A Survey of Key Concepts and Issues for Electronic Recordkeeping

CTG.MFA - 001

Models for Action Project:
Developing Practical Approaches to Electronic Records Management and Preservation

Center for Technology in Government
University at Albany--SUNY
State Archives and Records Administration

August 1997

Betsy Maio

This material is based upon work supported in part by the National Historical Publications and Records Commission under Grant No. 96023.

Introduction

The Models for Action project seeks to find practical solutions to electronic recordkeeping in networked computing environments. The project incorporates principles from business process analysis, information systems development, electronic records management and archival preservation in order to find solutions that address recordkeeping at all stages of the records life cycle and -- more importantly -- within the context of the business process which the records support.

The first step in this project was to identify the necessary requirements for creating, managing, and preserving access to records that support an organization's business needs including its legal and evidentiary requirements. Today, more than ever, this depends on compliance with various technology standards and legal and professional guidelines. Such standards allow for communication of records across different computing platforms. They also help to define a "secure" environment, authentication procedures, and terms and conditions for transacting business electronically, and for documenting and attesting to these transactions.

In order to test the project's tools for identifying record keeping requirements in a practical business application, the Models for Action project is developing a prototype for the New York State Adirondack Park Agency. APA's Permitting Process currently uses a mix of Geographic Information System information, paper documents, and a small desktop database. The prototype will apply electronic document management and workflow to the agency's Minor Permitting Process.

A review of technology standards, government policies, legal principals and best practices was conducted in April, 1997 addressing key issues the project expected to encounter during the design and development of the APA prototype. This report outlines the results of that survey and is intended to serve as an introduction to key concepts and to guide the associated choices which APA is excepted to face as they move from a largely paper-based business process to a networked, document management and workflow system.

Review of Key Issues

Digital Signatures and Authentication

Definition

Historically, the legal concept of a signature is very broad and can be defined as any mark that is made with the intention of authenticating a marked document or record. Signatures serve to give evidence or authenticate a record by identifying the signer with the signed record. In some contexts, a signature records the signer's approval or authorization of the signed record and the signer's intention to give it legal effect. A signature also has some ceremonial significance, and can impart a sense of clarity and finality to a record or transaction. For purposes of evidence, a signature must provide for: (1) Signer authentication: i.e., the signature must indicate who signed a record and should be difficult for another person to (re)produce without authorization, and (2) Record authentication: i.e., the signature should identify what is signed, making it difficult or

impractical to falsify without detection. Formal requirements for legal transactions, including the need for signatures, vary in different legal settings. In some settings, these requirements still involve documenting a transaction on paper with penned signatures. (Such requirements remain codified in specific laws, rules and regulations.) However, traditional methods of authentication are undergoing major changes today. For many reasons, computer-based transactions and information can achieve far more than their paper counterparts, including the level of security and authentication possible. Digital signatures are such an example. (American Bar Association, Digital Signature Guidelines, http://www.abanet.org.)

Standards

For purposes of this discussion, an examination of the issues and standards involved with electronic representation of traditional authentication, such as an electronic image of a handwritten signature, has not been included.

Digital Signature Standard (DSS)

Digital signatures represent a specific technology used to authenticate electronic messages, records, or transactions by confirming the identity of the signing/sending party and the integrity of the data/information received. Digital signatures are created and verified by cryptography which is the process of applying a mathematical algorithm to transform information into seemingly unintelligible forms and back again. Digital signatures use "public key cryptography," which employs an algorithm that uses two different but mathematically related keys -- one "private key" for creating and encrypting a digital signature; and another "public key" for verifying the digital signature and returning the information to its original form. Digital signature technology involves the use of "hash functions" which are the mathematical algorithms applied in the creation and verification of digital signatures.

The National Institute of Standards and Technology (NIST) has issued Federal Information Processing Standard (FIPS) 186, Digital Signature Standard (DSS), on May, 1994. The DSS defines a public key cryptographic system for generating and verifying digital signatures. The private key is randomly generated. Using this key and a mathematical process defined in the standard, the public key is generated. The DSS is used with FIPS 180, Secure Hash Standard (SHS), to generate and verify digital signatures. The DSS specifies a Digital Signature Algorithm (DSA) for use in computing and verifying digital signatures. The DSA could be employed in a variety of business applications requiring a replacement of handwritten signatures.

Information on FIPS 186, Digital Signature Standard, is available from: Computer Systems Laboratory, Room B64, Technology Building, National Institute of Standards and Technology, Gaithersburg, MD 20899-9001. Telephone: (301) 975-2816. Fax: (301) 948-1784. E-mail: dward@enh.nist.gov.

Professional Association Guidelines

Digital Signature Guidelines, Information Security Committee, Science and Technology Section, American Bar Association, 1996.

These Guidelines explain digital signature technology in simple terms and examine how this technology can be applied as a computer based alternative to traditional signatures. The Guidelines are designed to assist anyone involved in on line transactions that need to be secure and authentically signed. *(http://www.abanet.org/home.html)*

Public-Key Cryptography Standards (PKCS)

"RSA Laboratories' Public-Key Cryptography Standards (PKCS), the informal intervendor standard was developed in 1991 by RSA Laboratories with representatives of Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell and Sun. Since its publication in June 1991, PKCS has become a part of several standards and products, including Internet Privacy-Enhanced Mail, the NIST/OSI Implementers' Workshop, BLOC F3 Forms Automation, Apple's PowerTalk, Shana Informed, and Fischer International's Workflow 2000. These standards cover RSA encryption, Diffie-Hellman key agreement, password-based encryption, extended-certificate syntax, cryptographic message syntax, private-key information syntax, and certification request syntax, as well as selected attributes." (http://www.rsa.com/rsalabs/pubs/PKCS/)

Secure Electronic Transaction (SET)

"Secure Electronic Transaction (SET) is a technical specification for securing payment card transactions over open networks such as the Internet. SET was developed by Visa and MasterCard, with participation from several technology companies, including Microsoft, IBM, Netscape, SAIC, GTE, Terisa Systems and VeriSign. SET will be based on specially developed encryption technology from RSA Data Security."
(http://www.visa.com/cgi-bin/vee/sf/set/faq.html) "SET, which includes digital certificates - a way of verifying the actual cardholder is making the purchase - will provide financial institutions, merchants, and vendors with a new and secure way of getting the most from the emerging electronic commerce marketplace." *(http://www.visa.com:80/cgi-bin/vee/sf/standard.html)*

Best Practices

Digital Signature

Like a hand written signature in a printed document, a digital signature can be used to identify and authenticate the originator of an electronic document. A digital signature is an unforgeable piece of data, which asserts that a certain person either wrote or otherwise agreed to the electronic document to which the digital signature is attached. The recipient of a digitally signed electronic document can verify both that this document came from the person whose digital signature is attached and that this document is not altered after it is signed.

Pretty Good Privacy (PGP)

Sending e-mail message over the Internet is more like sending a paper mail on postcard than on a sealed envelope. Everybody who has the authority to get into the mail passageway can easily read or even alter the mail. Pretty Good Privacy (PGP), created by Philip Zimmermann, is software that allows the sender of an electronic mail to encrypt and digitally sign the e-mail message or files using the sender's private key. Only the designated e-mail recipient can use the sender's public

key to decrypt this e-mail message or files. While the recipient decrypting the e-mail message or files, the sender authenticates himself/herself to the recipient that the sender is the person who he/she claimed he/she is and the e-mail message or files are not altered after the sender signed the e-mail message or files. Once a digital signature is created, it is impossible for anyone to modify either the message or the signature without being detected by PGP.

Each PGP user must initially generate a pair of complementary keys: a public key and a secret key. Public key and private key are generated at the same time and each key unlocks the code that the other key makes. Public key is publicly distributed to whoever wants to send e-mail message to the person who distributed the public key. Only the person who distributed the public key knows the secret key and it should be guarded carefully.

Policies

On June 11, 1996, Governor's Task Force on Information Resource Management (now known as 'The Office for Technology') released 'Technology Policy 96-14 New York State Use of Electronic Mail.' The purpose of this policy is to promote the use of e-mail as an efficient communication and data gathering tool, and to ensure that State agencies have the information necessary to use e-mail to their best advantage in supporting agency business. It states general policies and security issues about using e-mail communications.

Electronic Data Interchange

Definition

Electronic data interchange (EDI) is commonly defined as the application-to-application transfer of business transactions between computers. Many businesses choose EDI as a fast, inexpensive, and safe method of sending purchase orders, invoices, shipping notices, and other frequently used business documents.

Standards

There are two main EDI standards that are currently used in North America and Europe: the ASC X12 group of standards supported by the American National Standards Institute (ANSI) and the EDIFACT standards supported by the United Nations Economic Commission for Europe (UN/ECE). Both standards activities are managed in the US by: Data Interchange Standards Association, Inc., 1800 Diagonal Road, Suite 200 Alexandria, Virginia, 22314-28552 Voice: 703-548-7005 FAX: 703-548-5738

ASC X12 Standards

ASC X12 is the ANSI Accredited Standards Committee charged with developing EDI standards for use in the United States. The committee develops standards to facilitate electronic interchange relating to such business transactions as order placement and processing, shipping and receiving, invoicing payment and cash application data. The work of ASC X12 is conducted primarily by a series of subcommittees and task groups whose recommendations are presented periodically to the full ASC X12 Committee for ratification (Data Interchange Standards Association, 1990).

The ASC X12 standards specify the segments used in a transaction set, the sequence in which the segments must appear, whether segments are mandatory or optional, when segments can be repeated, and how loops are structured and used.

The X12 Series of Standards

The X12 series of standards consist of a number of interdependent standards. The transaction set standards define the grouping of data into segments and the sequence of these segments to be used in a specified business transaction such as a purchase order. There are also the 'foundation' standards which define the syntax to be used in defining X12 transaction sets as well as the data elements, data segments, and control structures to be used. The full set of foundation standards required to interpret, understand and use the X12 series of transaction set standards, consists of:

- Data element dictionary (X12.3)
- Interchange control structure (X12.5)
- Application control structure (X12.6)
- Data Segment Directory (X12.22)
- Security Structures (X12.58)

EDIFACT

UN/EDIFACT stands for the United Nations rules for the Electronic Data Interchange for Administration, Commerce and Transport. They are a set of international standards, directories and guidelines for the electronic interchange of structured data, and, in particular, relate to trade in goods and services between independent computerized information systems (UN/EDIFACT Rapporteur's Team, 1990). The UN/EDIFACT work on EDI standardization developed from the need for a common international standard for the electronic transmission of commercial data.

In 1971, SITPRO, the Simplification of Trade Procedures Board in Great Britain began work on common EDI standards for Europe. In 1974, the UK EDI syntax called Trade Data Interchange (TDI) was published and was first used by UK customs authorities. In 1975, the UN began to develop terms of reference for international EDI standardization. In 1979, the United National Guidelines for Trade Data Interchange (UN/GTDI) syntax, based on the TDI guidelines developed by SITPRO was published.

By this time, the ANSI X12 standards were in use in North America. The value of merging the two to develop an international EDI standard was recognized and work was initiated within the United Nations/Economic Commission for Europe (UN/ECE) to develop the international EDIFACT standards.

The International Organization for Standardization (ISO) Standard which addresses EDIFACT is ISO 9735: 1988 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Amended and reprinted 1990). This standard includes:

- ISO/DIS 9735-1: Application level syntax rules -- Part 1: Syntax rules common to all parts, together with syntax service directories for each of the parts

- ISO/DIS 9735-2: Application level syntax rules -- Part 2: Syntax rules specific to batch EDI
- ISO/DIS 9735-3: Application level syntax rules -- Part 3: Syntax rules specific to interactive EDI
- ISO/DIS 9735-5: Application level syntax rules -- Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)
- ISO/DIS 9735-6: Application level syntax rules -- Part 6: Secure authentication and acknowledgement message (message type - AUTACK)
- ISO/DIS 9735-8: Application level syntax rules -- Part 8: Associated data in EDI
- ISO/DIS 9735-9 Application level syntax rules -- Part 9: Security key and certificate management message (message type- KEYMAN)

Other Related Standards

TDCC, VICS, WINS, UCS, ODETTE, AIAG, TRADACOM, CIDX, EIDX, HIBCC, EDIFICE, GTDI, GM, Ford Kmart, Sears, CISCO, CargoIMP, SPEC2000, NACHA, EAGLE, NWDA, DoD conventions, TCIF, etc.

Professional Association Guidelines

- *The Commercial Use of Electronic Data Interchange* -- A Report and Model Trading Partner Agreement, Science and Technology Section, American Bar Association. The Business Lawyer, (June 1990) Vol. 45 pp. 1645 1680.

  Model trading partner agreement with commentary and introduction for lawyers and business persons involved with electronic commerce. * Note: A Model Electronic Commerce Trading Partner Agreement Addendum is currently in development by the ABA Science and Technology Section for use as a supplement to trading partner agreements. The Addendum will facilitate the use of secure cryptographic technologies, including digital signatures and certificates, with or without the use of certification authorities.

- *Model Electronic Payments Agreement and Commentary*, Science and Technology Section, American Bar Association. Jurimetrics Journal of Law, Science, and Technology, (Summer 1992) Vol. 32, No. 4 pp. 601 669.

  Model agreement with commentary and introduction for lawyers and business persons involved with electronic payments.

- *EDI Control Guide*, Prepared by the EDI Council of Australia and Information Systems Audit and Control Association, 1990.

  The EDI Control Guide was developed to assist management, information systems personnel and auditors to address the risks and key control issues associated with EDI.

Best Practices

Electronic Data Interchange (EDI) is defined as the inter-process (computer application to computer application) communication of business information in a standardized electronic form. Therefore, Internet could be very useful because not only the communications are for inter-personal (person-to-person) like e-mail but also for inter-processing (process-to-process) like EDI.

For high reliability mission critical applications, redundant Internet Service Providers (ISPs) may be used (with separate backbones), and redundant mail servers at separate locations can be used. A single Internet email or server address can be used to transparently route to any of the redundant servers or network connections. If a dedicated Internet connection is used to transmit important information, the message should be delivered directly to the trading partner's system so that the delivery is assured.

The major uses of EDI are:

- To avoid re-keying EDI orders and invoices
- To achieve error reduction
- To eliminate redundant paper-based transactions
- To reduce document storage costs
- To reduce personnel overhead
- To log all transactions sent through EDI
- To increases sales due to faster order processing

Policies

On April 12, 1996, the Governor's Task Force on Information Resource Management issued 'Technology Policy 96-7 Electronic Data Interchange,' which states: "To facilitate the exchange of information between agencies, and from State agencies to other entities such as businesses, other governments, not-for-profit organizations, etc., the State is establishing a policy regarding Electronic Data Interchange (EDI). The first component of this policy is the State adoption of the ANSI ASC X 12 Standards and the UN/EDIFACT International Standards."

On July 19, 1996, the Governor's Task Force on Information Resource Management issued 'Technology Policy 96-16 Technology Standards,' which states: "The purpose of the technology standards is to provide general guidance to agencies for future technology acquisitions. These standards are, as a result, designed to be "forward looking" and are not intended to accommodate legacy and related systems. The attached standards represent the State's Preferred Standards for technology. The standards will be updated regularly to reflect the changing technology marketplace."

System Administration

Definition

The role of the system administrator is to install, maintain, and support the shared hardware and software resources of an organization. Areas of responsibility typically include:

- Setup and configuration of servers
- System administration: setting up and maintaining accounts, access control, and the user interface
- Installation of shared software and hardware
- System documentation
- Troubleshooting / Problem determination
- Problem management
- System performance analysis
- Change management
- Operations management
- Execution of back-up and recovery procedures
- System monitoring and maintenance of system logs
- User support

Standards

A number of standards have been recommended by the Governor's Task Force on Information Resource Management for providing guidance when acquiring technology (see Policies). These standards will be updated on an ongoing basis and the most recent version can be obtained from the Governor's Task Force Web site, available at http://www.irm.state.ny.us. A section of the recommended standards For Network Services is listed below:

Component	Proposed Standard	International Standard or Responsible Organization
Data Communications Model	TCP/IP	RFC 791, 793, 950, 919, 922
Network Management	SNMP (Simple Network Management Protocol RMON (Remote Monitor MIB2)	RFC 1157
Messaging and Email	SMTP X.400	RFC 821, 822 CCITT X.400-481 ISO/IEC 10021-1 to 15
Attachments to Email	MIME MIMAPI UU Encodes	RFC 1521, 1522 Macintosh
Directory Services	X.500	ISO/IEC 9594, ITU (CCITT) X.500
Digital Communications	ATM, Frame Relay, ISDN	ITU-T
File Services	FTP, FTAM	RFC 959 ISO 8571-1, 2, 3, 4, 5
Enterprise Network Topology	Collapsed Backbone	N/A
LAN Communications	Ethernet Token	IEEE IBM
Cable Plant	Category 5 UTP 62.5/ 25 multimode fiber	N/A

Best Practices

The System Administrator must keep abreast of organizational needs and objectives as well as developments in technology and suggest possible enhancements or changes that could improve productivity and performance. The system administrator must ensure that the networked environment is reliable and serves the needs of the organization. Recommended practices include:

- Make technical decisions which support organizational needs; let the users make the final decision regarding software choices whenever possible - the System Administrator should act as a consultant in this decision-making process.
- Know your users and anticipate their needs. Focus on learning technologies which can support those needs.
- Look at long-term objectives when building the system.
- Understand all components of the system.
- Test all components of the system. In particular, test the back-up and recovery plan. Do not assume that any software or recovery plan will work unless it has been periodically tested.
- Know what the most critical components of the system are and monitor these components. Develop a recovery/contingency plan in case problems occur with these components and test this plan frequently.

- Document all components of the system so that another staff member could troubleshoot when the System Administrator is not available.

Policies

On January 9, 1997, the Governor's Task Force on Information Resource Management issued 'Technology Policy 97-1 Information Security Policy,' which states: "the individual responsible for systems security should not be a system administrator whose primary responsibilities are for maintaining and upgrading operating systems. Separating systems administration from security duties improves the security climate."

On July 19, 1996, and again on January 3, 1997, the Governor's Task Force on Information Resource Management issued 'Technology Policy 96-16 - Technology Standards,' and Technology Policy 96-16A -- Electronic Document Management Systems - Standards, which provides general guidance to agencies for future technology acquisitions. Recommended standards are identified for Data Management Systems, Data Interchange, Network Services, Advanced Telephony, and Document Imaging.

Disaster Recovery

Definition

A disaster is any event that causes the computer systems to be unavailable to supply correct services to users. Disaster recovery is a plan which is developed to protect the computing environment, to re-establish computer and network operations, and to identify and address the critical application needs of the institution in case of disaster.

Standards

There are no current standards for disaster recovery procedures.

Best Practices

General Framework

In order to have an effective disaster recovery plan, an organization must:

- Develop a framework for disaster recovery policy, procedures and standards.
- Define a framework for procedures to interface between related groups in case of a disaster.

Recovery Plan

To have an effective disaster recovery plan, you must develop an organization responsible for writing and maintaining it. The people in this organization must, in turn, develop the plan, and identify who has a role to play in case of information or network disaster. These tasks are carried out as follows:

- Develop disaster recovery guidelines for each corporate application, including items such as:
    - Employee roles and responsibilities.
    - Recovery team roles and responsibilities.

- Recovery priority for each application.
- Operational guidelines.
- Location of production software and data.
- Location of offsite / onsite backup systems and data.
- Arrangements with backup and recovery vendors based on costs, capabilities and required response time.
- Communication trees including names, roles and responsibilities, regular and alternate phone and fax numbers and addresses.
- Procedures to maintain the communication trees.
- Maximum waiting times.
- Provision to relocate key staff and recovery teams after a disaster.

- Assess the effectiveness of existing inventory tracking procedures for computer hardware, network equipment, software packages and data storage media.
- Assess the cost-effectiveness of alternative backup and recovery solutions. Alternatives could include: in-house storage, reciprocal agreements, hot site vs. cold site options, etc.
- Recommend Solutions
- Negotiate backup and recovery arrangements with vendors if necessary.

Technical Procedures

Technical procedures should cover the following tasks:

- Develop and maintain a detailed up-to-date plan including:
  - Measurements of the time required to assemble the team, deploy equipment, reload tapes, etc.
  - A copy of the systems architecture, including system inter-dependencies.
  - Lists of software licenses.
  - Hardware serial numbers.
  - Documentation.
- Rehearse the plan at least once a year.
- Assess reciprocal arrangements vs. internal redundancy.
- Monitor the use of redundant backup systems for routine operations.
- Develop guidelines for diagnostic steps after a disaster, including:
  - An initial assessment of:
    * What caused the failures
    * What are the symptoms
    * The best course of action
  - Familiarization with the data recovery software.
  - Checking the backup tapes.
  - Running a thorough set of hardware diagnostics.
- Develop and maintain up-to-date backup media management, restoration testing and validation procedures.
- Assess new disaster recovery techniques to protect data such as electronic vaulting and server mirroring.

Network recovery involves the execution of technically complex procedures. To ensure a fast recovery, these procedures should always be up-to-date and easily accessible. The availability of such procedures will support effective team training.

Policies

On June 11, 1996, the Governor's Task Force on Information Resource Management issued 'Technology Policy 96-14 New York State Use of Electronic Mail,' which states: "Agency network administrators and internal control (and/or internal audit) staff are responsible for e-mail security, backup, and disaster recovery."

On January 9, 1997, the Governor's Task Force on Information Resource Management issued 'Technology Policy 97-1 Information Security Policy,' which states: "All systems must have back-up and recovery procedures that are documented, maintained and stored off site. The agency should make every effort to test these procedures on an annual basis."

Network Security

Note: this topic was not fully addressed due to time limitations and the complexity of the issues involved.

Definition

Security is understood to include protection of the privacy of information, protection of information against unauthorized modification, protection of systems against denial of service, and protection of systems against unauthorized access. Network security addresses these issues in a networked environment.

Standards

The development of network security standards facilitates the interoperability between security service implementations.

RSA

"RSA is a public-key cryptosystem for both encryption and authentication; it was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It works as follows: take two large primes, p and q, and find their product n = pq; n is called the modulus. Choose a number, e, less than n and relatively prime to (p-1)(q-1), and find its inverse, d, mod (p-1)(q-1), which means that ed = 1 mod (p-1)(q-1); e and d are called the public and private exponents, respectively. The public key is the pair (n,e); the private key is d. The factors p and q must be kept secret, or destroyed." (http://www.qualix.com/html/rsa.html)

DES

"DES is the Data Encryption Standard, an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard; the details can be found in the official FIPS publication. It was originally developed at IBM. DES has been extensively studied over the last 15 years and is the most well-known and widely used cryptosystem in the world.

DES is a secret-key, symmetric cryptosystem: when used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult; public-key cryptography was invented to solve this problem." (http://www.qualix.com/html/des.html)

Capstone

"Capstone is the U.S. government's long-term project to develop a set of standards for publicly-available cryptography, as authorized by the Computer Security Act of 1987. The primary agencies responsible for Capstone are NIST and the NSA (see above). The plan calls for the elements of Capstone to become official U.S. government standards, in which case both the government itself and all private companies doing business with the government would be required to use Capstone." (http://www.qualix.com/html/cstone.html)

Clipper

"Clipper is an encryption chip developed and sponsored by the U.S. government as part of the Capstone project. Announced by the White House in April, 1993, Clipper was designed to balance the competing concerns of federal law-enforcement agencies with those of private citizens and industry. The law-enforcement agencies wish to have access to the communications of suspected criminals, for example by wire-tapping; these needs are threatened by secure cryptography. Industry and individual citizens, however, want secure communications, and look to cryptography to provide it." (http://www.qualix.com/html/cstone.html)

Skipjack

"Skipjack is the encryption algorithm contained in the Clipper chip; it was designed by the NSA. It uses an 80-bit key to encrypt 64-bit blocks of data; the same key is used for the decryption. Skipjack can be used in the same modes as DES, and may be more secure than DES, since it uses 80-bit keys and scrambles the data for 32 steps, or "rounds"; by contrast, DES uses 56-bit keys and scrambles the data for only 16 rounds." (http://www.qualix.com/html/cstone.html)

DSS

"DSS is the proposed Digital Signature Standard, which specifies a Digital Signature Algorithm (DSA), and is a part of the U.S. government's Capstone project. It was selected by NIST, in cooperation with the NSA, to be the digital authentication standard of the U.S. government; whether the government should in fact adopt it as the official standard is still under debate. DSS is based on the discrete log problem and derives from cryptosystems proposed by Schnorr and ElGamal. It is for authentication only." (http://www.qualix.com/html/cstone.html)

Other Related Standards

NIST, NSA, MD2, MD4, MD5 (MD stands for Message Digest), SHS, Kerberos, RC2, RC4, PEM, RIPEM, PKCS, RSAREF.

Best Practices

The following security guidelines address the entire Internet community, consisting of users, hosts, local, regional, domestic and international backbone networks, and vendors who supply operating systems, routers, network management tools, workstations and other network components.

1. Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.
2. Users have a responsibility to employ available security mechanisms and procedures for protecting their own data. They also have a responsibility for assisting in the protection of the systems they use.
3. Computer and network service providers are responsible for maintaining the security of the systems they operate. They are further responsible for notifying users of their security policies and any changes to these policies.
4. Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls.
5. Users, service providers, and hardware and software vendors are responsible for cooperating to provide security.
6. Technical improvements in Internet security protocols should be sought on a continuing basis. At the same time, personnel developing new protocols, hardware or software for the Internet are expected to include security considerations as part of the design and development process.

Five areas should be addressed in improving local security:

1. There must be a clear statement of the local security policy, and this policy must be communicated to the users and other relevant parties. The policy should be on file and available to users at all times, and should be communicated to users as part of providing access to the system.
2. Adequate security controls must be implemented. At a minimum, this means controlling access to systems via passwords, instituting sound password management, and configuring the system to protect itself and the information within it.
3. There must be a capability to monitor security compliance and respond to incidents involving violation of security. Logs of logins, attempted logins, and other security-relevant events are strongly advised, as well as regular audit of these logs.
4. Up-to-date security information is a pre-requisite for sound decision-making and this information must be actively sought on an ongoing basis. The CERT Coordination Center (http://www.cert.org) is an excellent source for information relating to security issues on the Internet.
5. There must be an established chain of communication and control to handle security matters. A responsible person should be identified as the security contact. The means for reaching the security contact should be made known to all users and should be registered in public directories, and it should be easy for computer emergency response centers to find contact information at any time.

6. Sites and networks which are notified of security incidents should respond in a timely and effective manner. In the case of penetrations or other violations, sites and networks should allocate resources and capabilities to identify the nature of the incident and limit the damage.

Policies

On January 9, 1997, the Governor's Task Force On Information Resource Management released 'Technology Policy 97-1 Information Security Policy.' It states that "This document is designed to provide State agencies with recommended minimum security policies for protection of assets inclusive of information, computers, and networks." It provides physical access security guidances on Secure Locations, Location Selection, Review of New Collections to Outside Sources, Review of Installation, Platform-specific Physical Security, External Network Access to Agency Information, Transaction Controls and Database Security, Downloading Software, Non-Agency Owned IT Components, Agency Owned IT Components and Logging.

Digital Spatial Meta Data

Definition

Meta Data, or "data about data," describe the content, quality, condition, and other characteristics of data.

Standards

The FGDC Content Standard for Digital Geospatial Meta Data At its June 8, 1994, meeting, the Federal Geographic Data Committee (FGDC) approved the "Content Standards for Digital Geospatial Meta Data. The standard specifies the information content of meta data for a set of digital geospatial data. The purpose of the standard is to provide a common set of terminology and definitions for documentation related to these meta data. their geospatial data.

The standard specifies information that helps prospective users to determine what data exist, the fitness of these data for their applications, and the conditions for accessing these data. Meta Data also aid the transfer of data to other users' systems.

Other Related Standards

The FGDC Content Standard identifies and describes the fields to be included in the meta data record. It does not, however, provide guidelines for a standard vocabulary to be used when filling out the fields. Standard vocabulary has, however, been identified at the federal level for cadastral data and for the classification of wetlands. The FGDC Steering Committee, on December 17, 1996, formally adopted as FGDC Standards the 'Cadastral Data Content Standard' and the 'Classification of Wetlands and Deepwater Habitats of the United States.'

The "Classification of Wetlands and Deepwater Habitats of the United States," sponsored by the Wetlands Subcommittee, is a classification standard that provides specific ecological and hydrological information for the identification, classification, and mapping of wetlands in the United States and its territories. A limited number of written copies are available from the FGDC (see below). Additional copies of the Coward in Classification System (Coward in et al. 1979) are for sale by the U.S. Government Printing Office, Washington, D.C. Payment may be made by

check, money order, or deposit account. The publication is available through the Library of Congress (QH76U5a79/31 [QH104] 574.5'0973s [574.5'2632] 79-607795.

The Cadastral Data Content Standard, sponsored by the Subcommittee on Cadastral Data, describes a logical data model containing the attributes or elements that are found in land ownership related documents.

Requests for written copies of the above standards should be sent by mail to: FGDC Secretariat (attn: Jennifer Fox), U.S. Geological Survey, 590 National Center, 12201 Sunrise Valley Drive, Reston, Virginia, 22092; telephone 703-648-5514; fax 703-648-5755; or Internet "gdc@usgs.gov". Information is also available from the FGDC Web site: http://www.fgdc.gov

Best Practices

The main reason to document data is to maintain an organization's investment in its geospatial data. Organizations that do not document their data often find that, over time or because of personnel changes, they no longer know the content or quality of their data. Organizations then cannot trust the results generated from the data in which they have invested their time and resources. In addition, the lack of information about other organizations' data often leads to a needless duplicating of effort.

The major uses of meta data are:

- To help organize and maintain an organization's internal investment in spatial data,
- To provide information about an organization's data holdings to data catalogues, clearinghouses, and brokerages, and
- To provide information to process and interpret data received through a transfer from an external source.

The prototype NYS GIS Spatial Data Clearinghouse (http://www.ctg.albany.edu/gisny.html) employed the FGDC Meta Data Content Standard as the foundation for discovering and exchanging GIS datasets in New York State. While the federal standard may be refined and/or further defined by New York State, it is anticipated that a NYS standard will closely follow the structure of the federal standard.

Policies

On April 11, 1994, President Clinton signed Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure." This executive order instructs Federal agencies to use the FGDC Content Standard for Digital Geospatial Meta Data to document new geospatial data beginning in 1995, and to provide these meta data to the public through the National Geospatial Data Clearinghouse.

On September 17, 1996, the Governor's Task Force on Information Resource Management issued 'Technology Policy 96-18 Geographic Information Systems,' which states: "A GIS Meta Data Clearinghouse will be established in the State Library. The clearinghouse will be set up to

provide descriptions of the data available to users and easy access to data currently residing within State and local agencies. Other data coordination issues will be addressed through a work group (established by the NYS GIS Coordinating Body)."

Sources of Information

American Bar Association (ABA) Science and Technology Section. http://www.abanet.org
American National Standards Organization (ANSI). http://www.ansi.org
Information Systems Audit and Control Association. http://www.isaca.org
International Electrotechnical Commission (IEC). http://www.iec.ch
International Organization for Standardization (ISO). http://www.iso.ch
International Telecommunication Union (ITU). http://www.itu.ch
National Institute of Standards and Technology (NIST). http://www.nist.gov
NYS Governor's Task Force on Information Resource Management. http://www.irm.state.ny.us

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: A Survey of Key Concepts and Issues for Electronic Recordkeeping

B. DATE Report Downloaded From the Internet: 11 May 99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #:) **Lawrence Livermore National Lab**
7000 East Ave.
Livermore, CA 94550-9234

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date**: 11 MAY 99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.