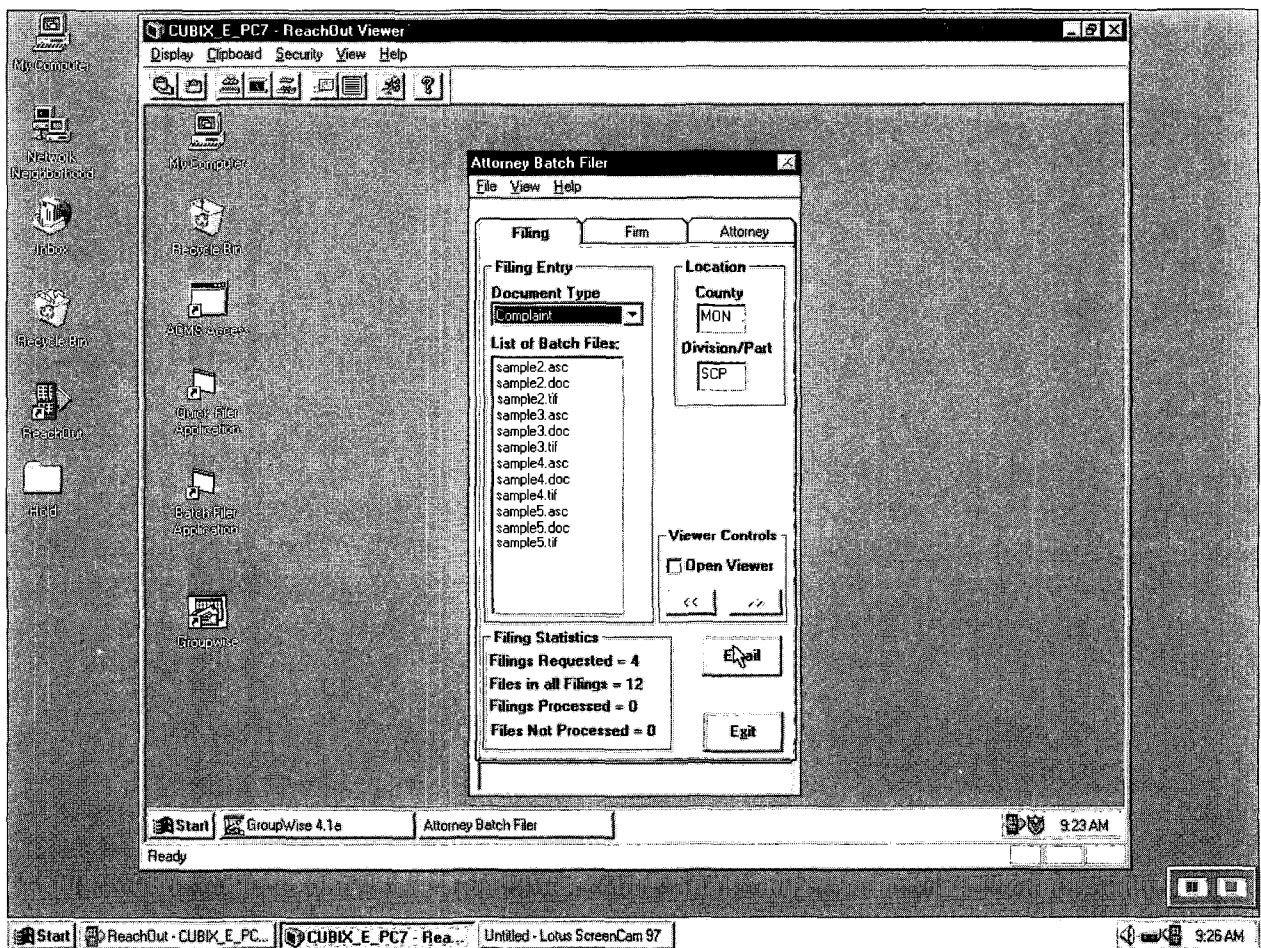
### Step 2.

The user selects the type of documents in the batch. Word processing files and TIF files (and ASCII files if the document type is a complaint) can be included for each case; however, the document and exhibit images must all be of one document type (e.g., complaint, answer, or motion).



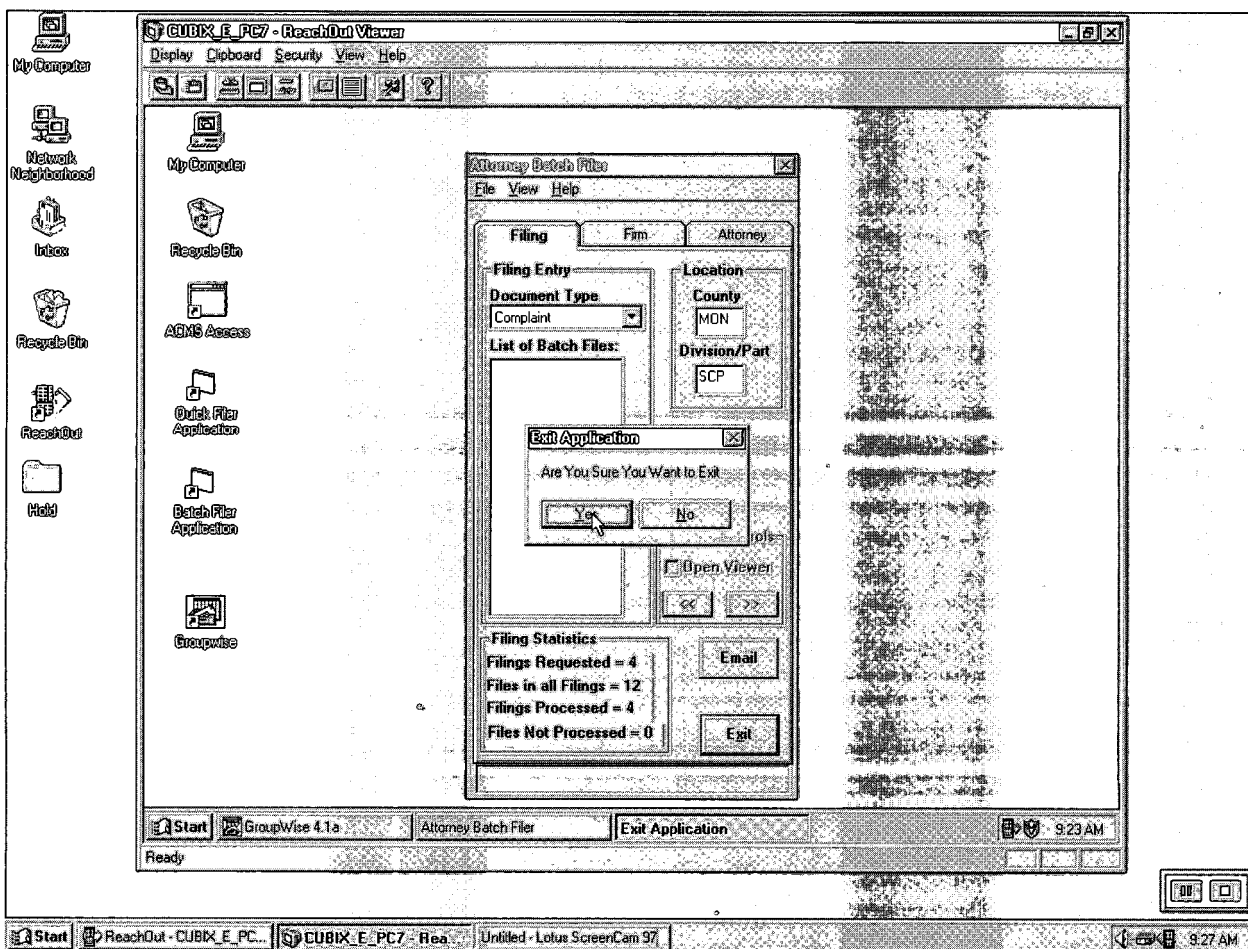
### Step 3.

The user clicks on the E-mail button. Batch Filer validates the set of files, links to Groupwise, and generates the e-mail for transmission to the target court. If any errors are reported, however, the user must execute Quick Filer to correct them, as Batch Filer does not include this capability. Cases with errors are simply omitted from the group transmitted to the court.



#### Step 4.

Batch Filer indicates the filing statistics for the batch transmitted. It displays the number of filings requested (i.e., the number of cases in the batch), the total number of files (including all ASC, DOC, and TIF files) contained in those filings, the actual number of filings processed successfully, and the total number of files that could not be processed. The user exits Batch Filer by clicking on the Exit button and then confirming the intended action by clicking the OK button on the dialogue window.



### *Import Function*

JEFIS incorporates a Windows system agent function at the local court level that polls incoming e-mail to detect electronic filings coming in. When it receives an e-mail containing a complaint filed electronically, it opens the ASCII text file (the electronic cover sheet) created through the Quick Filer function and saves the data to an SQL database. On the basis of the case information contained in the text file, it uses a word processing template to generate a summons.

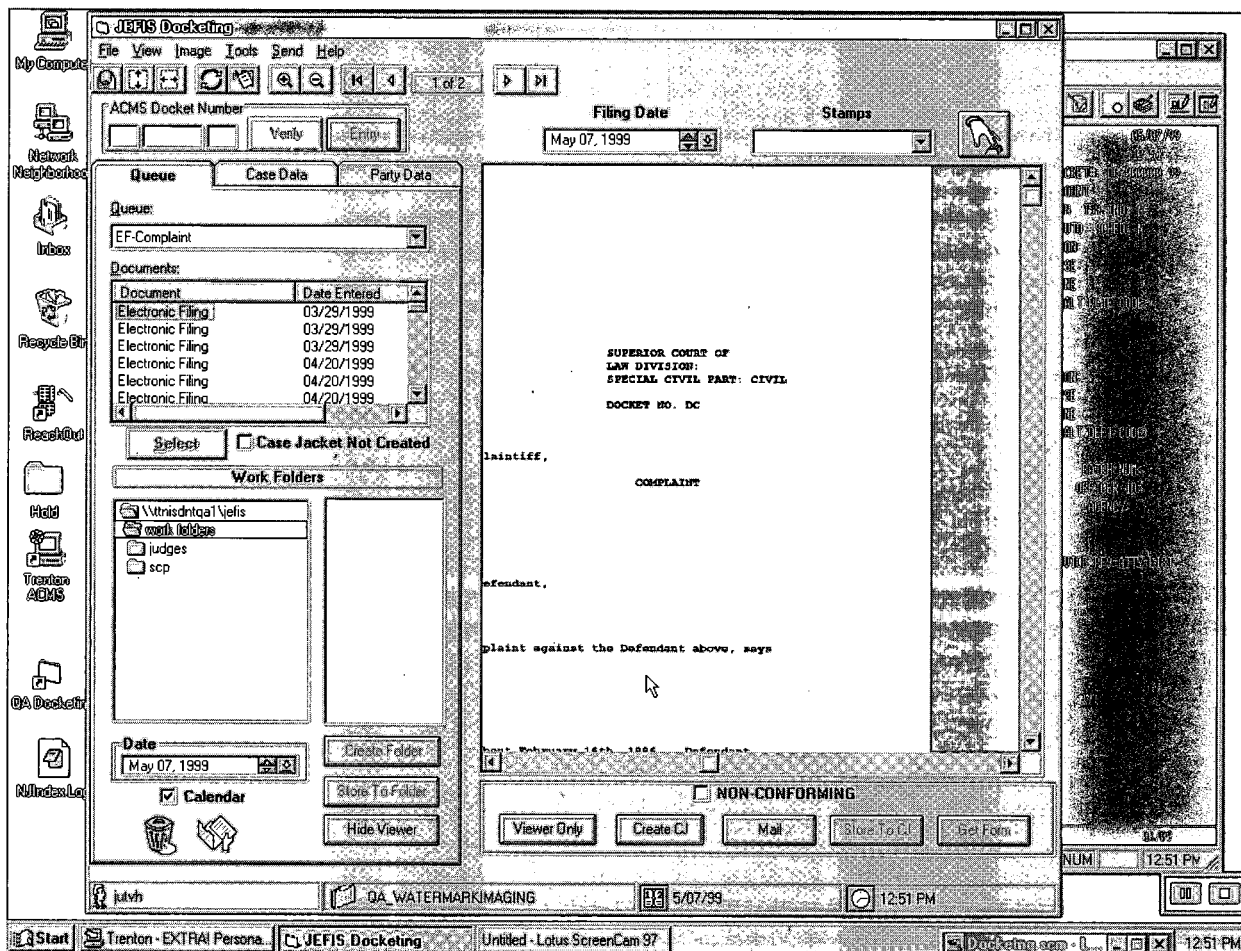
Then it opens the word processing document, converts it to a TIF image file, and appends any TIF files for exhibits that were filed with the complaint. The image file then is electronically stamped with the date and time received, and it is stored in the court's image database. The filing also enters the workflow procedures and is placed in a queue for the appropriate court staff.

## ***Docketing***

JEFIS has a docketing module that automates the process of transferring data from the complaint to the ACMS database. It uses data from the JEFIS SQL database that originated with the ASCII text file created by Quick Filer as the electronic cover sheet for the initial case filing. The docketing process is relatively fast and simple for the clerks, and it provides the human screening that the court desires to ensure that documents filed electronically are correct and appropriate for the case. The steps involved are summarized below.

Step 1.

The clerk reviews the work queue and retrieves the new filing. JEFIS displays the image of the complaint through a viewer window so that the clerk can inspect it and compare the information with the data from the electronic cover sheet.



## Step 2.

The docketing module opens the appropriate data entry screen in ACMS and displays it in a window beside the window displaying the complaint data. When the clerk approves the filing, the system automatically transfers data field-by-field from the JEFIS database to the ACMS screen. The clerk can watch this process. General case information is entered first; then the party data entry screen opens in the ACMS window, and the corresponding information is transferred from the JEFIS database window.

The screenshot displays two windows from the JEFIS Docketing application. The left window, titled 'JEFIS Docketing', shows a 'Case Data' tab with a table of case information. The right window shows a detailed view of the case data, including party information and case details.

**JEFIS Docketing - Case Data**

Description	Value
Attorney ID	6097774595
Receipt No	140009
Atty Attn Fname	Qandandy
Atty Attn Mid	Q
Atty Attn Lname	QJefis1
Venue	MDN
Case Type	028
Init Type	C33
Service Type	03
Demand Amount	6555.55
Amt Recvd	1234.12
Jury Ind	N
Charge Ref#	123456789
Payment Type	CG
Chg Batch No.	009
PI# Fname	lad Incor
PI# Mid	p
PI# Lname	Stracquatano & Bors
PI# Address1	123 Plain St
PI# Address2	Apt P-A
PI# City	Plainview
PI# State	NJ
PI# Zip	087651234
PI# Phone	6095551212
PI# Affiliation	CRP
Alt PI# Code	DB
Alt PI# Fname	tp

**JEFIS Docketing - Party Data**

```

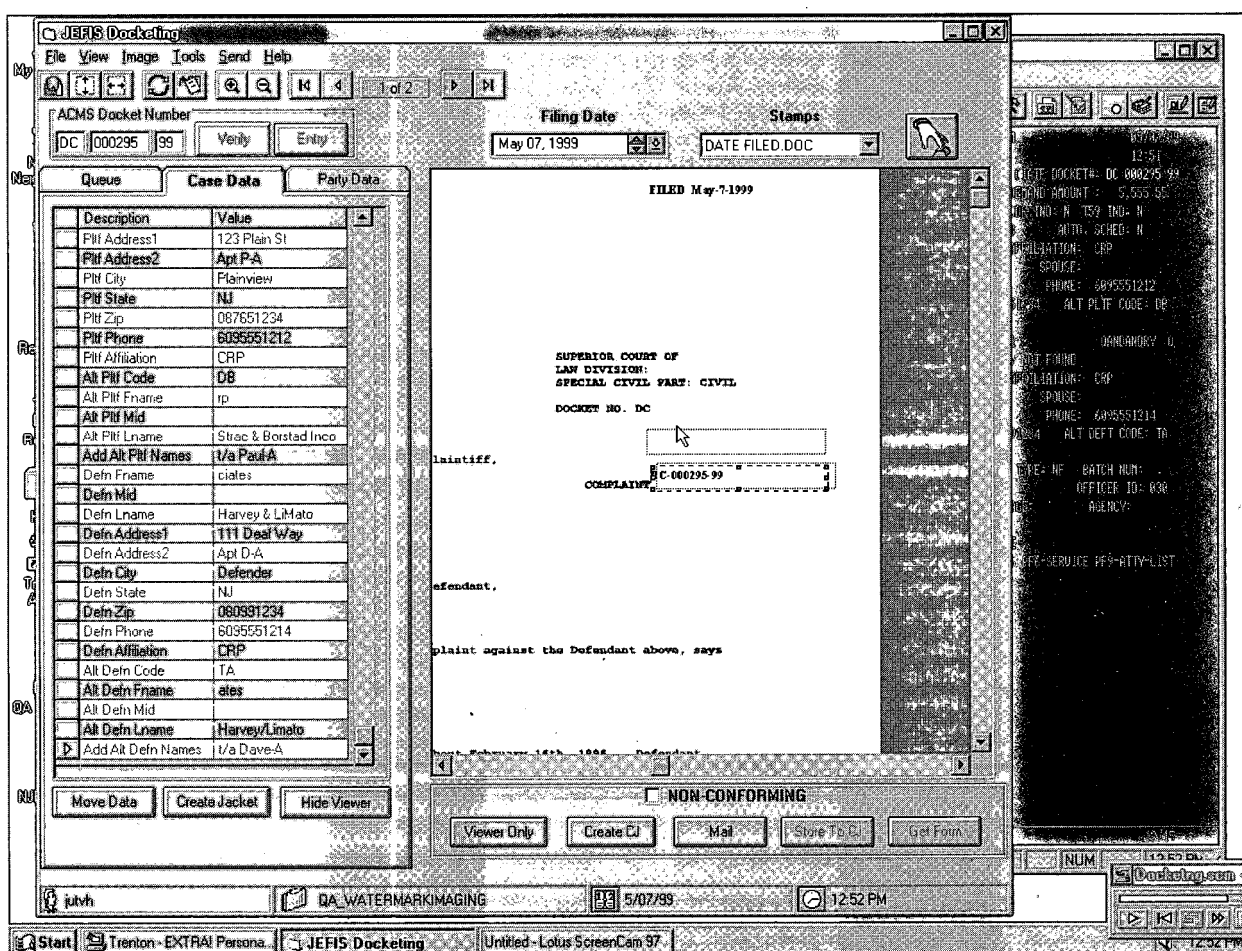
CASE TYPE : 028  DATE FILED : 05 02 1999  DEMAND AMOUNT : 5555.55
INIT DOC : C32  INIT TYPE : C  JURY IND : N  CR IND : N  T99 IND : N
FREQ FILER : 000  PRO SE IND : N  SERVICE TYPE : 03  AUTO. SCHED : N
PLAINTIFF : Stracquatano & Bors, tad Incor, p  AFFILIATION:
ADDRESS : 123 Plain St  SPOUSE:
          : Apt P-A  PHONE : 6095551212
CITY : Plainview  STATE: NJ  ZIP: 087651234  ALT PLTF CODE:
ALT PLTF:
ATTORNEY ID: 6097774595  ATTY ATTN: QJefis1  Qandandy, Q
          :  FIRM NAME:
DEFERMENT :  AFFILIATION:
ADDRESS :  SPOUSE:
          :  PHONE:
CITY :  STATE: NJ  ZIP: 080000000  ALT DEPT CODE:
ALT DEPT:
AMT REC'D : 1234.12  TRANS TYPE: FLF  PAYMENT TYPE: CG  BATCH NUM: 009
RECEIPT NO: 140009  CHARGE REF#: 123456789  OFFICER ID:
DISTRIBUTED FEES-STATE:  OFFICER:  MILEAGE:  AGENCY:
COMMENTS :

PF1-PARTY PF2-COMMENTS PF3-ATTY PF4-PROBMT PF5-TRANS PF6-SERVICE PF9-ATTY-LIST
  
```

The bottom of the screen shows the Windows taskbar with the Start button, open applications (Trenton - EXTRA! Persona..., JEFIS Docketing, Untitled - Lotus ScreenCam 97), and the system tray (12:51 PM).

### Step 3.

ACMS accepts the docketing action and generates a new case number. The clerk then selects an electronic stamp from a drop-down box and electronically imprints an image of the stamp on the image of the complaint. JEFIS extracts the case number generated by ACMS, updates the JEFIS database with it, and adds it to the image of the complaint document as another electronic stamp. The clerk can position both of these stamps in an appropriate, clear location on the image page. Because the filing is now officially accepted, JEFIS creates an electronic case jacket (a file folder) and “burns in” the stamps on the document image to make them permanent.



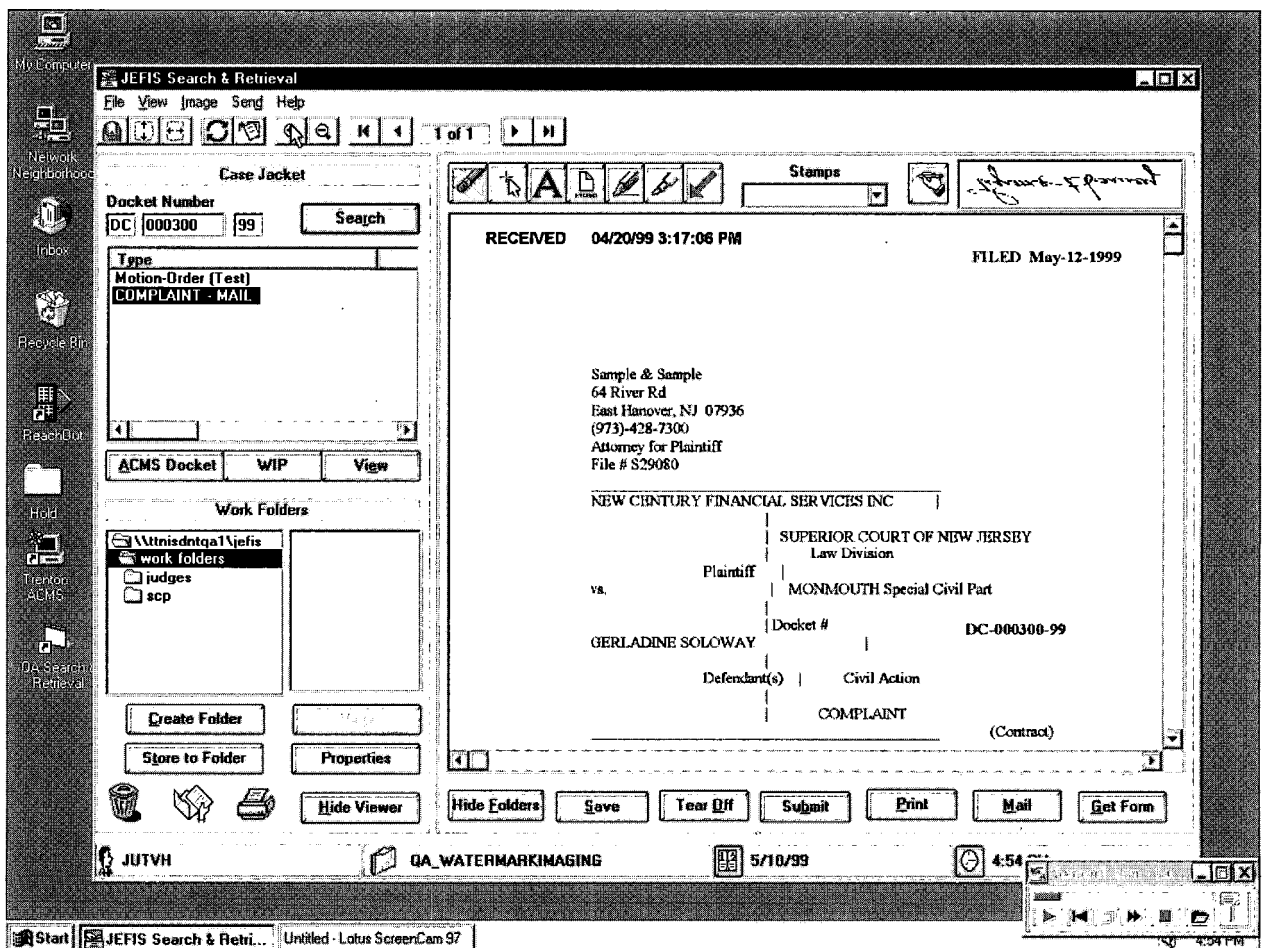
### Search and Retrieval Function

Once a document has been filed (either electronically or on paper with subsequent scanning) and entered into the image database, it can be retrieved for further processing through the Search and Retrieval function. Documents can be retrieved by entering the case number in ACMS and placing the cursor on the docket entry for the particular document of interest. The JEFIS Search and Retrieval function will pull up the corresponding document folder. Judges

work with case documents electronically through this function, which is illustrated through the following steps, in which a judge reviews a complaint and a subsequent motion. The motion includes a proposed order, which the judge approves with modifications and issues as an official order.

### Step 1.

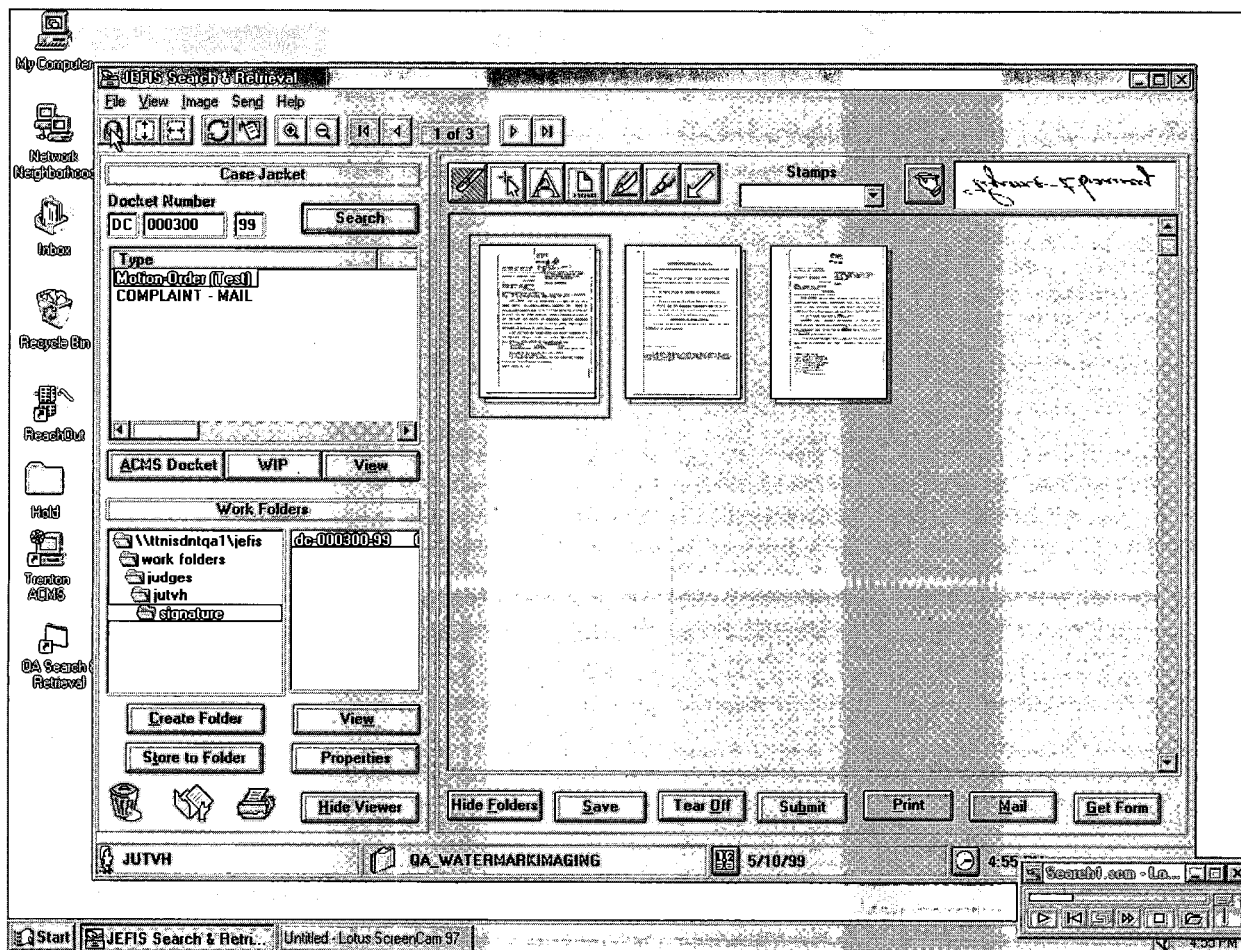
The judge retrieves, displays, and reviews the complaint (which was mailed in and scanned).





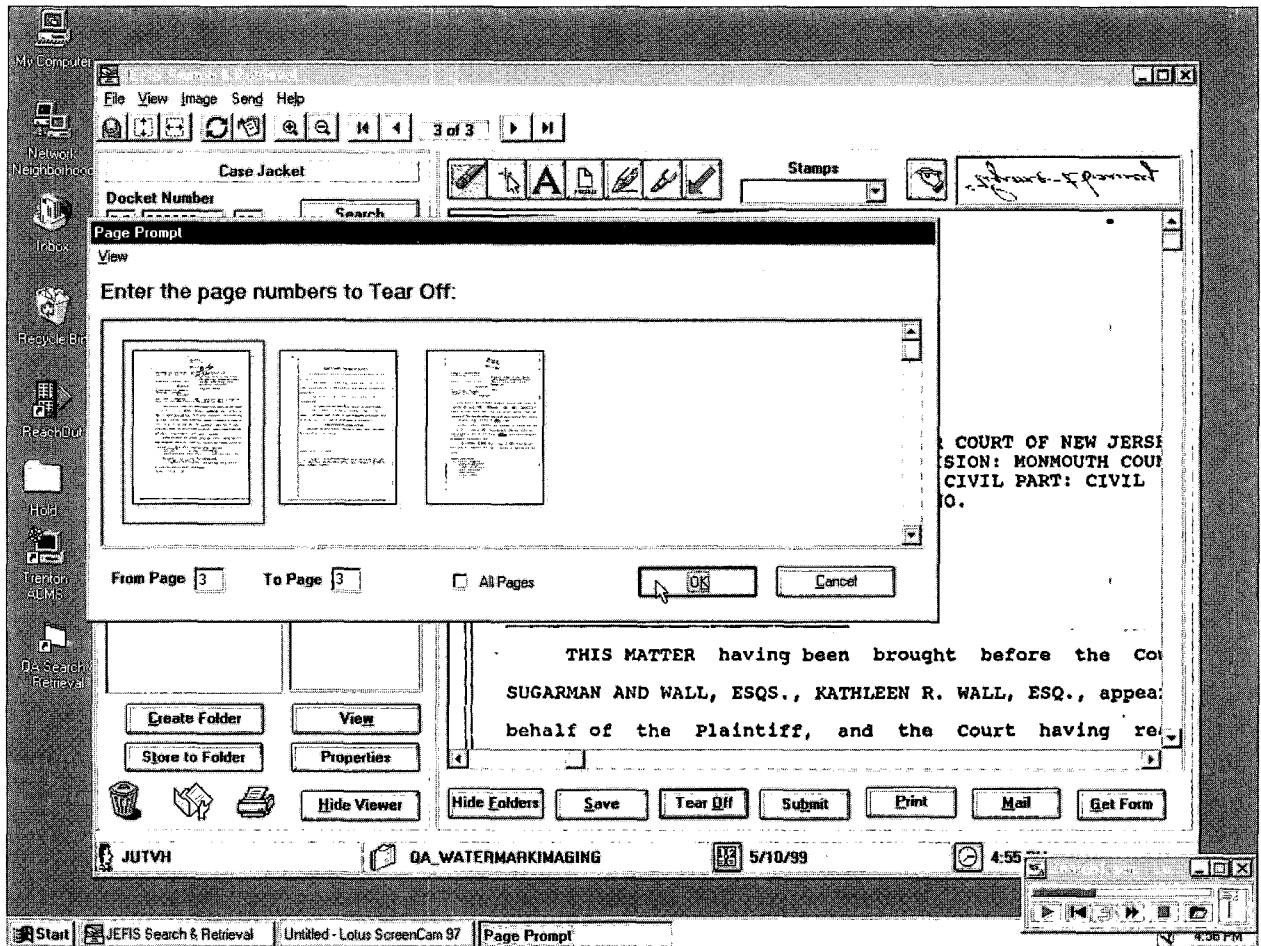
Step 2.

The judge retrieves and displays the motion and proposed order, then chooses a multipage window that presents a thumbnail image of all pages in the document.



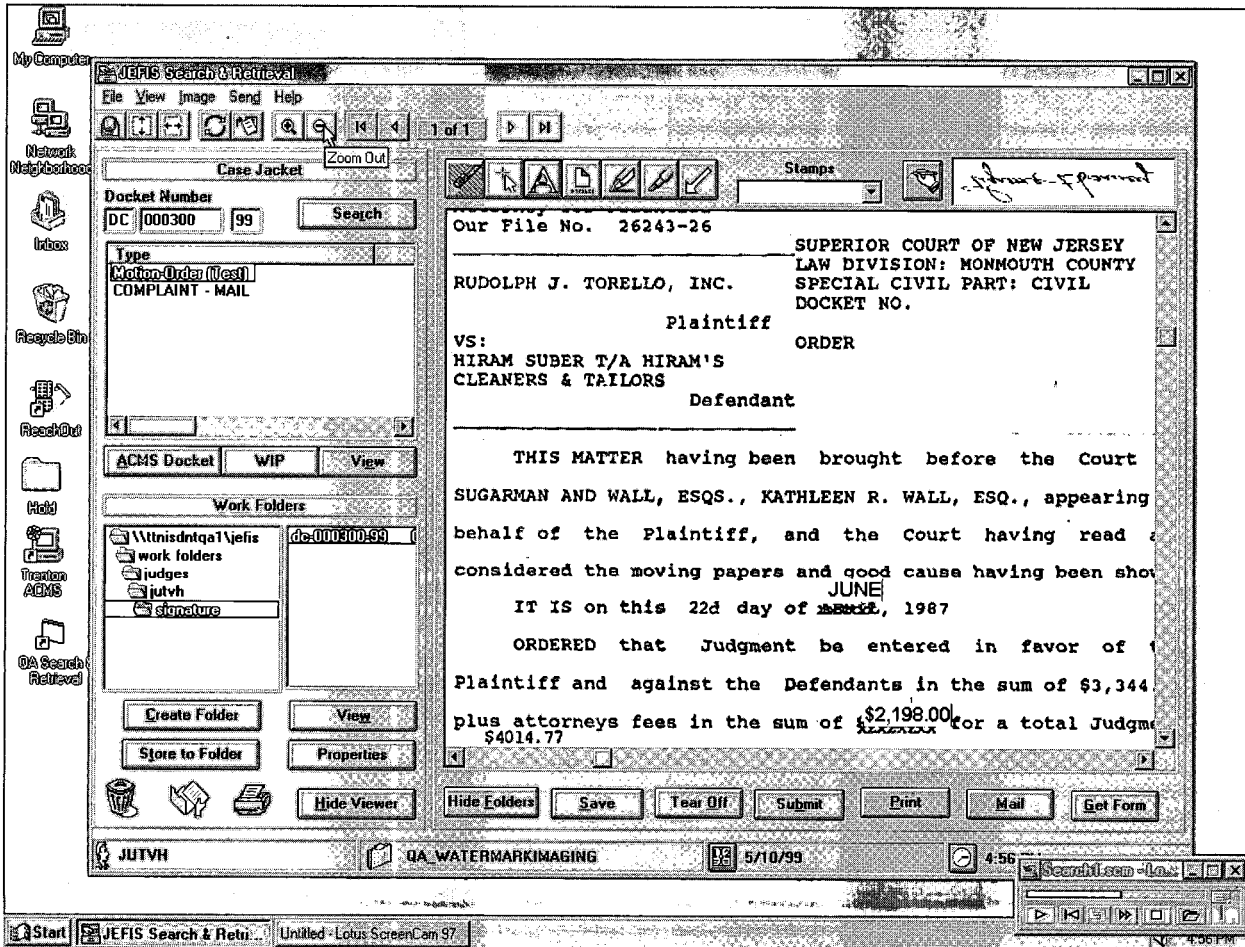
### Step 3.

The judge uses a “tear-off” function to select and create a copy of the last page of the document, which is the proposed order.



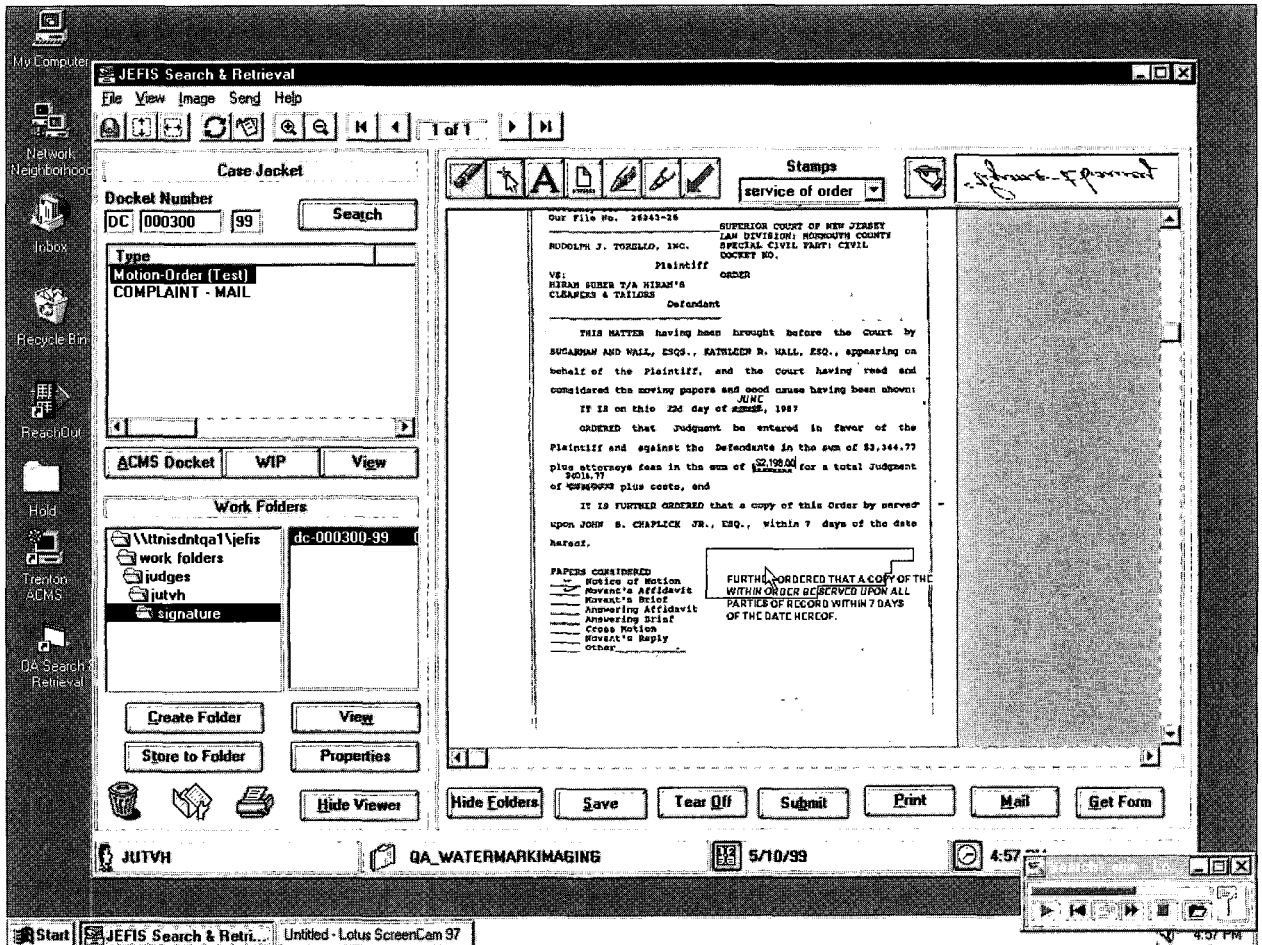
Step 4.

The judge edits the image of the proposed order, using electronic “whiteout” and typing in new fields such as the date and judgment amount.



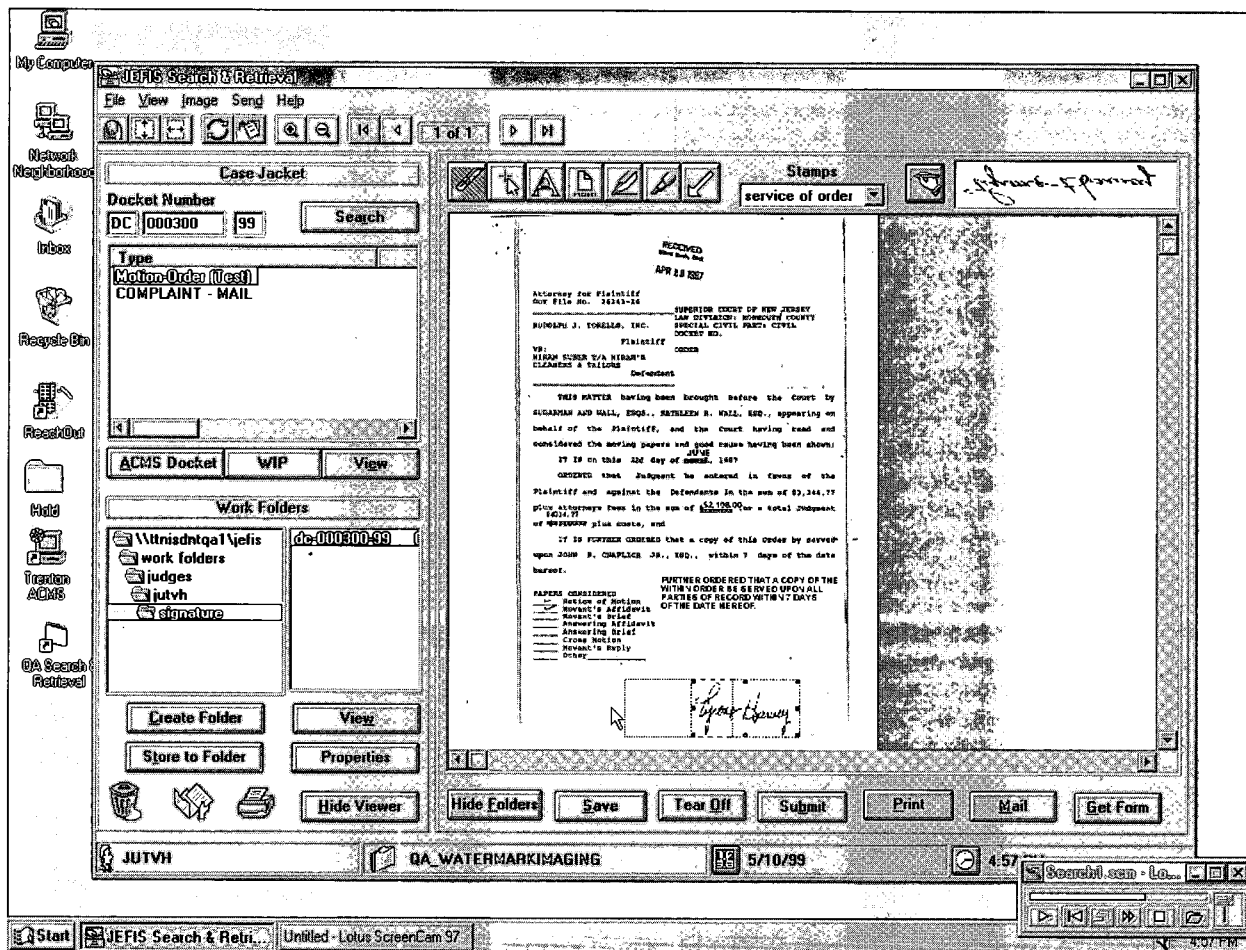
Step 5.

The judge adds a “service of order” stamp electronically, moving into the desired position on the image of the document.



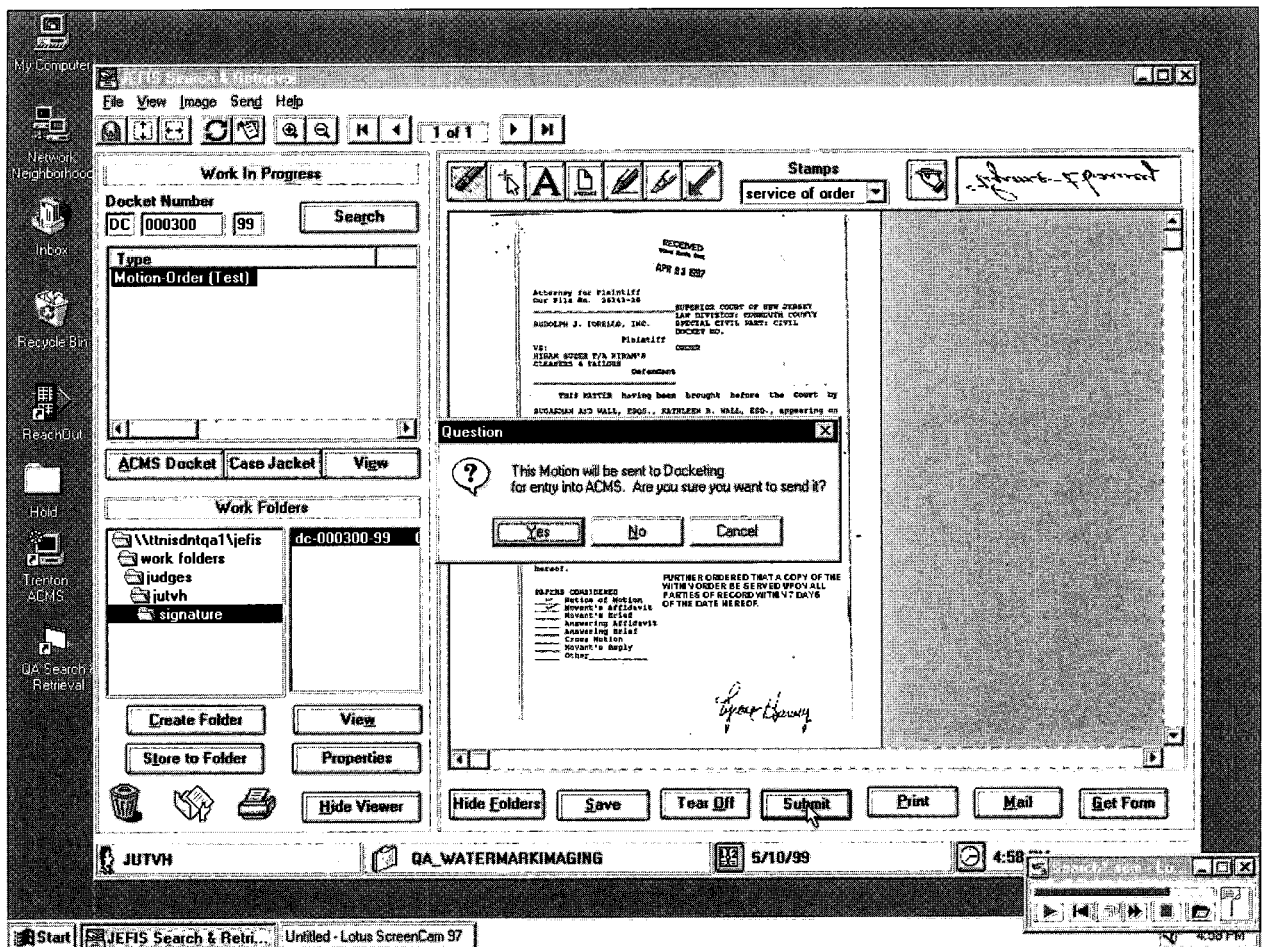
Step 6.

When all edits are completed, the judge adds his signature through an electronic signature stamp that imprints an image of the handwritten signature on the document image.



## Step 7.

The approved motion and new order are sent to the docketing workflow queue for review by the docketing clerk and (manual) docketing in the ACMS.



## Security

New Jersey's JEDDI project does not include digital signatures. For the present, the judiciary has established a policy and corresponding court rule that regards the typed name of the attorney on a filed document as the authoritative signature vouching for the authenticity of the document. System security is handled by a number of methods to control access. The first point of access is at the law firm, and it is up to the firm to control who is authorized to use the system. For example, PCs may be set up with passwords to control basic user access if desirable.

The first real control over access to JEFIS occurs through the ReachOut software used to dial into Trenton. ReachOut has one of the most robust sets of security features of any remote

access package, enabling the AOC staff to monitor and control user access. The attorney filer applications have their own security features, once a user has logged into JEFIS. The AOC’s Banyan network provides its own layer of security. Finally, the Import function of JEFIS is under the control of the clerks. This function provides a human checkpoint between information filed by the attorneys and updating of ACMS and the document management system.

## Future Plans

At the time of NCSC’s site visit, the court had approximately 2,000 electronic case files. About 15 percent of these filings originated electronically, with the remaining 85 percent coming from scanned paper documents. The immediate major goals are to increase the number of documents filed electronically from the current law firm participants and to extend the JEDDI system to additional firms. Project leaders hope to see the percentage of electronic filings increase from the current 15 percent to about 50 percent of the caseload. As one way to boost the percentage, the court is trying to convince the attorneys to use electronic filing also to file affidavits of proof in defaults, which include attached exhibits. Filing these electronically would involve scanning the originals and submitting them to the court as an image (TIF) file. Because most firms are not used to scanning documents, this process would require some adaptation of their current operations.

The top twenty firms in Monmouth County represent about 50 percent of the caseload for these special civil cases. By adding the rest of these firms as project participants, the goal for growth should be attainable. The current plan is to add the next six firms one at a time, then the remaining firms all at once. Because there is much overlap statewide, with many of these law firms filing in multiple jurisdictions, the top twenty firms in Monmouth County will represent a significant portion of the entire state caseload. For example, the top five law firms in Monmouth County currently represent about 17 percent of the statewide caseload for retail debt collection cases.

Other major goals include developing a Web-based version of JEFIS to supplement or replace the current version, expanding the pilot to other types of cases, and eventually implementing the system statewide.

## Primary Lessons Learned

The AOC and local court staffs have learned many lessons through the experience of planning, developing, and implementing New Jersey’s JEDDI pilot project. They offer several suggestions that may be of interest to other states or local courts planning a JEDDI project:

- ✓ Work to secure the support and participation of all involved parties early in the planning process and to maintain that support throughout the project. Achieving this requires respecting their viewpoints, communicating information clearly and fully, and understanding the operational environment and requirements of their organizations.

- ✓ Be diligent in managing expectations for the project. Explain that JEDDI technology is an evolving tool and a new approach—not a turnkey solution.
- ✓ Make certain that participating law firms have the proper technology installed and have received adequate training on its use before the pilot system goes into operation.
- ✓ When analyzing requirements and designing a statewide JEDDI system, work to keep a universal perspective. Avoid the trap of reflecting in the design local nuances that exist in the pilot court community, or introducing them through corrections or refinements made following initial pilot court implementation.



## CHAPTER EIGHT

### *Utah's JEDDI Project*

#### Project Background and Key Issues

The Utah judiciary has been pursuing electronic document and data interchange for a number of years. The main effort began in 1992 as a result of a visioning initiative conducted by the Utah Judicial Council. Among the statements describing the ideal future characteristics of the judiciary was a desire to be able to file court documents from anywhere at any time. The technology staff in the administrative office of the courts began to explore methods to achieve this goal.

#### Characteristics of Utah's JEDDI Project

- Criminal case pilot project
- "Ecosystem" approach
- High-level strategy body
- Intelligent electronic documents
- XML tagging
- Digital signatures
- Moving to Web interface

#### *The Internet*

The staff determined that the Internet was the logical telecommunications structure to support the concept of filing regardless of the location of the sender. Recognizing the tremendous potential of the Internet, the AOC became the first agency in Utah to establish a direct Internet connection. In 1992, however, the World Wide Web had yet to break into practical and widespread use. Internet based e-mail, on the other hand, was relatively well established. The staff began exploring how best to use e-mail to transmit electronic filings. They considered a relatively straightforward method relying on transmission of document files prepared with standard word processing packages, such as Microsoft Word and WordPerfect, but they also investigated the advantages and disadvantages of other document formats and technologies, such as Adobe Portable Document Format (PDF).

#### *SGML*

Among the other potential solutions, the AOC's technology staff began to look into Standardized General Markup Language (SGML) as a means to provide a standardized data format for transmitting electronic documents. The Department of Defense had announced plans to use SGML for its electronic interchange activities, and many of the advantages that SGML seemed to offer were applicable to the court system, as well. For example, it was an open, nonproprietary standard and would allow the judiciary to sidestep the problem of different word processing software being used by different organizations and individuals. After further analysis, the staff decided to base their initial exploratory development of a JEDDI system upon SGML.

### ***Case Type for Pilot***

Another issue that had to be decided before the AOC could initiate a JEDDI pilot project was whether to begin with a civil or criminal case filing system. A primary advantage of beginning with a criminal pilot project was that there was no filing fee involved. How to handle a filing fee over the Internet was a major consideration at that time in the evolution of Internet commerce. The downside of beginning with criminal cases, of course, was that criminal systems involve many different entities and large amounts of data. Based on their assessment of this issue, the planners decided to begin the analysis and design of a JEDDI system for criminal cases. The district attorney for the judicial district that encompasses Salt Lake City was more than willing to participate in a pilot project. This progressive attitude and spirit of cooperation added political impetus to the project, and the proximity of the two offices made it very efficient for the AOC staff and the DA's staff to work together to design, develop, and test the system.

### ***Digital Signatures***

As the planning continued, another significant issue was the need to provide some type of electronic signature to authenticate the electronic documents being filed. The staff investigated public key encryption as a potential solution to this problem. They realized that it would require the passing of new legislation to make effective use of digital signatures. A court rule alone would not be adequate authorization for its use, particularly in a widespread criminal justice setting. The lead conceptual architect for the JEDDI project orchestrated a co-operative effort involving the judiciary, the executive branch, and the legislature. In addition, the banking industry and other interested entities lobbied the legislators to help them understand the need for and advantages of a digital signature law. When the Utah Legislature passed the Digital Signature Act in 1995, it was the first such law in the nation. Much of the initial effort to develop a digital signature structure was centered in the Utah Department of Commerce, and the AOC loaned the department its conceptual architect to help with this effort.

### ***Broad Vision of Electronic Ecosystem***

Almost from the outset, Utah's vision of a JEDDI system encompassed more than the narrow concept of an electronic filing system developed by the judiciary to permit the prosecutor to send documents to the clerk's office. The vision emerged of an electronic "ecosystem" involving all participants in the justice system and extending to every aspect of capturing, processing, and exchanging case-related information. The decision to tackle the issue of digital signatures head-on was both a result of this vision and a cause for even broader involvement of entities outside the court.

An organization called the Utah Electronic Law and Commerce Partnership (UELCP) was established to provide high-level strategic planning for an initiative to streamline government and legal systems and improve public access to information and services. A major

goal of the UELCP is to promote electronic practice of law and electronic commerce. The UELCP consists of representatives from the executive and judicial branches, private-sector representatives from large and small companies and commercial associations, members of the state bar association and law firms, and participants from other interested organizations. Thus, the judiciary's project is a key component of this even larger vision for the state.

Having the UELCP serve as a high-level steering body for the JEDDI project has had many advantages. In addition to providing a much broader base of support for the project, it establishes a broader context within which policies, procedures, and technical solutions can be developed for the JEDDI system. The UELCP also serves as the forum for strong involvement of the bar association. In addition to formal meetings, several of the interested members meet weekly in an informal setting to discuss the issues surrounding the project. Besides the UELCP, key high-level participants include the state court administrator, a state legislator, a state bar commissioner, the state chief information officer, the district attorney, and the county criminal justice advisory committee.

Despite Utah's early involvement with JEDDI concepts and its groundbreaking use of promising technological approaches, the broad, ecosystem approach has governed the speed with which the JEDDI system could be developed from its conceptual origins. It has required substantial time and effort to develop the political, procedural, and technical infrastructure needed to support the system architecture. Now, however, that investment is beginning to pay off. Much of the approach and many of the components developed for the JEDDI system can be applied to future government e-commerce projects, such as voter registration and filing of deeds in the recorder's office.

### *Personnel Setbacks and Solutions*

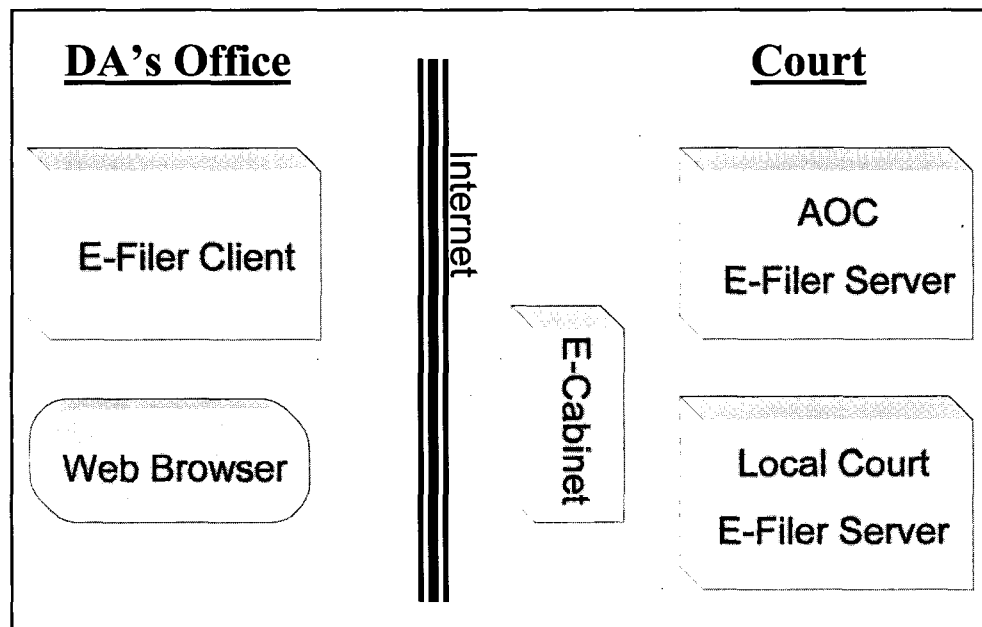
The project also has suffered from personnel-related setbacks that are all too common in court technology projects. Perhaps the most devastating blow was the resignation in 1996 of the staff member who had been the conceptual architect and driving force behind the project. Because of the high demands on the rest of the AOC's technology staff, there had been relatively little direct involvement of anyone else from that staff in the JEDDI project. For that reason, most of the resident knowledge about it was lost with the individual. The second setback came when the district attorney who had been involved in the pilot project and was a strong proponent of the technology left office. These two events slowed the project drastically while the players regrouped.

Recognizing that it would require outside expertise and staff resources to supplement its own technology staff, the AOC issued an RFP for the needed services. The bid was won by iLumin Corporation, a small technology company specializing in electronic commerce solutions. ILumin began working with the AOC technology staff newly assigned to the JEDDI project to develop a working system. ILumin concentrated primarily on the user interfaces and document-formatting technology, while the AOC staff focused on how to handle the back end of the filing process and the integration of the electronic documents with the Court Records Information System (CORIS), Utah's statewide case management system. With the emergence of XML as a

viable document format and data-tagging scheme, the team channeled the preliminary work that had been done with SGML into this even more practical approach. Later, as the criminal pilot project implementation progressed, the former district attorney regained office in Salt Lake County, adding to the momentum. The criminal JEDDI system became operational in the Third District Court in February 1999. The first type of document being filed through the new system was the initial filing for a fugitive-from-justice case.

## System Design and Operation

Utah's JEDDI system architecture can be divided into two major sets of components: the user interface and front-end components, called *E-Filer Client*, and the back-end components, consisting primarily of *E-Filer Servers* and an *E-Cabinet*. The Internet is the bridge between the two sets of components. Because the current E-Filer Client is not browser based, the client side of the picture also contains a standard Web browser to permit retrieval of case information over the Internet. The primary function of the E-Filer Client software is to generate an XML document from the filing information entered by the user. The AOC E-Filer Server processes all electronic documents filed through the system. The local court E-Filer Server handles the interface between the filed document and the case management database. The E-Cabinet is a directory on a Web server at the state level that stores all electronic documents and makes them available for subsequent inquiries. The figure below depicts the basic components of the system architecture.



### *E-Filer Client*

The first-generation E-Filer Client is based on a Windows Wizard approach. The application makes it very easy for the user in the DA's office to create an XML filing document through a

series of steps. The system uses both fill-in-the-blanks data entry and mouse selection from choices in drop-down boxes. In addition, the E-Filer Client pulls available information (e.g., defendant name, address, and law enforcement identification) from the DA's database and inserts it into the appropriate places in the document. This automated interface sharply reduces redundant data entry and errors of inconsistency. (ILumin also is developing a Wizard-based utility application to allow a user to process an existing free-text document to set it up as an XML document.)

After all information has been entered and initial validations performed, the E-Filer Client generates an XML document, tagging the data elements according to the DTD standards developed by the AOC for the type of document being filed. The document is displayed in a window as a formatted text document that looks essentially the same as if it had been created on a word processor. The filing attorney can review the document, sign it digitally (currently through PGP digital signature technology), and direct the system to file it in the court. The E-Filer client then interfaces with the standard e-mail package used by the DA's office and sends the encrypted electronic document to the designated e-mail address at the AOC (all filings throughout the state will be sent to a single location and automatically distributed to the appropriate court). If the e-mail server or the Internet is down, the document can be saved for later transmission.

### *Court Components and Processes*

On the court (AOC and local court) side of the architecture, the JEDDI system comes into play when triggered by the arrival of an e-mail message that was sent from the DA's office by the E-Filer Client. The AOC's main gateway e-mail server passes the message to the E-Filer Server, which initiates a series of steps to process the document, send an acknowledgment to the filing party, and send the case information on to the case management system. These steps are described below. They involve a series of special files that are created at different stages of the process as the encrypted e-mail message containing the XML document is decoded and interpreted and the information it contains is routed to the appropriate places in the system. A log file also is created to record the activity and outcome at each step. Log files are used internally only and provide an audit trail and a diagnostic tool in case of problems.

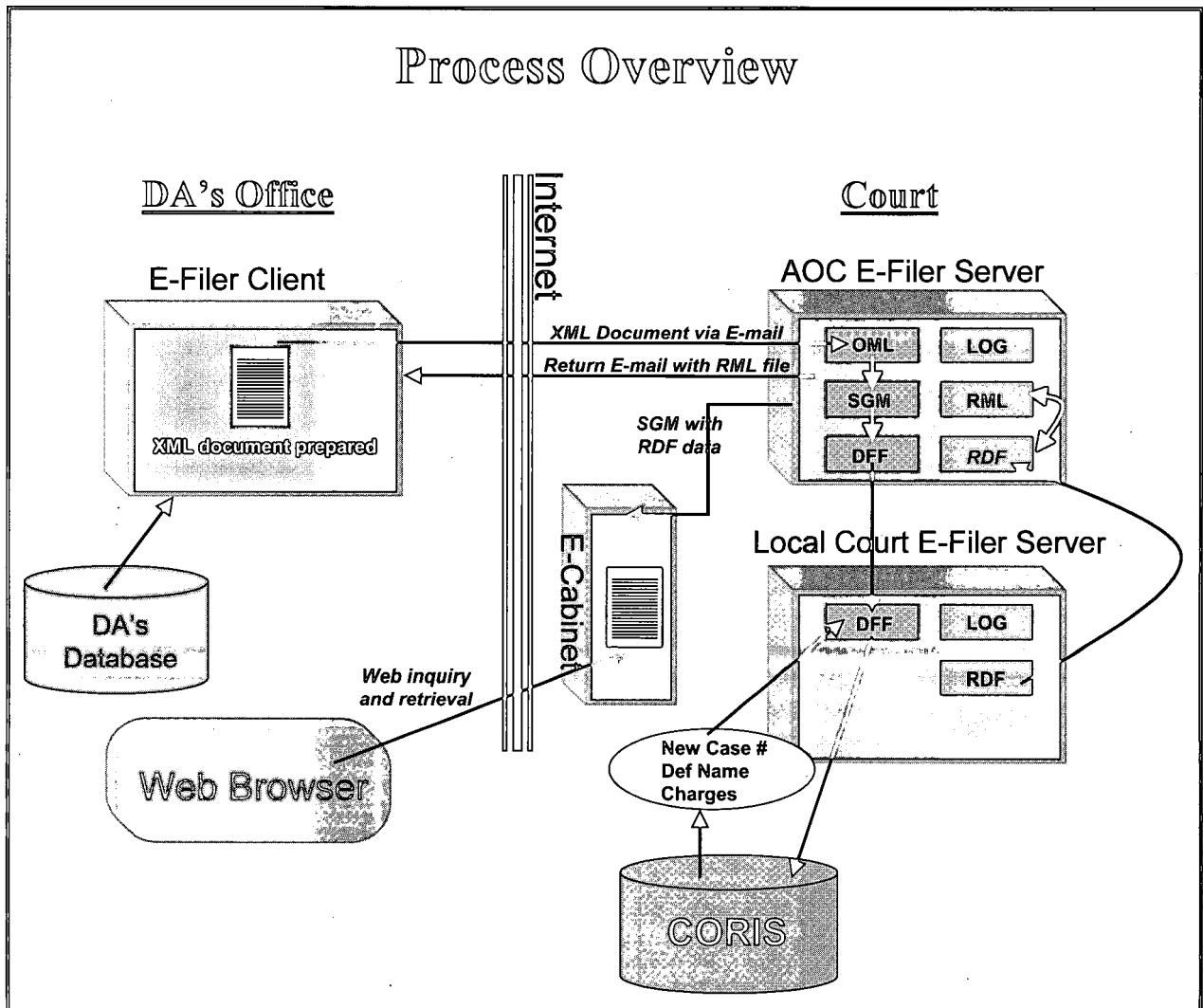
#### **Processing Steps for Filing**

1. The AOC E-Filer Server creates a document ID for the new filing, consisting of a serial number based on the date and the next sequential number for the filings received on that date (e.g., 990617.15 for the fifteenth filing received on June 6, 1999). The document ID will be used as the file name for the series of special files created during processing of the filed document. The first such file is initialized at this point, although it will continue to be built throughout subsequent steps. This file is called the Return Mail File and has the corresponding designated file extension RML. The complete name for the file created from the above example of a document ID would be 990617.15.RML. At this step an acknowledgment of the date received would be written to the RML file.

2. The AOC E-Filer Server saves the entire e-mail message into a file named with the serial number and the extension OML (for Original Mail). The OML file preserves the message exactly as it was received, including the PGP encryption below the e-mail header information.
3. The AOC E-Filer Server validates the digital signature, decrypting the signed message, and then it creates a file with the extension SGM (a holdover from the original use of SGML for tagging) containing the XML document (which is now just an ASCII text file with XML tags to identify the data elements). If the coding is improper or the digital signature is not valid, an error message is generated and written to both the RML file and the log file.
4. An XML parser software application extracts all the information content based on the DTD for this type of document, identified as UCDBCR (Utah Court Document Beginning a Criminal Case) by the start tag "<UCDBCR>" that was inserted by the E-Filer Client in the DA's office. The E-Filer Server then creates a flat data file with the extension DFF that contains the extracted data in a prescribed record layout.
5. If processing terminates at this point because of errors or system problems, the RML file is e-mailed back to the filing party and to the technical system administrator to alert both to the problem. Otherwise, the RML continues to be built and is held for transmission until after all steps have been completed.
6. The AOC E-Filer Server sends the DFF file to the E-Filer Server for the appropriate local court, based on the court identification tag embedded in the XML document (currently, there is a local court E-Filer Server for only the Third District Court in addition to a test court server). The file is sent over the Internet using File Transport Protocol (FTP).
7. The local court E-Filer Server opens the flat file and initiates a case-filing event in the CORIS database, going through all the tables and inserting the appropriate data fields from the flat file. It also creates an entry for the local log file. CORIS generates a case number for the new court case and assigns a judge to it.
8. The local court E-Filer Server generates a Return Data File with the extension RDF. This is in essence an abbreviated log file containing only basic information, including the assigned case number, date filed, and judge. Alternatively, if there is a failure in the processing of the DFF file or creation of the CORIS record, the local E-Filer Server generates an error message, writes it to the RDF file and the log file, and sends an e-mail to the system administrator. Either way, the RDF file is sent to the AOC E-Filer Server via Internet FTP.
9. The AOC E-Filer Server appends the information in the RDF file to the RML file that it has been constructing throughout this process. It then e-mails the RML file to the filing party. The RML file serves as both an acknowledgment and a means to convey to the filing party the case-filing information generated by CORIS (the case number, assigned judge, etc.).

10. The AOC E-Filer Server reads the SGM file (created in step 3) containing the XML document that was filed, inserts the new case number and date filed, and stores the resulting file in the E-Cabinet with a TXT extension, where it is available for public retrieval. The unmodified SGM file remains in the E-Filer Server (although future system revisions may not retain this file, because it can easily be re-created from the OML file).

The figure below is a diagram summarizing the process described in these steps. Examples of the specialized files used or created throughout these steps are shown on the pages that follow.



### Example of OML File

From [Cearl@da-mail.co.slc.ut.us](mailto:Cearl@da-mail.co.slc.ut.us) Mon Jun 14 13:27:43 1999  
 Received: from [198.50.1.4] ([198.50.1.4]) by courtlink.utcourts.gov (AIX4.2/UCB 8.7/8.7) with SMTP id NAA97926 for <[efiler@courtlink.utcourts.gov](mailto:efiler@courtlink.utcourts.gov)>; Mon, 14 Jun 1999 13:27:41 -0600 (MDT)  
 Received: from da-mail.co.slc.ut.us by [198.50.1.4]  
 via smtpd (for courtlink.utcourts.gov [192.120.193.2]) with SMTP; 14 Jun 1999 19:27:43 UT  
 Received: from CS-DOM-Message\_Server by co.slc.ut.us  
 with Novell\_GroupWise; Mon, 14 Jun 1999 13:26:37 -0600  
 Message-Id: <s765030d.027@co.slc.ut.us>  
 X-Mailer: Novell GroupWise 5.5  
 Date: Mon, 14 Jun 1999 13:26:07 -0600  
 From: "Carol Earl" <[Cearl@da-mail.co.slc.ut.us](mailto:Cearl@da-mail.co.slc.ut.us)>  
 To: <[efiler@courtlink.utcourts.gov](mailto:efiler@courtlink.utcourts.gov)>  
 Subject: Filing of Information Fugitive at 06/14/1999 1:25:57 PM  
 Mime-Version: 1.0  
 Content-Type: text/plain; charset=US-ASCII  
 Content-Transfer-Encoding: quoted-printable  
 Content-Disposition: inline

-----BEGIN PGP MESSAGE-----

Version: 2.6.2

```

hEwDxqyMgXe00REBAf40FNSdqmoqaHOYHHdFahHR2ApykH9W+dEFs1XK+0iNyBn0
6DwSkKxH6lteLkKwE9RZM2IJcdfIPmdt2ePb3iespgAAB8RIJwHSMmjB+HIAgxSO
2wsbKJleJQgpWBq+30coZU9A/yUpIkA/H7kmGzwlgBxaP/8Ptys/qh43zbHXw9R/
uuVc0cpafyULbZzJ/yNOFDS1EoVGg/HyyJ2NkRMQTAdZ7wobR7QrLNaabJ8PmoT2
f1O9Ksqab4ZN/sn1Eh1LeAwQi8nCyPR5MJHwbJNTI1jOQYgxx+TOCrdNUM9/Gap3
wkvzmwOyGZRs4hOuKWISrb0MjltmbGxB0wThKOjYCVt1HTkQ2bsrS4314MaG6SeQ
+MnuYJsvXN8ujaMplO6N2Mv9RiStqEbdZoaLYfs5svik9KGUywxgiSlSvGbcu8+J
ln/+ujlKJHuTQ+jrY3Dr+Xa/Nqlwwwy6Hyx3Yn2W5gQ0gshE5/fNqLGEj/jF5aDM
n3ZLWTiocIDXJHq5UdBykg47TtviUW5eZaCuam3Xa3oP8wMHWxOVz7ZKGEge6W3J
SVMnAviV8Wr2jslkO06nWYnndeLD+EF2pUGwY+YbV7h9foBUiwnCQJt4b1NI3HxM
6lveDIA+WuwvRr5Dg24z24Zo5Hu3xJmusvoiwCu+600dloedXnTui+kz5EAGQEEp
Vozw/n7g/Gm1WinKJ2Q8y6aQYAru8TExBfWBYuUNbmoNph1balMyDv1Ufa2DhF/D
4rr0s5Did7Wwg7fU+oiWFVPV2bs/D9HqPWAOC8Mq87y+LJsr6D3xgi2JXwX9O5KR
70QbEDN6UVPfoVkJmgtndBjqYtBeM3sisrj7O4TXT9Rtl6ttK3rhe4x8rtvRFSKwz
8VQ8rhXYhJD1Y1UP1Gy8O1aqZ0NGQa17kCpjQcSmhq4yZSFhi1c4yniyKYRxAwEL
KTcWVgc3ZgvFXtm8XlKCVXEPFLQumJ7XMYftgqss/P6O5Vmz1iz3MoCEvPy2XyRL
d5HLk+zE9gZjmlMzPW4ZZ3ZzdQ5TtXXpxVvYnTWloqa3Ums7nW5WRQ/Q3q9fvu6s
AmvshO8hX8/QFQ2Lnd8VXYLpakaDIAx6wrnyLGDkIMvKJx4BNgXm65Lrvk2g2lvG
vAw5wnfbTTLjKtZKLmqNRh15DR4Xp2hwcAzSmMWEi+9qsQwx+WF7qwO1PcUAAHjp
x8+rqDFGubR/tPldnYLv1ctMI5dwSNbi3nJ25JgCpPqnFfCfcJzPKZw1QdRvU6i
SF8oLupcJDorJRM6FdfMx8L9Lz41eTLqmvOo3L01feWlyxhESAWQ5YsMMfzP4Oun
ZotM6ny9ZBIcuHMirKkdhi8KhoyY7ZpkoYBI9S0vMdnrTpRyrUF72in841BilrOm
AsMlw3XnyL1pky3UtVDai74QEZqgLhwB44fkLWBRzWPDrf2O5j9sqaKa8Vjqy5sT
l18xBeO1AOR56kC5Hb3ePPgB/B7H0Pfgq9B4rieEPIsC7GgoU4Chcl72EgCX4Nnn
trrKgnngn8r/mVa4x9MF1760iXnuhsa0bgzEPKHekIDislaYgVh7+HV/3ulKfrpjj
SDK6yCZA/AMyDq0WQ8lImmvmyryMZqYB0JqA/XXfsLEEA4rUhmhNWEkr1wB/s1s2
qnxqTJIOE2OPVdVp5nLpE4AtsBMFs+pY+8Ms04xzDpLmFGMPjxTvTG6newoyaJ
nvTf7GllnyU10TcNiNA0kcCaZEEXnAht4p/UpuNS+3yJ4Q+jbOpVvmqpn7LaGg7
0zxp39ShNvf4DLTF90bY54RC/5wiVdP0cyoQvRKnp6v2wEwjjsUSNkk1CbLjvMh4
ZsQvVmnJtDZGvZgmJPdIfmuWKEz9tXg+u+8S4uPdjm/UCTWLon/BMkVjt4waJWt
M5rkeCQRkboWuBfX339ejfnc89bw030Xvulkt762TQ0oQmduvcTtaMmJlulLTOJV
DfMHG0hfoKcO0v+t7MHKW5i9B5gZo1WwS+u3HrMJjfwNBbKpkxluBFokAAC2qcx
  
```



jxoLH/7X233QZvW/XFoJM5xz7n9th7DymipOZMZ9qBrRs5DstEeltsAg+Id2AsN5  
SGP42qA2DH6L8j/iSKWtqpXXT/4FsqQkowjwEKTW1vPGBTSK10hyg+gAM7a4J5Fc  
NvY6hkIMs4I7qcZwURyjJ4OeFJGsaevzm92FTXzSEXcbupCyJUnSPVmVFKASuGOW  
FquUmg5Tot0Oocs7+THVwcVBj3LaxGXVPQ2aauxmvs+WXdl6v298qgbeKWWewRq4  
air9gLDNJ7RWHg3/hjK1uH9M4QeT9PnxP4ParRxBuu/18HR0Pzm49pmvWGZ8fY9H  
vRtO8glMvWFKG/hwQ5ulnfoBvSVX7IMe8u9F1dvklz6a9jxrzJdfhVHXZ+aJnjt  
p7S5dPF4pLiCfxuMl6jUr6aBS3seDTyHywiBUjbL16EGl9zZvUKWur2060OwbiY8  
T6hoUDYDuSbrFGE4sJxE0hMxGZqABij+PHcx3JKFC54VPKCIF9A9Na0fRaJUPvvU  
cG0S65br1YmWSQnzOa/941vyx0CfcXU0e/vmoa5rB/B8skWkuT3xQgcKgy1Sucpm  
m1U:kIYkWPQI+hGOz//OugjvfBeoilLv+QjooP1NCEE6odv+fXIWIDjB/uAyrEKs  
LGDzquiJwQ=3D=3D  
=3Duz6h  
-----END PGP MESSAGE-----

### Example of SGM File

<UCDBCR>  
 <TBSigned SigID="FILER">  
 DAVID E. YOCOM  
 District Attorney for Salt Lake County  
 <PersInfo Role=Filer PID=SHEPHERD1><Given>RICHARD S</Given> <Last>SHEPHERD </Last>,  
 <BarNum>2939</BarNum>  
 Deputy District Attorney  
 231 East 400 South, Suite 300  
 Salt Lake City, Utah 84111  
 Telephone: (801) 363-7900  
 E-Mail: <Email>rshepherd@da-mail.co.slc.ut.us</Email></PersInfo>  
 <Caption>  
 IN THE <CtName>THIRD DISTRICT COURT, SALT LAKE DEPARTMENT IN AND FOR SALT LAKE  
 COUNTY, STATE OF UTAH</CtName>  
  
 THE <PersInfo Role=Plaintiff PID=Utah><BusGov>STATE OF UTAH</PersInfo>,  
  
     Plaintiff,  
  
     v.  
  
 <PersInfo Role=Defendant PID=ESPINOSA2><Given>RICHARD JOSEPH</Given> <Last>ESPINOSA  
 </Last>,  
     AKA: <AKA><Last>Espinosa</Last> <Given>Matt </Given></AKA>  
         DOB: <DOB>8/27/77</DOB>  
     OTN: <OTN>10652329</OTN>  
     Defendant</PersInfo>  
  
 BAIL:       \$100,000.00  
  
 </Caption>  
  
 <Title>Information</Title>  
  
 <para>The undersigned MICHAEL V WELCH - SLP, under oath, states on information and belief that  
 the defendant committed the crimes of:  
  
 <Offense><OffDesc>BEING A FUGITIVE FROM JUSTICE</OffDesc>, in <VioLoc>Salt Lake  
 County</VioLoc> on or about <VioDate>June 13, 1999</VioDate>, in violation of <OffAuth>Title 77,  
 Chapter 30, Section 13, Utah Code Annotated 1953, as amended</OffAuth><OffLabel>77-30-  
 13</OffLabel>, in that the defendant, RICHARD JOSEPH ESPINOSA , was then and there a fugitive  
 from justice from the State of Kansas, the defendant having been duly charged in the City of Topeka,  
 County of Shawnee, State of Kansas, with the crime of Parole Violation, on or about February 18,  
 1999, the same having been filed in a Court having proper jurisdiction, and a warrant having been  
 duly issued for the arrest of said RICHARD JOSEPH ESPINOSA having fled from the State of  
 Kansas after the commission of the offense charged to the Salt Lake County, State of Utah.  
  
 <Heading1>THIS INFORMATION IS BASED ON EVIDENCE OBTAINED FROM THE FOLLOWING  
 WITNESSES:</>  
  
 DUSTI MARSHALL and MICHAEL V. WELCH  
 <Heading1>PROBABLE CAUSE STATEMENT:</>  
 <para>Affiant received a communication from Kansas Dept. Of Corrections of Shawnee County,  
 State of Kansas, stating that Kansas Dept. Of Corrections holds a warrant for the arrest of RICHARD

JOSEPH ESPINOSA for Parole Violation and produced a description of said RICHARD JOSEPH ESPINOSA . RICHARD JOSEPH ESPINOSA who fit that description was located in Salt Lake County, Utah on June 13, 1999, by DUSTI MARSHALL , SLP.</para>

<para>MICHAEL V WELCH - SLP – 99116733</para>

<DataTab>

<Bold><Undln>Data Table for Initial Criminal Filing</Undln></Bold>

<Undln>Case-Specific Information</Undln>:

Prosecuting governmental entity : <ProsGov>SALT LAKE COUNTY</ProsGov>  
 Prior related cases : None  
 S.L. County Attorney's case number : <PIRef>99011676</PIRef>  
 Law Enforcement Agency : <LEA>SLP</LEA>  
 Law Enforcement Agency's Number : <LEARef>99116733</LEARef>  
 Arresting Officer : <PersInfo Role=officer PID=MARSHALL3>  
 <Given>DUSTI </Given> <Last>MARSHALL </Last>  
 Officer's Badge No. : <Badge>K19</Badge></PersInfo>

<Undln>Defendant Tracking Information</undln>:

<PIRef PID=ESPINOSA2>  
 Sheriff's Office Number :237556  
 Arrest Date : <ArrDate>6/13/99</ArrDate>  
 Jail Booking Number : <BkNum>9914506</BkNum>  
 Defendant's Sex : <Sex>M</Sex>  
 Defendant's Race : <Race>Hispanic</Race>  
 Defendant's Social Security Number : <SSN>511-80-1691</SSN>  
 Defendant's Driver's License Number : <DrvNum></DrvNum>  
 State Issuing Defendant's Driver's Lic. : <DrvSt></DrvSt>  
 Defendant's Address : <Address>3360 South Weschris  
 Road</Address>  
 Defendant's City, State : <City>West Valley City</City>,  
 <State>UT</State>

</PIRef>

</DataTab>

</TBSigned>

<Sig PID=SHEPHERD1 sigID="FILER"></Sig>

</UCDBCR>

**Example of DFF File**

CTEMAIL|efiladm@alexk||  
CTTYPE|D||  
CTLOCN|1868||  
TITLE|INFORMATION||  
GOVCODE|C18||  
PLREF|99011676||  
LEA|SLP||  
LEAREF|99116733||  
LAST|ESPINOSA|100|  
GIVEN|MATT |100|  
AKA||100|  
ROLE|FILER|1|  
PID|SHEPHERD1|1|  
GIVEN|RICHARD S|1|  
LAST|SHEPHERD |1|  
BARNUM|2939|1|  
EMAIL|rshepherd@da-mail.co.slc.ut.us|1|  
ROLE|PLAINTIFF|2|  
PID|UTAH|2|  
BUSGOV|STATE OF UTAH|2|  
ROLE|DEFENDANT|3|  
PID|ESPINOSA2|3|  
GIVEN|RICHARD JOSEPH|3|  
LAST|ESPINOSA |3|  
DOB|8/27/77|3|  
OTN|10652329|3|  
OFFENSE|3|1|  
OFFDESC|BEING A FUGITIVE FROM JUSTICE|1|  
VIOLOC|Salt Lake County|1|  
VIODATE|1999-06-13|1|  
OFFAUTH|Title 77, Chapter 30, Section 13, Utah Code Annotated 1953, as amended|1|  
OFFAUTHCODE|UT|1|  
OFFLABEL|77-30-13|1|  
ARRDATE|6/13/99|3|  
BKNUM|9914506|3|  
SEX|M|3|  
RACE|Hispanic|3|  
SSN|511-80-1691|3|  
DRIVNUM|||3|  
DRIVST|||3|  
ADDRESS|3360 SOUTH WESCHRIS ROAD|3|  
CITY|WEST VALLEY CITY|3|  
STATE|UT|3|  
ROLE|OFFICER|4|  
PID|MARSHALL3|4|  
GIVEN|DUSTI |4|  
LAST|MARSHALL |4|  
BADGE|K19|4|

**Example of RDF File****CHARGE|1****Submitted offense: BEING A FUGITIVE FROM JUSTICE****Filed offense: FUGITIVE FROM JUSTICE FROM ANOTHER STATE****<Judge>WILKINSON,HOMER</Judge>****<Comm></Comm>****<SN>990614.1</SN>****<CtCode>D1868</CtCode>****<CaseNum>991911982</CaseNum>****<IntCaseNum>1574848</IntCaseNum>****<Def>ESPINOSA, RICHARD JOSEPH</Def>****<Pla>State Of Utah</Pla>****Example of RML File****Filing [Filing of Information Fugitive at 06/14/1999 1:25:57 PM](990614.1) produced:CHARGE|1****Submitted offense: BEING A FUGITIVE FROM JUSTICE****Filed offense: FUGITIVE FROM JUSTICE FROM ANOTHER STATE****<Judge>WILKINSON,HOMER</Judge>****<Comm></Comm>****<SN>990614.1</SN>****<CtCode>D1868</CtCode>****<CaseNum>991911982</CaseNum>****<IntCaseNum>1574848</IntCaseNum>****<Def>ESPINOSA, RICHARD JOSEPH</Def>****<Pla>State Of Utah</Pla>****<FileDate>06-14-99</FileDate>****<FileTime>13:27:43</FileTime>**

-----  
Please e-mail alexk@email.utcourts.gov or phone 578-3874 for more information

### Example of TXT File Stored in E-Cabinet

From CEarl@da-mail.co.slc.ut.us Mon Jun 14 13:27:43 1999  
 Received: from [198.50.1.4] ([198.50.1.4]) by courtlink.utcourts.gov (AIX4.2/UCB 8.7/8.7) with SMTP id NAA97926 for <efiler@courtlink.utcourts.gov>; Mon, 14 Jun 1999 13:27:41 -0600 (MDT)  
 Received: from da-mail.co.slc.ut.us by [198.50.1.4] via smtpd (for courtlink.utcourts.gov [192.120.193.2]) with SMTP; 14 Jun 1999 19:27:43 UT  
 Received: from CS-DOM-Message\_Server by co.slc.ut.us with Novell\_GroupWise; Mon, 14 Jun 1999 13:26:37 -0600  
 Message-Id: <s765030d.027@co.slc.ut.us>  
 X-Mailer: Novell GroupWise 5.5  
 Date: Mon, 14 Jun 1999 13:26:07 -0600  
 From: "Carol Earl" <CEarl@da-mail.co.slc.ut.us>  
 To: <efiler@courtlink.utcourts.gov>  
 Subject: Filing of Information Fugitive at 06/14/1999 1:25:57 PM  
 Mime-Version: 1.0  
 Content-Type: text/plain; charset=US-ASCII  
 Content-Transfer-Encoding: quoted-printable  
 Content-Disposition: inline

=====

<UCDBCR>  
 <TBSigned SigID="FILER">  
 DAVID E. YOCOM  
 District Attorney for Salt Lake County  
 <PersInfo Role=Filer PID=SHEPHERD1><Given>RICHARD S</Given> <Last>SHEPHERD </Last>,  
 <BarNum>2939</BarNum>  
 Deputy District Attorney  
 231 East 400 South, Suite 300  
 Salt Lake City, Utah 84111  
 Telephone: (801) 363-7900  
 E-Mail: <Email>rshepherd@da-mail.co.slc.ut.us</Email></PersInfo>  
 <Caption>  
 IN THE <CtName>THIRD DISTRICT COURT, SALT LAKE DEPARTMENT IN AND FOR SALT LAKE COUNTY, STATE OF UTAH</CtName>  
  
 THE <PersInfo Role=Plaintiff PID=Utah><BusGov>STATE OF UTAH</PersInfo>,  
  
 Plaintiff,  
  
 v.  
  
 <PersInfo Role=Defendant PID=ESPINOSA2><Given>RICHARD JOSEPH</Given> <Last>ESPINOSA </Last>,  
 AKA: <AKA><Last>Espinosa</Last> <Given>Matt </Given></AKA>  
 DOB: <DOB>8/27/77</DOB>  
 OTN: <OTN>10652329</OTN>  
 Defendant</PersInfo>  
  
 BAIL: \$100,000.00  
  
 <CaseNum>Case number: 991911982</CaseNum>  
 <PersInfo Role=Judge pid=judg><Last>Judge: WILKINSON,HOMER</></PersInfo>  
 <CalDate>Filing date: 06/14/99</CalDate>

</Caption>

<Title>Information</Title>

<para>The undersigned MICHAEL V WELCH - SLP, under oath, states on information and belief that the defendant committed the crimes of:

<Offense><OffDesc>BEING A FUGITIVE FROM JUSTICE</OffDesc>, in <VioLoc>Salt Lake County</VioLoc> on or about <VioDate>June 13, 1999</VioDate>, in violation of <OffAuth>Title 77, Chapter 30, Section 13, Utah Code Annotated 1953, as amended</OffAuth><OffLabel>77-30-13</OffLabel>, in that the defendant, RICHARD JOSEPH ESPINOSA, was then and there a fugitive from justice from the State of Kansas, the defendant having been duly charged in the City of Topeka, County of Shawnee, State of Kansas, with the crime of Parole Violation, on or about February 18, 1999, the same having been filed in a Court having proper jurisdiction, and a warrant having been duly issued for the arrest of said RICHARD JOSEPH ESPINOSA having fled from the State of Kansas after the commission of the offense charged to the Salt Lake County, State of Utah.

<Heading1>THIS INFORMATION IS BASED ON EVIDENCE OBTAINED FROM THE FOLLOWING WITNESSES:</>

DUSTI MARSHALL and MICHAEL V. WELCH

<Heading1>PROBABLE CAUSE STATEMENT:</>

<para>Affiant received a communication from Kansas Dept. Of Corrections of Shawnee County, State of Kansas, stating that Kansas Dept. Of Corrections holds a warrant for the arrest of RICHARD JOSEPH ESPINOSA for Parole Violation and produced a description of said RICHARD JOSEPH ESPINOSA. RICHARD JOSEPH ESPINOSA who fit that description was located in Salt Lake County, Utah on June 13, 1999, by DUSTI MARSHALL, SLP.</para>

<para>MICHAEL V WELCH - SLP - 99116733</para>

<DataTab>

<Bold><UndIn>Data Table for Initial Criminal Filing</UndIn></Bold>

<UndIn>Case-Specific Information</UndIn>:

Prosecuting governmental entity : <ProsGov>SALT LAKE COUNTY</ProsGov>

Prior related cases : None

S.L. County Attorney's case number : <PIRef>99011676</PIRef>

Law Enforcement Agency : <LEA>SLP</LEA>

Law Enforcement Agency's Number : <LEARef>99116733</LEARef>

Arresting Officer : <PersInfo Role=officer PID=MARSHALL3> <Given>DUSTI </Given>

<Last>MARSHALL </Last>

Officer's Badge No. : <Badge>K19</Badge></PersInfo>

<UndIn>Defendant Tracking Information</undIn>:

<PIRef PID=ESPINOSA2>

Sheriff's Office Number :237556

Arrest Date : <ArrDate>6/13/99</ArrDate>

Jail Booking Number : <BkNum>9914506</BkNum>

Defendant's Sex : <Sex>M</Sex>

Defendant's Race : <Race>Hispanic</Race>

Defendant's Social Security Number : <SSN>511-80-1691</SSN>

Defendant's Driver's License Number : <DrivNum></DrivNum>

State Issuing Defendant's Driver's Lic. : <DrivSt></DrivSt>

Defendant's Address :<Address>3360 South Weschris Road</Address>

Defendant's City, State :<City>West Valley City</City>, <State>UT</State>

</PIRef>

</DataTab>

</TBSigned>

<Sig PID=SHEPHERD1 sigID="FILER"></Sig>

**CHARGE|1**

Submitted offense: BEING A FUGITIVE FROM JUSTICE

Filed offense: FUGITIVE FROM JUSTICE FROM ANOTHER STATE

&lt;Judge&gt;WILKINSON,HOMER&lt;/Judge&gt;

&lt;Comm&gt;&lt;/Comm&gt;

&lt;SN&gt;990614.1&lt;/SN&gt;

&lt;CtCode&gt;D1868&lt;/CtCode&gt;

&lt;CaseNum&gt;991911982&lt;/CaseNum&gt;

&lt;IntCaseNum&gt;1574848&lt;/IntCaseNum&gt;

&lt;Def&gt;ESPINOSA, RICHARD JOSEPH&lt;/Def&gt;

&lt;Pla&gt;State Of Utah&lt;/Pla&gt;

## Case Lookup and Document Retrieval

Once an electronic document has been filed successfully and stored in the AOC's E-Cabinet, it can be retrieved for viewing through the Web. From the filing party's point of view, the document is available within one or two minutes after the filer mouse-clicked the button on the E-Filer Client to send the document to the court. During that time the filer received an e-mail acknowledgment confirming the filing and providing the resultant case number (or an error message explaining why the filing was not successful). Because both the E-Cabinet and the local court E-Filer Server are Web-accessible, the filing party and the general public can look up the case through their Web browsers and display documents and other case data as well. Any of four different inquiry reports are available from CORIS: case information, party information, case schedule, and case summary.

When a user accesses the E-Cabinet through a Web browser, the system displays a table showing the serial number document IDs for the stored documents. The document IDs are shown as hypertext links. When the user clicks on a link, the system retrieves the corresponding XML document and activates an XML parser to show the document content without the tags. Because the XML document is not bound by any particular format for appearance, the court can control how it is displayed. Shown below is an illustration of how the document represented in the above examples of the specialized JEDDI system files can be displayed and printed from a Web browser.



document

file:///C:/Work/Docwrt/Utah/Files/3rdPage.htm

DAVID E. YOCOM  
District Attorney for Salt Lake County  
RICHARD S SHEPHERD , 2939  
Deputy District Attorney  
231 East 400 South, Suite 300  
Salt Lake City, Utah 84111  
Telephone: (801) 363-7900  
E-Mail: rshepherd@da-mail.co.slc.ut.us

IN THE THIRD DISTRICT COURT, SALT LAKE DEPARTMENT IN AND FOR SALT LAKE  
COUNTY, STATE OF UTAH

THE STATE OF UTAH,

Plaintiff,

v.

MATTHEW JOSEPH ESPINOSA ,  
AKA: Espinosa Matt  
DOB: 8/27/77  
OTN: 10652329  
Defendant

BAIL: \$100,000.00

Case number: 991911982  
Judge: WILKINSON,HOMER

Filing date: 06/14/99  
Filing time: 13:28 PM

Screened by: RICHARD S SHEPHERD  
Assigned to: TBAM

BAIL:  
Warrant/Release:

**Information**

The undersigned MICHAEL V WELCH - SLP, under oath, states on information and belief that the defendant committed the crimes of:

BEING A FUGITIVE FROM JUSTICE, in Salt Lake County on or about June 13, 1999, in violation of Title 77, Chapter 30, Section 13, Utah Code Annotated 1953, as amended 77-30-13, in that the defendant, MATTHEW JOSEPH ESPINOSA , was then and

document	file:///C:/Work/Docwire/Tools/Docwire/DocPage.htm
<p>there a fugitive from justice from the State of Kansas, the defendant having been duly charged in the City of Topeka, County of Shawnee, State of Kansas, with the crime of Parole Violation, on or about February 18, 1999, the same having been filed in a Court having proper jurisdiction, and a warrant having been duly issued for the arrest of said MATTHEW JOSEPH ESPINOSA having fled from the State of Kansas after the commission of the offense charged to the Salt Lake County, State of Utah.</p>	
<p><b>THIS INFORMATION IS BASED ON EVIDENCE OBTAINED FROM THE FOLLOWING WITNESSES:</b></p>	
<p>DUSTI MARSHALL and MICHAEL V. WELCH</p>	
<p><b>PROBABLE CAUSE STATEMENT:</b></p>	
<p>Affiant received a communication from Kansas Dept. Of Corrections of Shawnee County, State of Kansas, stating that Kansas Dept. Of Corrections holds a warrant for the arrest of MATTHEW JOSEPH ESPINOSA for Parole Violation and produced a description of said MATTHEW JOSEPH ESPINOSA . MATTHEW JOSEPH ESPINOSA who fit that description was located in Salt Lake County, Utah on June 13, 1999, by DUSTI MARSHALL , SLP.</p>	
<p>s/MICHAEL V WELCH - SLP - 99116733</p>	
<p><b>Data Table for Initial Criminal Filing</b></p>	
<p><u>Case-Specific Information:</u></p>	
<p>Prosecuting governmental entity : SALT LAKE COUNTY</p>	
<p>Prior related cases : None</p>	
<p>S.L. County Attorney's case number : 99011676</p>	
<p>Law Enforcement Agency : SLP</p>	
<p>Law Enforcement Agency's Number : 99116733</p>	
<p>Arresting Officer : DUSTI MARSHALL</p>	
<p>Officer's Badge No. : K19</p>	
<p><u>Defendant Tracking Information:</u></p>	
<p>Sheriff's Office Number :237556</p>	
<p>Arrest Date : 6/13/99</p>	
<p>Jail Booking Number : 9914506</p>	
<p>Defendant's Sex : M</p>	
<p>Defendant's Race : Hispanic</p>	
<p>Defendant's Social Security Number :</p>	
<p>Defendant's Driver's License Number :</p>	
<p>State Issuing Defendant's Driver's Lic. :</p>	
<p>Defendant's Address :3360 South Weschris Road</p>	
<p>Defendant's City, State :West Valley City, UT</p>	
2 of 3	12/8/99 9:33 PM

### *Flexibility of the Court Side of the Architecture*

From the court's perspective, it is irrelevant how the XML document is created by the filing party. The AOC E-Filer Server is designed to expect an XML document based on the prescribed DTD to arrive as an ASCII text e-mail message (encrypted with a digital signature). After processing is completed, the system sends an e-mail acknowledgment back to the return e-

mail address contained in the original message. Everything else on the front end of the system is transparent to the court components. The electronic document might have been created manually in the attorney’s office, using a standard word processor or simple text editor, with the data tags inserted individually through keyboard entry. Or the user might have set up a word processing template and macro to automate the insertion of data tags. Alternatively, the document might have been created through a sophisticated software package, such as the E-Filer Client, or generated through a Web site using a specially prepared Web form. The end result is the same once the document reaches the E-Filer Server, provided it conforms to the standards.

Similarly, the court’s e-mail response (containing the RML file) would be the same, regardless of the method of origination for the electronic document filed. It would be up to the filer to decide how to process the return message. It could be handled manually (because the RML file is human-readable), or it could be interfaced with application software on the filer’s computer to permit automated processing of the information returned by the court.

This flexibility frees potential filers to seek the best technical solution for their particular office procedures and technical environment. They can use the E-Filer Client developed by iLumin, develop their own templates or software application to prepare XML documents, or use another third-party software package or electronic filing service.

## Future Plans

### *Web-based Filing*

With the successful implementation of the criminal pilot system in the Third District Court and Salt Lake County DA’s Office, the AOC is moving forward rapidly, but cautiously, with expansion of its JEDDI project. iLumin is nearly finished developing a Web browser-based E-Filer Client to replace the current system. The browser-based approach offers many advantages. It will enhance the ability of users to file documents from any location or any computer equipped for Web access, rather than being restricted to a computer on which the E-Filer Client has been installed. Another primary benefit is that it will permit interactive, real-time filing with immediate confirmation. The XML document will be uploaded to the court’s Web site and processed, and the acknowledgment that includes the case number assigned and other information generated by the court will be returned almost immediately to the user’s Web browser. The AOC plans to continue the e-mail interface after the Web-based interface is implemented. This will permit users to file through either method, for even more flexibility.

### *Expanded Scope*

The AOC and iLumin also are moving forward with extending the scope of the JEDDI system. The Web-based user interface is a strategic component of the expanded vision for the JEDDI system, which will include more participants in the process. The concept of online “signing rooms” will be an important part of the system architecture. Along with other features,

these will permit law enforcement officials, attorneys, and judges to view documents staged for their input, add whatever information is needed, and digitally sign the documents.

In this expanded phase for the criminal JEDDI system, the DA's office will have its own Web-accessible E-Filer Server. Law enforcement officers will access the Web site through their browsers, logging in to a secure Internet connection. They will fill out an online fact sheet (a Web form) for a new case, and the system will create an electronic XML document and place it in the queue for the DA's office. An attorney in that office will enter the online screening room and select the document to be screened. The law enforcement information will be viewable, but "grayed out" to prevent modification. The attorney will enter the information needed from the DA's office and submit the form. This system will display a summary sheet for the information entered and permit the attorney to correct any mistakes. Next, in the attorney's signing room, the complete document containing both the officer's and the attorney's information will be displayed as a formatted text document, which is a much more natural and comfortable format for review. After approving the final document, the attorney will sign it digitally and submit it.

The system will create the finished XML document, encrypted with the attorney's digital signature, and submit it to the court for a judge's review. The judge will see the document in his or her queue and go through a screening process to accept, reject, or modify it (modifications are restricted to certain fields, such as bail amount). The system also will permit the judge to enter free text that will be included in the information sent back to the DA's office. When satisfied with the document, the judge will digitally sign it, and the system will send it back to the DA's office.

### ***Additional Improvements and Expansion***

The JEDDI project is pushing forward on a number of other fronts. In addition to expansion of the current criminal system used by the DA's office, the Utah Attorney General's Office is eager to implement the system. The AG's staff sees several advantages for their operation: faster processing at reduced costs, the ability to file at any time of the day and more easily meet deadlines, the ability to file from anywhere (important both for their need to travel throughout the state and to support telecommuting), the capability to search and view what the opposing counsel has filed, and the potential to create a brief-bank database of XML documents. The AG's office will be able to adapt the system developed for the DA's office, with the result that they could possibly begin operation by the end of 1999.

A civil case JEDDI module is under development, as well. Because of the groundwork accomplished during development and enhancement of the criminal system, the civil system is progressing rapidly. The Web-based user interface is a pivotal part of the strategy for civil implementation, because it will give private attorneys a much more direct, interactive connection to the court for filing documents and receiving confirmation. The AOC expects to begin testing the civil system before the end of the year.

The AOC also is exploring different options for digital signature technology. The current system is using PGP as a stopgap measure, but more robust PKI technology is being planned.

The state bar association may issue digital certificates to attorneys, although how the certificate authority will be structured (e.g., to what extent a commercial CA will be used, if at all) has yet to be worked out. Utah currently licenses several commercial CAs (Digital Signature Trust Company, Arcanvs, Inc., Universal Secured Encryption Repository Company (USERFirst), and VeriSign, Inc.). The AOC believes the user should have some flexibility in the technology choices. For example, the AG’s office tentatively is planning to use a “smart floppy” device. This is essentially a smart card packaged in a floppy disk case. Under control of the digital signature software, the computer reads the smart card’s stored information through the read head in the floppy drive. The advantage of this technology is that it provides much of the convenience of a smart card without requiring additional card-reader hardware. The AG’s staff resisted the idea of any kind of smart card technology, but decided that it was far less objectionable than security based on biometrics. (See Chapter Six for a discussion of security technologies.)

The AOC is improving its general technology infrastructure that supports the JEDDI system. The current applications are written using a mixture of C with other programming languages and application development tools. The technology staff plans to convert all applications to Perl and JavaScript, which offer the advantages of high-level programming without sacrificing low-level control. Special-purpose programming subroutines written in C++ and other languages may still be used where needed. The conversion process already is well under way. Another goal is to permit local courts and other organizations (such as the DA’s office and AG’s office) to have their choice of server environments for their E-Filer Server. Although the AOC plans to continue using a Unix-based hub, NT server software will be developed for implementation where it is preferred.

Plans also call for development of an indexing scheme for the document database (the AOC currently is using Folio for document management). This feature will enable automatic indexing of the XML tags for efficient document search and retrieval capabilities.

Well down the road, but already on the conceptual drawing board, is the capability to conduct complete virtual hearings in which the parties are in different locations. The courts already videotape proceedings, and video arraignments are being conducted in some courts. The JEDDI system would extend the capabilities to include all the “paperwork” in electronic form. The virtual hearing room would connect all parties through audio and video links, and Web browsers and Internet connections at all sites would permit access to electronic file cabinets and sharing of documents among the parties. Guilty pleas and other documents in both criminal and civil hearings could be signed digitally and immediately filed and distributed.

## Primary Lessons Learned

Utah’s judiciary has experienced a long journey in planning and implementing its JEDDI project. Many changes have taken place during that time, including sweeping advances in the technology industry and turnover of key personnel. Rather than pursue an isolated and limited project, the judiciary pushed forward a broad effort involving many issues and multiple organizations. Although the speed of implementation has been slowed, the investment is beginning to pay off handsomely, not only in the working systems that are being installed, but

also in the future capabilities and benefits of the e-commerce foundation that has been created. Utah's judicial leaders are convinced that the broad, ecosystem vision was the best one to pursue.

The success of Utah's project is a result of paying attention to human and technology issues. It is critical to involve all affected parties in the planning process. High-level backing in all organizations is necessary, as is representation at the operational level. The digital signature was the galvanizing issue that brought together the legislative, executive, and judicial branches to break new ground and create a mindset for cooperative movement toward a statewide e-commerce environment. Recognizing the potential benefit of long-term technology solutions such as SGML and XML, along with PKI security technology, was fundamental to the development of a system with such widespread potential capabilities. The involvement of outside technical expertise to complement the knowledge and skills of the AOC's technology staff also was a necessary and highly productive move. While other JEDDI systems have been put into place much more quickly, Utah's approach has positioned it to provide greatly improved services to its constituents for years to come. It also has advanced the status of court technology to the benefit of all judicial systems.

## CHAPTER NINE

### *Conclusions*

Judicial Electronic Document and Data Interchange is a growing reality in the state courts, with substantial progress having been made during the last half of the 1990s. Individual trial courts and state administrative offices of the courts have undertaken a number of pilot projects. Although a few efforts did not come to fruition, several first-generation JEDDI implementations now are operating successfully. The projects range from the simplistic to the complex. Some have been conducted mainly by a handful of court employees, while others have involved many people and multiple organizations, including third-party technology vendors and service providers. Virtually all of these systems are undergoing expansion and enhancement.

The visionary courts that have implemented successful JEDDI systems have achieved the “proof of concept” needed for this new application of technology. Together, these pioneers have laid a foundation of real-world experience upon which others can build. Along with recent developments in relevant technologies, sweeping progress in addressing legal and policy issues, and growing public expectations for technology use and Internet-based commerce, this base of experience will help propel courts toward widespread adoption of JEDDI solutions.

Indeed, interest in JEDDI has risen sharply during the past three years. NCSC’s Technology Information Service is handling record numbers of requests for JEDDI-related information, especially through the TIS Web pages (access NCSC’s Web site at [www.ncsc.dni.us](http://www.ncsc.dni.us) and click on the *technology information* link). JEDDI issues frequently are discussed at local, state, and national meetings and conferences. Over 2,000 participants attended educational sessions and workshops on JEDDI topics that NCSC conducted during 1998 and 1999. Dozens of courts now are actively engaged in JEDDI projects, and the number of courts or court organizations planning JEDDI initiatives is estimated to be in the hundreds.

### Growth Factors

A number of factors have influenced the growth of the JEDDI movement. However, the following factors seem to be primarily responsible.

- The widespread adoption of other types of judicial and general technology solutions over the years now makes it easier for court leaders to see the potential benefits of a new application of technology and to justify the financial investment in it.
- Private attorneys and other organizations that exchange information with the courts have become accustomed to using technology to obtain, prepare, and send information.

- State courts have made great strides in addressing obsolete statutes and court rules that impede the adoption of new technologies to improve court operations. Especially during the last three to four years, much attention has been focused on the changes necessary to facilitate electronic filing and electronic court records.
- The unprecedented growth of the Internet and the spread of both e-mail and Web interactions for personal and business transactions have laid the foundation for an effective communications infrastructure to support JEDDI.
- Advances in the capabilities of off-the-shelf software (e.g., word processing, Web browsers, Adobe PDF writers, and network and desktop operating systems) and hardware (e.g., personal computers, servers, monitors, printers, scanners, and modems) have made it relatively easy to create, store, retrieve, and exchange information electronically.
- Developing technology standards—notably XML—for creating and exchanging intelligent electronic documents are making it feasible to plan and design systems that can reduce manual data entry for all involved parties, trigger automated functions that previously have had to wait for human intervention, and allow courts to present different views of the same information to different categories of users.
- Advances in security technologies and standards, along with legislation and rules governing digital signatures, are providing long-term solutions to ensure the authenticity and integrity of electronic documents.

## **Trends**

Although JEDDI technology is still in its infancy in many ways, several trends are developing.

- Courts are investing substantial time and effort to integrate electronic filing front-end systems with their case management systems.
- Court technology vendors are emerging who provide JEDDI technology as part of a case management product, as a separate product that can be integrated with existing systems, or as an independent service that connects attorneys with the court and delivers their documents electronically.
- There is a rising use of digital signatures and other security technologies to ensure the authenticity of electronic documents.
- Courts are moving toward intelligent text documents, with document imaging used when an original electronic document is not available, rather than JEDDI systems based almost completely on imaging.



- There is growing interest in XML as a viable solution, and steps are being taken toward establishing XML standards for courts.
- The combination of more flexible court rules, new technologies and standards to create intelligent electronic documents, and digital signature technology is making it possible to take a more holistic approach to planning a JEDDI system. Court leaders are starting to recognize the advantages of an electronic “ecosystem” that can be expanded over time to include all entities and functions involved in exchanging justice-related documents and information.

## Planning for JEDDI Implementation

Courts planning JEDDI projects can benefit from the lessons learned through the experiences of other courts and an appreciation for the trends emerging from this relatively new application of technology. The projects that have been most successful have been broad-based efforts, even when the scope of initial implementation has been kept narrow. An essential factor for success is the involvement of all affected parties early in the planning process and throughout the development and implementation phases. A relatively small team can accomplish the actual legwork of planning, analysis, design, development, implementation, and training. However, projects need the backing, oversight, and input provided by both policy-level bodies and operational task forces. Both groups should have adequate representation from all involved entities, such as judges, court administrators, clerks of court, attorneys, prosecutors, and technologists.

Court rules and state statutes need to be addressed adequately to remove any existing barriers to the use of electronic documents. While much work has been accomplished toward this goal, often overlooked is the need to provide flexibility to the courts in managing the details of the system design and the procedures governing its operation. Rules that are too specific regarding how the technology can be used can be almost as crippling as the former rules that permit only paper filings. Because technology is advancing so rapidly, court rules should allow technology-based procedures to be controlled at the administrative level. Court administrators or clerks of court then can respond quickly to system improvements and immediately notify the bar or other users through electronic communication of any resulting changes in procedures. Another area that needs more attention is developing court rules that recognize the vastly different nature of electronic documents and records. Examples of these issues include indefinite page boundaries, multimedia content, and hypertext constructs that permit great flexibility in the ways a document can be organized and navigated and can present references to internal and external sources of supplemental information.

The Internet has proven to be the most practical and effective electronic communications infrastructure on which to base a JEDDI system. The global nature of the Internet greatly increases the potential scope of electronic document applications. Consequently, it becomes very important for courts to establish a long-range vision that includes an entire electronic community. Even though initial pilot projects may be restricted to a specific case type and a handful of filers, those projects should be compatible and consistent with the broader vision. In

keeping with the global nature of the Internet, the use of this public, unregulated network requires the adaptation of standards and appropriate technologies for packaging, transmitting, and protecting electronic documents. Fortunately, these issues are being addressed aggressively by the commercial sector and, at the policy level, by public-sector agencies. The judicial system can benefit greatly from the developments emerging from those efforts.

XML standards and technologies offer the most promising solution for a standardized method to exchange complex electronic text documents. Under this approach, intelligent documents can be constructed and exchanged in a form that permits the systems at each end to identify the information content and process it automatically. The need to ensure the authenticity and integrity of electronic documents is being addressed through PKI technology, which uses digital signatures to establish the level of trust needed for electronic interchange of those documents. Although neither XML nor PKI is necessary to construct a working and useful pilot JEDDI system, court leaders would be wise to include both in their long-range plans.

Although there are no detailed blueprints or prescribed methodologies for planning and implementing JEDDI systems, the path ahead is far less rocky and unsure than it was as recently as three years ago. Moreover, the concept has been shown to be practical and effective. Courts and end users generally are pleased with the results JEDDI technology delivers now and the almost open-ended improvements in the accessibility and exchange of justice-related information it makes possible for the future. Court leaders planning JEDDI projects today are indebted to the earlier practitioners who have blazed the trail, if not paved the road for them.