Standard Guide for Electronic Authentication of Health Care Information[1]

This standard is issued under the fixed designation E1762; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide covers:

1.1.1 Defining a document structure for use by electronic signature mechanisms (Section 4),

1.1.2 Describing the characteristics of an electronic signature process (Section 5),

1.1.3 Defining minimum requirements for different electronic signature mechanisms (Section 5),

1.1.4 Defining signature attributes for use with electronic signature mechanisms (Section 6),

1.1.5 Describing acceptable electronic signature mechanisms and technologies (Section 7),

1.1.6 Defining minimum requirements for user identification, access control, and other security requirements for electronic signatures (Section 9), and

1.1.7 Outlining technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism (Section 8 and Appendix X1-Appendix X4).

1.2 This guide is intended to be complementary to standards under development in other organizations. The determination of which documents require signatures is out of scope, since it is a matter addressed by law, regulation, accreditation standards, and an organization's policy.

1.3 Organizations shall develop policies and procedures that define the content of the medical record, what is a documented event, and what time constitutes event time. Organizations should review applicable statutes and regulations, accreditation standards, and professional practice guidelines in developing these policies and procedures.

2. Referenced Documents

2.1 *ISO Standards:*

ISO 9594-8 1993: The Directory: Authentication Framework (also available as ITU-S X.509)[2]

ISO 8825-1 1993: Specification of Basic Encoding Rules for ASN.1[2]

ISO 7816 1993: IC Cards with Contacts[2]

ISO 10036 1994: Contactless IC Cards[2]

2.2 *ANSI Standards:*

ANSI X9.30 Part 3: Certificate Management for DSA, November 1994 (ballot copy)[3]

ANSI X9.31 Part 3: Certificate Management for RSA, July 1994 (draft)[3]

ANSI X9.31 Part 1: RSA Signature Algorithm, July 1994 (ballot copy) (technically aligned with ISO/IEC 9796)[3]

ANSI X9.30 Part 1: Digital Signature Algorithm, July 1994 (ballot copy) (technically aligned with NIST FIPS PUB 186)[3]

ANSI X9F1, ANSI X9.45: Enhanced Management Controls Using Attribute Certificates, September 1994 (draft)[3]

2.3 *Other Standards:*

FIPS PUB 112: Standards on Password Usage, May 1985[4]

FIPS PUB 181: Secure Hash Standard, 1994 (technically aligned with ANSI X9.30–1)[4]

FIPS PUB 186: Digital Signature Standard, 1994 (technically aligned with ANSI X9.30–1)[4]

PKCS #1: RSA Encryption Standard (version 1.5), November 1993[5]

PKCS #5: Password-Based Encryption Standard, 1994[5]

PKCS #7: Cryptographic Message Syntax Standard, 1994[5]

3. Terminology

3.1 *Definitions:*

3.1.1 *access control*—the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 *accountability*—the property that ensures that the actions of an entity may be traced uniquely to the entity.

3.1.3 *attribute*—a piece of information associated with the use of a document.

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.25 on Healthcare Data Management, Security, Confidentiality, and Privacy.

Current edition approved March 1, 2013. Published March 2013. Originally approved in 1995. Last previous edition approved in 2009 as E1762–95 (2009). DOI: 10.1520/E1762-95R13.

[2] Available from ISO, 1 Rue de Varembe, Case Postale 56, CH 1211, Geneve, Switzerland.

[3] Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036, http://www.ansi.org.

[4] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

[5] Available from RSA Data Security, 100 Marine Parkway, Redwood City, CA 64065.

3.1.4 *attribute certificate*—a digitally signed data structure that binds a user to a set of attributes.

3.1.5 *authorization*—verification that an electronically signed transaction is acceptable according to the rules and limits of the parties involved.

3.1.6 *authorization certificate*—an attribute certificate in which the attributes indicate constraints on the documents the user may digitally sign.

3.1.7 *availability*—the property of being accessible and useable upon demand by an authorized entity.

3.1.8 *computer-based patient record (CPR)*—the computer-based patient record is a collection of health information concerning one person linked by one or more identifiers. In the context of this guide, this term is synonymous with electronic patient record and electronic health record.

3.1.9 *computer-based patient record system (CPRS)*—the CPRS uses the information of the CPR and performs the application functions according to underlying processes and its interacting with related data and knowledge bases. CPRS is synonymous with electronic patient record systems.

3.1.10 *data integrity*—the property that data has not been altered or destroyed in an unauthorized manner.

3.1.11 *data origin authentication*—corroboration that the source of data received is as claimed.

3.1.12 *digital signature*—data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, for example, by the recipient.

3.1.13 *document access time*—the time(s) when the subject document was accessed for reading, writing, or editing.

3.1.14 *document attribute*—an attribute describing a characteristic of a document.

3.1.15 *document creation time*—the time of the creation of the subject document.

3.1.16 *document editing time*—the time(s) of the editing of the subject document.

3.1.17 *domain*—a group of systems that are under control of the same security authority.

3.1.18 *electronic document*—a defined set of digital information, the minimal unit of information that may be digitally signed.

3.1.19 *electronic signature*—the act of attaching a signature by electronic means. After the electronic signature process, it is a sequence of bits associated with an electronic document, which binds it to a particular entity.

3.1.20 *event time*—the time of the documented event.

3.1.21 *one-way hash function*—a function that maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

3.1.21.1 It is computationally infeasible to find for a given output an input that maps to this output.

3.1.21.2 It is computationally infeasible to find for a given input a second input that maps to the same output.

3.1.22 *private key*—a key in an asymmetric algorithm; the possession of this key is restricted, usually to one entity.

3.1.23 *public key*—a key in an asymmetric algorithm that is publicly available.

3.1.24 *public key certificate*—a digitally signed data structure which binds a user's identity to a public key.

3.1.25 *repudiation*—denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.26 *role*—the role of a user when performing a signature. Examples include: physician, nurse, allied health professional, transcriptionist/recorder, and others.

3.1.27 *secret key*—a key in a symmetric algorithm; the possession of this key is restricted, usually to two entities.

3.1.28 *signature*—the act of taking responsibility for a document. Unless explicitly indicated otherwise, an electronic signature is meant in this guide.

3.1.29 *signature attribute*—an attribute characterizing a given user's signature on a document.

3.1.30 *signature purpose*—an indication of the reason an entity signs a document. This is included in the signed information and can be used when determining accountability for various actions concerning the document. Examples include: author, transcriptionist/recorder, and witness.

3.1.31 *signature time*—the time a particular signature was generated and affixed to a document.

3.1.32 *signature verification*—the process by which the recipient of a document determines that the document has not been altered and that the signature was affixed by the claimed signer. This will in general make use of the document, the signature, and other information, such as cryptographic keys or biometric templates.

3.1.33 *user authentication*—the provision of assurance of the claimed identity of an entity.

3.2 *Acronyms:*

AAMT	American Association for Medical Transcription
ABA	American Bar Association
AHIMA	American Health Information Management Association
AIM	Advanced Informatics in Medicine
ASC X3	Accredited Standards Committee X3
ASC X9	Accredited Standards Committee X9
ASC X12N	Accredited Standards Committee X12N
CA	Certification Authority
CEN	Comité Européen de Normalisation (European Standards Committee)
CLC	Comité Européen de Normalisation Electrotechnique (CENELEC)
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm (NIST)
EWOS	European Workshop for Open Systems
ES	Electronic Signature
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard
ISO	International Standards Organization
ITSTC	International Technology Steering Committee
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
MAC	Message Athentication Code
NIST	National Institute for Standards and Technology
NTP	Network Time Protocol
PCMCIA	Personal Computer Memory Card Interface Association
RSA	Rivest-Shamir-Adleman (signature algorithm)

SEISMED	Secure Environment for Information Systems in Medicine
THIS	Trusted Health Information Systems
TTP	Trusted Third Party

4. Significance and Use

4.1 This guide serves three purposes:

4.1.1 To serve as a guide for developers of computer software providing, or interacting with, electronic signature processes,

4.1.2 To serve as a guide to healthcare providers who are implementing electronic signature mechanisms, and

4.1.3 To be a consensus standard on the design, implementation, and use of electronic signatures.

5. Background Information

5.1 The creation of computer-based patient record systems depends on a consensus of electronic signature processes that are widely accepted by professional, regulatory, and legal organizations. The objective is to create guidelines for entering information into a computer system with the assurance that the information conforms with the principles of accountability, data integrity, and non-repudiation. Although various organizations have commenced work in the field of electronic signatures, a standard for the authentication of health information is needed. Consequently, this standard is intended as a national standard for electronic signatures for health care information. Technological advances and increases in the legitimate uses and demands for patient health information led the Institute of Medicine (IOM) to convene a committee to identify actions and research for a computer-based patient record (CPR). The committee's report endorsed the adoption of the CPR as the standard for all health care records and the establishment of a Computer-based Patient Record Institute (CPRI). National Information Infrastructure initiatives, the ever increasing complexity of health care delivery, a growing need for accessible, affordable, and retrievable patient data to support clinical practice, research, and policy development support this recommendation. Major issues identified by CPRI as essential to the timely development of CPRs include authentication of electronic signatures (as replacements for paper signatures), as well as patient and provider confidentiality and electronic data security.

5.2 User authentication is used to identify an entity (person or machine) and verify the identity of the entity. Data origin authentication binds that entity and verification to a piece of information. The focus of this standard is the application of user and data authentication to information generated as part of the health care process. The mechanism providing this capability is the electronic signature.

5.3 Determination of which events are documented and which documents must be signed are defined by law, regulation, accreditation standards, and the originating organization's policy. Such policy issues are discussed in Appendix X4.

5.4 Signatures have been a part of the documentation process in health care and have traditionally been indicators of accountability. Health care providers are faced with the inevitable transition toward computerization. For electronic health record systems to be accepted, they must provide an equivalent or greater level of accurate data entry, accountability, and appropriate quality improvement mechanisms. In this context, a standard is needed that does not allow a party to successfully deny authorship and reject responsibility (repudiation).

5.5 The guide addresses the following requirements, which any system claiming to conform to this guide shall support:

5.5.1 Non-repudiation,

5.5.2 Integrity,

5.5.3 Secure user authentication,

5.5.4 Multiple signatures,

5.5.5 Signature attributes,

5.5.6 Countersignatures,

5.5.7 Transportability,

5.5.8 Interoperability,

5.5.9 Independent verifiability, and

5.5.10 Continuity of signature capability.

5.6 Various technologies may fulfill one or more of these requirements. Thus, a complete electronic signature system may require more than one of the technologies described in this guide. Currently, there are no recognized security techniques that provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques.

5.7 The electronic signature process involves authentication of the signer's identity, a signature process according to system design and software instructions, binding of the signature to the document, and non-alterability after the signature has been affixed to the document. The generation of electronic signatures requires the successful identification and authentication of the signer at the time of the signature. To conform to this guide, a system shall also meet health information security and authentication standards. Computer-based patient record systems may also be subject to statutes and regulations in some jurisdictions.

5.8 While most electronic signature standards in the banking, electronic mail, and business sectors address only digital signature systems, this standard acknowledges the efforts of industry and systems integrators to achieve authentication with other methods. Therefore, this standard will not be restricted to a single technology.

6. Document Structure

6.1 For any data or information for which authentication is required, the system shall:

6.1.1 Provide to the signer an accurate representation of the health care information being signed,

6.1.2 Append one or multiple signatures,

6.1.3 Include, with each signature, information associated with the signer (that is, signature attributes and possibly unsigned attributes), and

6.1.4 Append zero or more document identifiers and attributes associated with the document.

6.2 A document therefore consists of the health care information, one or more signatures with corresponding signature attributes, and, when desired, one or more document attributes. A user's signature then applies to the health care information, the document attributes, and that user's signature attributes. The signer need not be accountable for those document attributes supplied by the system, but they are rendered non-alterable by the signature process. The verifier must be made aware of which document attributes the signer takes responsibility for. This might be done via bilateral agreements or other contractual arrangements, or it might be signalled explicitly as part of the signer's signature attributes.

6.3 This guide describes the physical representation of one or more of the document components when presented to the signature mechanism. This does not imply that the document must be stored, transmitted, or otherwise manipulated using this representation at any time other than signature processing.

6.4 This guide does not put any explicit restrictions on the type or format of the health information content. Health information may be of a particular type, or may be a combination of several information types, for example:

6.4.1 Numeric data (either encoded, or not),

6.4.2 Text,

6.4.3 Graphic,

6.4.4 Images, for example, scanned documents, and clinical digital images,

6.4.5 Audio,

6.4.6 Video, and

6.4.7 Waveforms.

6.5 It is expected that the internal structure of the health information content, while not visible to the electronic signature mechanism, will be defined in other standards.

6.6 Document attributes allow a cataloguing and or interpretation of the content of a document according to a standard without having to examine the health information content itself.

6.7 Policies, procedures, and other standards of the originator and recipient will dictate which attributes are required in various documents and applications (see Appendix X4). The scope of accountability for a given document, in terms of each individual signatory, relates to the combined set of document content, document attributes, and signature attributes visible (that is, displayed or otherwise accessible) to the user at the time the signature is applied. This information may be conveyed between originator and recipient as part of bilateral agreements or trade practice.

6.8 The system shall support the presence of at least the following attributes:

6.8.1 Document creation time,

6.8.2 Document type information, which may be hierarchical,

6.8.3 Event time (user or system assigned),

6.8.4 Document modification and access times,

6.8.5 Location of origin,

6.8.6 Data type(s),

6.8.7 Data format(s), including character sets,

6.8.8 Originating (source) organization,

6.8.9 Patient identifier,

6.8.10 Event type, and

6.8.11 Document identifier.

6.9 Although this guide does not specify the structure of a document identifier, it shall convey sufficient information to locate and retrieve the document, including the originating organization identifier, originating system or application identifier, a document serial number assigned by the application, and (if needed) a revision number. The document identifier is also used as a signature attribute to link related documents, as described in Section 8.

6.10 The electronic signature model discussed in Sections 7-9 requires the ability to attach multiple signatures to a document, as well as the ability to include per-signer information in the signature process.

6.11 Note that a combination of signatures with various purposes (see Section 6) may be required for a document to be accepted by the recipient. For example, a transcriptionist/recorder signature by itself would likely not be sufficient for a document to be accepted. Appendix X1 discusses the use of authorization certificates to indicate which combinations of signatures are considered acceptable by a particular originating system. It also discusses mechanisms for representing the rules used to determine these signature requirements in a data structure called an authorization certificate.

7. Electronic Signature Requirements

7.1 The electronic signature uniquely identifies the signer and ensures the signed document was not modified after the signature was affixed. If the signed document is converted to another format (for example, between various image formats), the electronic signature applies only to the original format.

7.2 The electronic signature process, at an abstract level, consists of two operations, each of which has several characteristics or components.

7.2.1 Signing of a document has the following three components:

7.2.1.1 Secure user authentication (proof of claimed identity) of the signer, at the time the signature is generated,

7.2.1.2 Creation of the logical manifestation of signature, and

7.2.1.3 Ensuring the integrity of the signed document.

7.2.2 Verifying a signature on a document has the following two components:

7.2.2.1 Verifying the integrity of the document and associated attributes, and

7.2.2.2 Verifying the identity of the signer.

7.3 This leads to several general requirements, as well as requirements that are specific to one of these components. All of these requirements shall be met by systems claiming to implement electronic signatures for health care authentication.

7.3.1 *General Requirements:*

7.3.1.1 *Non-repudiation*— Proof (to a third party) that only the signer could have created a signature. Non-repudiation cannot be ensured until the completion of the applicable dispute resolution process. This process may be influenced by agreements between the signer and verifier (for example, trading partner agreements or system rules), and such agreements would implicate the appropriate technologies that could be used to provide electronic signatures.

7.3.1.2 *Integrity*—After a signature has been affixed, any change in the information will cause the signature verification process to detect that the information has been changed. Action taken as a result of this discovery is dependent on a number of factors, including the purpose of the signature, and might include rejection of the document, forwarding to some (human) user for manual review, etc.

7.3.2 *User Authentication Requirements:*

7.3.2.1 *Secure User Authentication* —The act of signing shall include a secure means of proving the signer's identity. Relevant technologies include the use of biometrics (fingerprints, retinal scans, handwritten signature verification, etc.), tokens, or passwords (if implemented in conformance with appropriate guidelines). The type and frequency of user authentication (for example, authentication at logon versus authentication every time a signature is applied) is determined by the rules and security policy of the signer's organization. Examples of such policies might include: (*1*) explicit user authentication at system access and explicit user authentication at signature time for each document (that is, each document requires a formal signature action or process) and (*2*) explicit user authentication at system access but thereafter implicit (that is, each document requires formal review/acceptance but not a formal signature action or process).

7.3.3 *Logical Manifestation Requirements:*

7.3.3.1 *Multiple Signatures*—It shall be possible for multiple parties to sign a document. Multiple signatures are, conceptually, simply appended to the document. Fig. 1 illustrates a document with a single signature attached. Fig. 2 illustrates a document with an additional signature attached.

7.3.3.2 *Signature Attributes*—It shall be possible for a signer to supply additional information (for example, timestamp, signature purpose), specific to that user, in the signed data. That is, the signed data consists of at least the document and the particular signer's signature attributes.

7.3.3.3 *Countersignatures*—It shall be possible to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where some party signs a document which has already been signed by another party. See Fig. 3.

7.3.4 *Verification Requirements:*

7.3.4.1 *Transportability*— The signed document can be transported (over an insecure network) to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

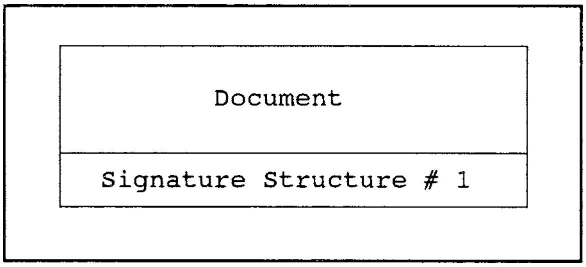


FIG. 1 Single Signature

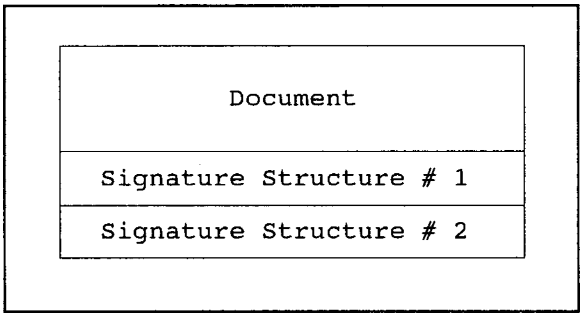


FIG. 2 Multiple Signatures

7.3.4.2 *Interoperability*— The signed document can be processed by a recipient, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

7.3.4.3 *Independent Verifiability*—It shall be possible to verify the signature without the cooperation of the signer.

7.3.4.4 *Continuity of Signature Capability*—The public verification of a signature shall not compromise the ability of the signer to apply additional secure signatures at a later date.

8. Signature Attributes

8.1 Signature attributes identify characteristics about the signature and the signer. The signature attributes include:

8.1.1 Signature purpose,

8.1.2 Signature sub-purpose (for use with the addendum Signature),

8.1.3 Signature time,

8.1.4 Location,

8.1.5 Signer's identity,

8.1.6 Signer's role,

8.1.7 Signer's organization,

8.1.8 Document link,

8.1.9 Biometric information,

8.1.10 Annotation, and

8.1.11 Other attributes, as defined by organizations or other standards.

8.1.12 Signature time and signer identity are mandatory attributes; the others may be optional in a given application or signed document, depending on the originating organization's security policy.

8.1.13 The signer identity may be implicit in some cases. For example, when using digital signatures, it may be the identity contained in a certificate used to verify the signature.

8.2 *Health Information Electronic Signature Purposes:*

8.2.1 The following signature purposes shall be supported under this guide:

8.2.1.1 Author's signature,

8.2.1.2 Coauthor's signature,

8.2.1.3 Co-participant's signature,

8.2.1.4 Transcriptionist/Recorder signature,

8.2.1.5 Verification signature,

8.2.1.6 Validation signature,

8.2.1.7 Consent signature,

8.2.1.8 Witness signature,

8.2.1.9 Event witness signature,

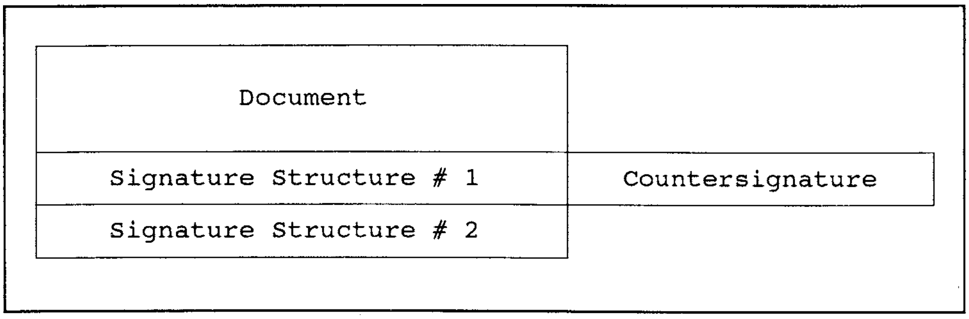


FIG. 3 Countersignatures

8.2.1.10 Identity witness signature,

8.2.1.11 Consent witness signature,

8.2.1.12 Interpreter signature,

8.2.1.13 Review signature,

8.2.1.14 Source signature,

8.2.1.15 Addendum signature,

8.2.1.16 Administrative signature,

8.2.1.17 Timestamp signature, and

8.2.1.18 Other.

8.2.2 Each of these signature types can be executed by multiple user types. Any definition rules as to user type and signature type should be system configurable and not be part of the digital signature standard.

8.2.2.1 *Author's Signature*—the signature of the primary or sole author of a health information document. There can be only one primary author of a health information document.

8.2.2.2 *Coauthor's Signature*—the signature of a health information document coauthor. There can be multiple coauthors of a health information document.

8.2.2.3 *Co-participant's Signature* —the signature of an individual who is a participant in the health information document but is not an author or coauthor. (*Example*—a surgeon who is required by institutional, regulatory, or legal rules to sign an operative report, but who was not involved in the authorship of that report.)

8.2.2.4 *Transcriptionist/Recorder Signature*—the signature of an individual who has transcribed a dictated document or recorded written text into a digital machine readable format.

8.2.2.5 *Verification Signature*—a signature verifying the information contained in a document. (*Example*—a physician is required to countersign a verbal order that has previously been recorded in the medical record by a registered nurse who has carried out the verbal order.)

8.2.2.6 *Validation Signature*—a signature validating a health information document for inclusion in the patient record. (*Example*—a medical student or resident is credentialed to perform history or physical examinations and to write progress notes. The attending physician signs the history and physical examination to validate the entry for inclusion in the patient's medical record.)

8.2.2.7 *Consent Signature*—the signature of an individual consenting to what is described in a health information document.

8.2.2.8 *Signature Witness Signature* —the signature of a witness to any other signature.

8.2.2.9 *Event Witness Signature*—the signature of a witness to an event. (*Example*—the witness has observed a procedure and is attesting to this fact.)

8.2.2.10 *Identity Witness Signature* —the signature of an individual who has witnessed another individual who is known to them signing a document. (*Example* —the identity witness is a notary public.)

8.2.2.11 *Consent Witness Signature*—the signature of an individual who has witnessed the health care provider counselling a patient.

8.2.2.12 *Interpreter Signature*—the signature of an individual who has translated health care information during an event or the obtaining of consent to a treatment.

8.2.2.13 *Review Signature*— the signature of a person, device, or algorithm that has reviewed or filtered data for inclusion into the patient record. (*Examples:* (*1*) a medical records clerk who scans a document for inclusion in the medical record, enters header information, or catalogues and classifies the data, or a combination thereof; (*2*) a gateway that receives data from another computer system and interprets that data or changes its format, or both, before entering it into the patient record.)

8.2.2.14 *Source Signature*— the signature of an automated data source. (*Examples:* (*1*) the signature for an image that is generated by a device for inclusion in the patient record; (*2*) the signature for an ECG derived by an ECG system for inclusion in the patient record; (*3*) the data from a biomedical monitoring device or system that is for inclusion in the patient record.)

8.2.2.15 *Addendum Signature*—the signature on a new amended document of an individual who has corrected, edited, or amended an original health information document. An addendum signature can either be a signature type or a signature sub-type (see 8.1). Any document with an addendum signature shall have a companion document that is the original document with its original, unaltered content, and original signatures. The original document shall be referenced via an attribute in the new document, which contains, for example, the digest of the old document. Whether the original, unaltered, document is always displayed with the addended document is a local matter, but the original, unaltered, document must remain as part of the patient record and be retrievable on demand.

8.2.2.16 *Modification Signature*—the signature on an original document of an individual who has generated a new amended document. This (original) document shall reference the new document via an additional signature purpose. This is the inverse of an addendum signature and provides a pointer from the original to the amended document.

8.2.2.17 *Administrative (Error/Edit) Signature*—the signature of an individual who is certifying that the document is invalidated by an error(s), or is placed in the wrong chart. An administrative (error/edit) signature must include an addendum to the document and therefore shall have an addendum signature sub-type (see 8.1). This signature is reserved for the highest health information system administrative classification, since it is a statement that the entire document is invalidated by the error and that the document should no longer be used for patient care, although for legal reasons the document must remain part of the permanent patient record.

8.2.2.18 *Timestamp Signature*—the signature by an entity or device trusted to provide accurate timestamps. This timestamp might be provided, for example, in the signature time attribute.

8.2.3 Systems shall support at least the above signature purposes but may allow organizations to define their own additional purposes. If no signature purpose is specified, then none can be assumed, but the usual security services (authentication, integrity, etc.) are provided.

8.3 *Signature Time*— The signature time indicates the time when a particular signature was affixed to the document. This need not be the same as the document (creation) time or event time.

8.4 *Location*—The location indicates the physical location (device or machine identifier) or network address where the signature was generated.

8.5 *Signer Identity*— The signer identity indicates the name or other identifying information of the entity signing the document. It may also include information useful in retrieving any data, such as certificates or templates, required for verification of the signature.

8.6 *Signer Role*— The signer role may be used to indicate which of several possible roles (for example, primary provider, consultant, care giver) a user is exercising for a particular signature. Different roles might have different capabilities and restrictions, as discussed in Section 10.

8.7 *Signer Organization*—The signer organization indicates the organization with which the signer is affiliated. (Note that this information may also be derived from the signer identity or location, depending on their structure).

8.8 *Document Link*— The document link is a reference to a prior or later version of the document. This attribute is present in an addendum or modification signature. The link is a document identifier, as described in Section 6.

8.9 *Biometric Information*—This attribute contains biometric measurements and other information, along with indications of the biometric and cryptographic algorithms used with the information.

8.10 *Annotation*—This attribute is a simple textual string. This may be used for a variety of purposes. In particular, a signer may use this to indicate "disagreement" with the document content.

9. Electronic Signature Technologies

9.1 *User Authentication versus Data Authentication*—Secure electronic signatures are dependent upon the availability of secure user authentication, but they are not interchangeable. Technologies that have been developed for user authentication include traditional password systems, cryptographic systems, and biometric identification methods. These methods for user authentication can be extended to provide electronic signatures by combining them with cryptographic techniques of various kinds. This standard addresses both issues, and care should be taken not to confuse the two.

9.2 *User Authentication:*

9.2.1 *Infometric User Authentication :*

9.2.1.1 *User Authentication with Passwords*—Passwords have proved to be a very effective means of proving identity when used properly, but they have severe limitations in the realm of electronic signatures.

9.2.1.2 Systems using passwords shall conform to the following requirements: (*1*) If a password is communicated over a network, then the password shall either be encrypted or physical controls shall be used on the network, or both, to prevent eavesdropping. (*2*) Passwords shall be chosen or generated, and used, in compliance with FIPS PUB 112, or Secure User Identification for Healthcare; Identification and Authentication by Passwords (**1**), or both.

9.2.1.3 For discussion of sound practices for password usage, see FIPS PUB 112. For a means of generating hard-to-guess passwords that are easier for humans to remember, see FIPS PUB 181.

9.2.1.4 The security that passwords provide is dependent on the manner in which they are used, but generally the common practice of simple user entry of passwords is inadequate to meet the intent of an electronic signature.

9.2.2 *User Authentication with Secret Key Cryptography:*

9.2.2.1 *Secret Key User Authentication* —To overcome some of the problems of passwords, secret pieces of information can be used in other ways. In particular, the problem of eavesdropping can be overcome by using a challenge-response form of user authentication, where a secret key is shared between the system and the user (or the server system and the user system), and the system challenges the user to answer challenges that they could only answer if they were in possession of the secret. This can be accomplished by the having the system choose a random number at login time, send it to the user, having the user encrypt the random number with the secret key, and returning the response to the system. The system can then compare this returned value with their own encrypted random value to validate that the user is in possession of the secret key. In this way the secret key itself never travels over a network, and is therefore not subject to eavesdropping. This technique is commonly used with a token held by the user to store their secret key and perform the encryption for them (see 9.2.4).

9.2.2.2 *User Authentication with Public Key Cryptography*—Challenge/response protocols can also be performed using public key cryptography to digitally sign a challenge. Use of public key cryptography eliminates the need to share a secret key between the user device and the host, greatly simplifying the key management requirements. Digital signatures, the technique used to provide authentication with public key cryptography, are described in greater detail in 7.3 and Section 10.

9.2.3 *Biometric User Authentication* —A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual. As a means to identify humans, they improve upon passwords by eliminating the need for the human to remember anything. In addition, biometrics can sometimes be used to identify humans without their knowledge, or without their having to do anything out of the ordinary. The range of features or actions that may be used is fairly large now, and new technologies can be expected to be developed in the future. Currently existing technologies, some of which are described in Appendix X2, include:

9.2.3.1 *Physical features:*

(1) Hand Geometry—the user places their right hand into a device that measures several distances such as the length and thickness of fingers.

(2) Retinal Scan—an infrared beam is used to take a measurement of blood vessel patterns in the retina of a user.

(3) Iris Scan—An infrared beam is used to measure certain features of the iris of a user.

(4) Fingerprint Patterns—the user places their finger on a scanner that measures the pattern of ridges on the finger.

(5) Facial Characteristics—measurements of certain characteristics of the face such as eye placement and nose length.

(6) DNA Sequence Characteristics—the sequence order of genes in human DNA can identify individuals with high probability.

9.2.3.2 *Behavioral Actions:*

(1) Voice Print—various measurements of speech patterns.

(2) Handwritten Signature Dynamics—the user can be asked to sign their signature with a special pen that measures acceleration and velocity of hand movements.

9.2.3.3 Biometric user identification can produce two kinds of errors, depending on whether the system fails to recognize a legitimate user (Type I error), or the system falsely identifies an illegitimate user (Type II error). It is often possible to make changes in the way measurements are made that can exercise some degree of control over the probabilities of such events. Even such simple characteristics as height and weight can be used to distinguish people at some coarse level of granularity, but clearly we would have a very high rate of Type II errors for such a method since there are many people who weigh 150 pounds. In any practical system, we would also incur some incidence of Type I errors, because the weight of an individual may vary considerably over time.

9.2.3.4 Biometric techniques vary in the reliability and expense of technology that is used for measuring them, and the degree to which they are prone to errors of Types I and II. In addition, some of the biometric techniques carry special advantages and disadvantages with them. For example,

(1) the use of fingerprints brings with it a certain amount of social stigma and suspicion because of their widespread use by law enforcement authorities.

(2) handwritten signature dynamics carry a higher level of acceptance by the lay public because of the obvious connection to the widespread practice of authenticating paper documents with a handwritten signature.

(3) voice print identification has an advantage that identification can be carried out remotely with a very common instrument, namely a telephone or microphone.

(4) retina and iris scanning technology generally shines beams of infrared light into the eye. While generally regarded by self-professed experts as safe even after repeated use, this is a practice that is viewed with great suspicion by the lay public.

9.2.3.5 A complete survey of the various technologies and evaluation of their effectiveness is beyond the scope of this document, in part because independent testing is in short supply, and technology is moving rapidly in this area. Further information on this subject may be obtained through the biometric consortium and (**2**).

9.2.3.6 Systems that rely on biometric features can be used in one of two modes, depending on whether a user first enters a code or string to look up their record, after which the problem is simply to verify the measurement against the stored template. If no such identifying information is supplied at the beginning of the procedure, then the system must compare the measurement against all of the stored templates in order to find a (hopefully unique) match. Since the comparison methods are often computationally challenging, and the database of templates may be fairly large in some situations, there are potential barriers to effective implementations.

9.2.4 *Token-based User Authentication* —User authentication is commonly based on one or more of the following attributes:

9.2.4.1 something you know,

9.2.4.2 something you possess, and

9.2.4.3 something you are.

9.2.4.4 The something you possess can generally be referred to as a token and may be something as simple as a card with a storage medium such as a magnetic strip. The term smart token is used to describe a small device (often the size of a credit card, but at least as small as a small handheld calculator) that contains a certain amount of processing power and is able to store and perform processing on information on behalf of the holder. Three examples of token technologies include:

(1) ISO has adopted standards [7816 and 10036] for smart cards the size of common credit cards that contain microprocessors, crude I/O channels, and small amounts of memory. CEN TC 251, CEN 224, ASTM E31.17, and ASC X3 are working on standards for application of smart cards to health care.

(2) The Personal Computer Memory Card Interface Association (PCMCIA) has defined a series of standards for small cards that can be plugged into computing devices.

(3) SmartDisk provides smart card capabilities on a 3.5 in. form factor that is inserted in a floppy disk drive and interacts with the host system using the operating system's disk driver software.

9.2.4.5 As mentioned in 9.2.4.4, smart tokens can be used to store secret pieces of information that are used as password or secret cryptographic keys. In addition, the token can be used to store biometric templates for identification of humans to the tokens.

9.3 *Data Authentication*—At the highest level, we can separate out the handwritten signature on paper from the notion of electronic signature, which is recorded as an electronic signal. Below this, we can break down electronic signatures into several types. This section discusses appropriate cryptographic mechanisms. A canonical representation for documents shall be specified for use by cryptographic mechanisms described in this section. In general, a document may be stored on an end system in a different form than the one in which it was generated. For example, if the document contains many numeric values, some systems may store them as integers, and others as text. Since signatures are computed over representations (encodings), rather than abstract values, there must be a specific representation the signature is computed over. Such a representation can be defined using Abstract Syntax Notation One (ASN.1) with an appropriate set of encoding rules, such as the Distinguished Encoding Rules specified in ISO 8825-1. As an added benefit, a number of existing ISO, ANSI, and de facto (PKCS) standards (notably X.509, ANSI X9.30 Part 3, and PKCS #7) are available which define ASN.1 structures for digital signatures.

9.3.1 *Digital Signatures:*

9.3.1.1 *Technology Overview*—Digital signatures are a cryptographic technique in which each user is associated with a pair of keys. One key (the private key) is kept secret, while the other key (the public key) is distributed to the potential verifiers of the user's digital signature. To sign a document, the document and private key are input to a cryptographic process which outputs a bit string (the signature). To verify a signature, the signature, the document, and the user's public key are input to a cryptographic process, which returns an indication of success or failure. Any modification to the document after it is signed will cause the signature verification to fail (integrity). If the signature was computed using a private key other than the one corresponding to the public key used for verification, the verification will fail (authentication).

9.3.1.2 *Allowable algorithms include:* (*1*) RSA, either as specified in X9.31 Part 1 (ISO 9796) or PKCS #1, or (*2*) DSS, as specified in ANSI X9.30 Part 1 (NIST FIPS PUB 186). The cited standards reference appropriate hash algorithm standards for use with the signature algorithms [15, 16].

9.3.1.3 Digital signatures meet the requirements for non-repudiation, integrity, interoperability, and independent verifiability. Specific signature standards, such as ANSI X9.30-3, define data formats that support multiple signatures, signature attributes, and countersignatures.

9.3.1.4 Additional system requirements.

9.3.2 *Private Key Protection:*

9.3.2.1 To support a true non-repudiation service, the user's private key shall be protected from disclosure to other users. The most secure way to protect the private key is to embed it in a tamperproof cryptographic module, which will perform the signature computation internally. Such modules might include smart cards, SmartDisks, and PCMCIA cards. Access to the signature function would require the user to authenticate himself to the module, using passwords, PINs, or biometric controls (even including graphic signature verification), or a combination thereof.

9.3.2.2 A less secure way to protect the private key is to encrypt it under a secret (for example, DES) key computed from a password entered by the user. (One such mechanism is described in PKCS #5: Password-Based Encryption.) The encrypted password is stored on removable media, like floppy disk, and decrypted when needed to perform a signature.

9.3.3 *Public Key Authentication*—To verify a signature, a user must obtain the signer's public key from a source that the user trusts. One such source is a (public key) certificate, which binds a user's name to his public key. Certificates are signed by a trusted issuer, the Certification Authority (CA). CAs are described in greater detail in Appendix X1.

9.3.4 *Digital Signature Representation* —A document may be signed by one or more users. Each user's signature and other information are contained in a separate signature structure. Each signature structure contains an indication of the certificate needed to validate the signature and a bit string containing the actual signature. Additionally, other information relevant to the particular signer would be included in an individual signature computation. This per-signer information would be included in the signature computation as signature attributes. A signature structure may also include per-signer information, which is not signed but merely appended to the signature structure (unsigned attributes). An important unsigned attribute is the countersignature. A countersignature is a signature on the signature structure in which it is found, rather than on the document itself. A countersignature thus provides proof of the order in which signatures were applied. Since the countersignature is itself a signature structure, it may itself contain countersignatures; this allows construction of arbitrarily long chains of countersignatures.

9.3.5 *Secret-Key Based Data Authentication:*

9.3.5.1 In symmetric (conventional) cryptography, the sender and recipient share a secret key. This key is used by the originator to encrypt a message and by the recipient to decrypt a message. It may also be used to authenticate a message by computing some function such as a Message Authentication Code (MAC) over the message, using the key; the recipient can be assured of the identity of the originator since only the originator and the recipient know the secret key used to compute the MAC. DES is an example of a symmetric algorithm.

9.3.5.2 Note the use of MACs requires the sender and receiver to share a secret key. This key must be distributed in a secure manner. Such approaches may not scale to large numbers of users as well as public key systems. Additionally, such systems generally do not provide true non-repudiation, since either the sender or receiver can compute the MAC. Some systems can provide non-repudiation, generally through hardware mechanisms that ensure a given key cannot be used to both generate and verify a MAC.

9.3.5.3 Non-repudiation may also be provided if the parties use symmetric cryptography to communicate evidence of a transaction (for example, a hash of a document) to a trusted third party that could retrieve and present such evidence in the event of a dispute. The identity of the originator and the integrity of the data must be ensured, which can be done with symmetric cryptography.

9.3.5.4 Typically the trusted third party would be a separate entity, not under control of the originator or the recipient. It might use cryptographic mechanisms to ensure that the authenticity and integrity of the evidence which it stores can be verified during the dispute resolution process.

10. Health Information Document Timestamps

10.1 To be valid, health information documents shall have explicit and accurate timestamps. Timestamps can relate to the document itself, or can be the time of a specific signature, or both. Health information documents need to support the following types of timestamps:

10.1.1 Event time,

10.1.2 Document creation time,

10.1.3 Signature time(s),

10.1.4 Document access times, and

10.1.5 Document modification times.

10.2 All systems shall support these timestamps. Event time can be set by the primary author or coauthor(s), or it can be derived from signature time. These times are to be supported, but the rules for establishing event time are system configurable. Note however, that the accuracy, security, and consistency of these timestamps will depend on having sufficiently robust methods for these system configurations.

10.3 A variety of timestamp mechanisms are available. They all convey timestamp information as signed or unsigned attributes in the signature structure. Timestamp mechanisms can be assessed in terms of a number of factors, including:

10.3.1 The precision of the system, or the resolution with which it can resolve a timestamp.

10.3.2 The conformance of the system to national or internationally accepted external notions of time.

10.3.3 The consistency of the system, that is, how well it can maintain a consistent notion of time (for example, does it ever go backwards?)

10.3.4 Scalability to large distributed networks.

10.3.5 The ability to verify the accuracy of a timestamp at a later date.

10.3.6 Resistance to malicious or inadvertent tampering by users or intruders, or both.

10.4 The system should adhere to the following requirements:

10.4.1 The system should have the ability to record timestamp information generated by the system as well as those generated by users and devices outside the system (for example, monitors or other computers). Whether a timestamp is generated by the system, an external device, or a user will depend on the type of timestamp and the policies of the organization.

10.4.2 The source of a timestamp, as well as the timestamp itself, should be recorded.

10.4.3 Timestamps entered into a system should be comparable to each other. In situations where an inconsistency is discovered (either by a user or the system) the ability should exist to either record an additional timestamp or to resolve the discrepancy.

11. Security

11.1 Electronic signatures are dependent upon, but separate from, computer system security and user authentication.

11.2 Security is the protection of a system and the data within the system from unauthorized access or modification.

11.3 User authentication is the process of verifying a claimed user identity as discrete and inviolate to a specific user.

11.4 User authentication in computer systems is based on a means of identifying individuals such as passwords, magnetic cards, numbers, and biometric systems based on fingerprints, retinal images, or other behavioral or physical identifiers.

11.5 Security and user authentication are essential to electronic signatures because the signature, once applied, irrevocably identifies the document as derivative from the individual(s) or device(s) whose signatures are attached to it. In order to ensure the authorship of the document is accurate, the system shall reliably identify the signer and ensure they are who they say they are.

11.6 For the purposes of this guide, security and user authentication will be assumed to be in place, to meet health information system standards, and to be inviolate in identifying a discrete individual. In other words, this guide will not concurrently set standards for security and authentication. It will be a requirement, however, for a system implementing this standard to also meet relevant security and authentication standards. This guide will, therefore, cite security and authentication standards and other documents based on work from other standards bodies.

11.7 Auditing of specific signature-related actions shall be performed as defined in the organization's security policy.

12. Keywords

12.1 accountability; authentication; authorization; biometric authentication; certificate; cryptography; data integrity; digital signature; electronic signature; non-repudiation; responsibility; timestamp; trusted third party; user identification

APPENDIXES

(Nonmandatory Information)

X1. DIGITAL SIGNATURE TECHNOLOGY

X1.1 Digital signatures are based on asymmetric (public key) cryptography, where different keys are used to encrypt and decrypt a message. Each user is associated with a pair of keys. To provide confidentiality, one key (the public key) is publicly known and is used to encrypt messages destined for that user, and the other (private) key is known only to the user and is used to decrypt incoming messages. Authentication can be provided using a public key system, too, using the concept of digital signatures described below. RSA PKCS #5 is the most well-known asymmetric algorithm. Since the public key need not (indeed cannot) be kept secret, it is no longer necessary to secretly convey a shared encryption key between communicating parties prior to exchanging confidential traffic or authenticating messages.

X1.2 Some asymmetric algorithms, like RSA, can also provide authentication and non-repudiation when used as follows: to sign data, the user encrypts it under his private key. To validate the data, the recipient decrypts it with the originator's public key. If the message is successfully decrypted, it must have been encrypted by the originator, who is the only entity that knows the corresponding private key.

X1.3 A digital signature is a piece of data appended to a data unit that allows the recipient to prove the origin of the data unit and to protect against forgery. Digital signatures are formed using asymmetric encryption algorithms as described above. To sign a message, it is first digested (hashed) into a single block using a one-way hash function. A one-way hash function has the property that, given the digest (hash), it is computationally infeasible to construct any message that hashes to that value, or to find two messages that hash to the same digest. The digest is encrypted with the user's private key, and the result is appended to the message as its signature. Separating the signature from the message reduces the amount of data to be encrypted to a single block. This is important since public key algorithms are generally substantially slower than conventional algorithms. The signature process also introduces redundancy into the message. Redundancy allows the recipient to detect unauthorized changes to the message. Most messages already contain sufficient redundancy to detect such a forgery (for example, English text, timestamps, etc.). The signature process adds additional redundancy, since the message must also hash to the specified digest.

X1.4 A digital signature provides the following security services:

X1.4.1 Integrity, since any modification of the data being signed will result in a different digest, and thus a different signature,

X1.4.2 Origin authentication, since only the holder of the private key corresponding to the public key used for validation could have signed the message, and

X1.4.3 (Support for) non-repudiation, that is, irrevocable proof to a third party that only the signer could have created the signature.

X1.5 *Public Key Certificates:*

X1.5.1 For a user to identify another user by his possession of a private key, the user shall obtain the other user's public key from a source he trusts. A framework for the use of public key certificates is defined in ISO 9594-8 (X.509). These basic certificates bind a user's name to a public key and are signed by a trusted issuer called a Certification Authority (CA). Besides the user's name and public key, the certificate contains the issuing CA's name, a serial number, and a validity period.

X1.5.2 Although ISO 9594-8 (X.509) does not impose any particular structure on the CAs, many implementations find it reasonable to impose a hierarchical structure in which each CA (in general) certifies only entities that are subordinate to it. Hence, a hierarchy of CAs can be set up, where the higher level CAs sign the certificates of the CAs beneath them, etc. The lowest level of CAs sign user certificates. At the top of this hierarchy are a relatively few CAs (perhaps one per country) that may "cross-certify" each other's public keys.

X1.5.3 Various security architectures define mechanisms to construct a certification path through the hierarchy to obtain a given user's certificate and all CA certificates necessary to validate it. These architectures share the common characteristic that a user need only trust one other public key in order to obtain and validate any other certificate. The trusted key may be that of the top-level CA (in a centralized trust model), or the local CA that issued the user's certificate (in a decentralized model).

X1.5.4 Certificates contain an expiration date. If it is necessary to cancel a certificate prior to its expiration date (for example, if the name association becomes invalid or the corresponding private key is lost or compromised), the certificate may be added to the CA's certificate revocation list (CRL) or "hot list." This list is signed by the CA and widely distributed, for example, as part of the CA's directory entry. Each entry contains the revoked certificate's serial number, a revocation time, and optionally a revocation reason and time of suspected compromise. The certificate remains on the hot list until its expiration date. A system will typically archive expired and revoked certificates and CRLs, in order to be able to verify signatures after the fact.

X1.5.5 Certificates for use with this standard are defined in ANSI X9.30-3 and X9.31-3.

X1.6 *Attribute Certificates:*

X1.6.1 Certain additional information concerning an entity or CA may need to be made available in a trusted manner. This information is placed in an attribute certificate (ANSI X9.45), which is signed by a CA in the same manner as the public key certificate. This is a separate structure for the following reasons:

X1.6.1.1 Proper separation of duties might require that a different CA issue the attribute certificate than issued the public key certificate. A central CA might rarely of itself possess the required security or authority to sign for all of a user's authorizations. Having separate CAs generate various types of attribute certificates distributes risks more appropriately.

X1.6.1.2 The defined attributes may not be required for all domains, networks, or applications. The need for these attributes (and for additional domain-specific attributes) is determined by each domain.

X1.6.1.3 The user's basic public key certificate remains X.509 compatible, allowing its use with other applications and allowing use of commercial products for certificate generation.

X1.6.2 Attribute certificates would be created on presentation of the proper credentials by the user. For example, the user would obviously present his public key certificate and prove he possesses the corresponding private key as one form of identification. Attribute certificates are linked to the user's basic public key certificate by referencing its serial number and are revoked by an identical CRL mechanism.

X1.7 *Authorization:*

X1.7.1 There may be a need, in the absence of bilateral agreements or system rules, to convey authorization information between systems. For example, one might receive a document with a single transcription signature on it, where in reality the originating system requires the signature of a physician (as author). ANSI X9.45 defines mechanisms to externalize user authorization information in attribute certificates. This would allow the recipient to:

X1.7.1.1 Ensure the document was authorized according to the originating system's rules (as defined in the attribute certificates), and

X1.7.1.2 Verify the originator's authorization policy is acceptable to the recipient.

X1.7.2 An authorization certificate is a particular type of attribute certificate, which explicitly expresses the rules for acceptance of signed documents. Authorization attributes indicate the authorizations, restrictions, and cosignature requirements for the subject of the certificate. In the case of health care information, such attributes would include, for example:

X1.7.2.1 The user type(s) of the certificate subject,

X1.7.2.2 The document types the subject may sign,

X1.7.2.3 The signature purposes the subject may use when signing a document, and

X1.7.2.4 Any other signatures that must be present for the document to be considered valid (authorized).

X1.7.3 ANSI X9.45 contains a variety of useful attributes for authorization; additional attributes specific to health care information are defined in Appendix X2. Other useful ANSI X9.45 concepts might include:

X1.7.3.1 Use of role names or user types as signature attributes.

X1.7.3.2 Combination of attributes into Boolean expressions (filters).

X1.7.3.3 A mechanism to delegate authorizations, both on a temporary basis (for example, "power of attorney" certificates), and when initially creating authorization certificates.

X1.7.3.4 Various receipt requirements (confirm-reception-to, verify-by), which are analogous to several of our current signature purposes.

X2. BIOMETRIC AUTHENTICATION

X2.1 This appendix presents an overview of various biometric technologies that can be used to meet the requirement for secure user authentication as part of the electronic signature process. A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual. As a means to identify humans, they improve upon passwords by eliminating the need for the human to remember anything. In addition, biometrics can sometimes be used to identify humans without their knowledge, or without their having to do anything out of the ordinary.[6]

X2.2 *Handwritten Electronic Signatures*—Handwritten signatures may be captured electronically, using image scanners, digitizers connected to standard desktop PCs, or pen computers. In the case of pen computers, the digitizer is an integral part of the unit, such that the pen leaves a trail of "electronic ink" as it writes on the display.

X2.2.1 *Antecedent Signing:*

X2.2.1.1 This is analogous to having a signature on a rubber stamp. In some systems, a bitmap of a signature (written previously on paper and scanned, or written on a digitizer) is stored away from the document in another location on the system. The document has a reference to this image, so that at view or print time, the image and document are logically merged. In other systems, the signature might be physically appended to and stored with the document.

X2.2.1.2 In the absence of cryptographic mechanisms, this method would appear to be a weak solution for some of the requirements. The portability of the document might be tied to portability of the graphical image. Also, the ability to represent the signed document as originally displayed would be lost if the graphical file were lost or corrupted. This "one signature fits all" approach would not meet the requirement for integrity; the signature would not be affected if a document were altered. Finally, as the fixing of the signature to a document does not necessarily involve the intervention of the signatory, the requirement for non-repudiation cannot be met.

[6] Currently, this appendix only deals with handwritten signature authentication, due to lack of contributions on other technologies. Section 9.2.3 lists various other biometric technologies.

X2.2.1.3 Antecedent signing, when used by itself, does not meet the requirement for secure user authentication.

X2.2.2 *Concomitant Signing*—This method is closer to pen and paper, where a signature is written directly on the document in question as and when required. Such "live" signing involves the use of a digitizer, which may be either peripheral or integral to a computer, as described above. Two methods are identified for capturing signatures on documents: sketch fields and signature verification.

X2.2.3 *Sketch Fields:*

X2.2.3.1 Here, signatures are captured and displayed by a "sketch field" that is included as part of the electronic document. When written in, sketch fields reproduce the pen's "ink" on screen or printer as a bitmap. This image of the signature so created is roughly the same as a signature written on paper, although the higher resolutions of laser printers (typically 300 dpi) provide better quality than on screens (typically 100 dpi).

X2.2.3.2 Being a concomitant approach, this method is seen as a stronger solution as compared with signatures incorporated by reference, because a fresh signature is required for each document. However, there is no integrity because the document can be altered without affecting the sketch field and its signature. Also, because (in the absence of cryptographic mechanisms) it is technically feasible to "lift" a sketch field's contents from one document to another, non-repudiation is a problem. Finally, authenticating the signature is difficult, especially as a signature forged by tracing would be identical to a true original.

X2.2.4 *Signature Verification:*

X2.2.4.1 Signature verification programs have been developed to capture and verify handwritten signatures entered onto pen-equipped computers. The purpose of signature verification is the evaluation of authenticity of a signature inscription.

X2.2.4.2 The capture mechanism is similar to that of sketch fields, except that signature dynamics (such as speed, acceleration, order, and direction of each pen stroke) are also recorded. By building such characteristics into a template, subsequent signatures can be verified for their authenticity based on earlier signing behavior. Typically, signature verification programs "learn" signing behavior using the first four or five signatures from an individual.

X2.2.4.3 Given that dynamic characteristics are invisible, the authenticity of a handwritten signature can be verified with a reliability that exceeds that of visual comparison of signatures on paper.[7] Signatures forged by tracing can be readily detected. Because a signature cannot be guessed, transcribed, or disclosed to unauthorized parties, the programs are considered to provide a biometric measurement of the signatory.

X2.2.4.4 The program verifies that a particular user signed a document by verifying that the signature characteristics in the biometric token conform to the user's signature stored in a template. The signature verification program returns this match as a percentage by comparing the signature with the template. The controlling program then records whether the signature match percentage does or does not exceed a predetermined threshold for authentication.

X2.2.4.5 Based on the threshold established for verification of the signature, a signing may be rejected as false and, therefore, the signatory prevented from access to the client application or from authenticating an electronic document. Therefore, an attempt made in a computer-based patient record system to sign a physician's signature falsely—for example, to obtain controlled substances illegally—is likely to be rejected.

X2.2.4.6 Two problems are inherent in signature verification. The first is described as false acceptance: the acceptance of another's signature rather than the signature stored in the template. Vendors describe that false acceptance is prevented through the establishment of a high threshold. The second, false rejection, is the rejection of the signature of the originator of the signature template. Signatures change over time. It is not uncommon for one's signature to change sufficiently over the period of a few months to prevent access to the client application or rejection of an attempt to authenticate a document. Vendors minimize false rejections by permitting updates to the user's template on a predetermined basis or when requested by the signatory.

X2.2.4.7 This technology meets the requirement for secure user authentication in Section 7, as well as the requirement for the logical manifestation of the signature (that is, the dynamic information contained in the biometric token).

X2.2.4.8 Signature verification programs can cryptographically bind the document to the signature characteristics, forming a biometric token which allows the signature verification process to be separated from the application. Mechanisms for performing this binding are discussed in 7.3.1 and 7.3.2. An archive of the biometric token might then be stored for future analysis if desired or required, for example, as evidence of whether the signing of an electronic record constitutes a legal writing in court.

[7] Note that, with conventional signatures, there are forensic attributes such as type of paper, color and chemistry of the ink, etc., that can increase their reliability beyond that of a simple visual comparison.

X3. TIMESTAMP TECHNOLOGIES

X3.1 *Timestamp Generation Systems:*

X3.1.1 Methods for generating timestamps can be broken down into several categories:

X3.1.1.1 Self-contained systems providing a local notion of time,

X3.1.1.2 Networked timestamp servers,

X3.1.1.3 Distributed systems with multiple timestamp servers, and

X3.1.1.4 Global timestamp systems.

X3.1.2 In a self-contained system, if the signer has access to a trustworthy time source, the signer could simply include the timestamp in the original signature calculation rather than requiring a timestamp from a third party. In such a case, the timestamp required for verification is conveyed as an unsigned attribute associated with the signer. When this method is used, the signature does not convey anything about the trustworthiness of the time source, making independent verification of this information problematic. Note also that the time of events in a medical records system may often need to be compared to the time of events that take place outside of the system (for example, the time when transportation of a patient began). For this reason it may be important for the local notion of time to be kept consistent with an external time source. Methods for doing so are discussed in X3.1.3.

X3.1.3 In small networked environments, systems may make use of a stand-alone timestamp server to sign documents (or other signatures), using a timestamp as a signature attribute. Trust in the timestamp may be established by a combination of trust in the security of the stand-alone server and either the CA hierarchy or the device certificate of the server. This offers the capability of having systems maintain a consistent notion of time across the entire network and is likely to be used in small networked environments where the client systems have no protection against tampering with their local clocks (for example, personal computers with only a single level of privilege for all users). Unfortunately, this approach introduces other problems:

X3.1.3.1 A party wishing to attack the system need only compromise the single server,

X3.1.3.2 A rather powerful machine may be required to satisfy the peak demand for timestamp services. For large networks, this may quickly become a performance bottleneck,

X3.1.3.3 If only a single timestamp server is used, then the entire network is dependent on this system and it becomes a single point of failure for the entire network, and

X3.1.3.4 The accuracy of the time server is not guaranteed by this method, but only that the server provided the timestamp.

X3.1.3.5 In order to address some of these problems, the client-server model can be extended to include a deeper hierarchy of peers, where machines that are unable to contact servers directly can exchange information with peers that have contacted servers more recently, and multiple servers are available to service the requests of the network. If more than one server is used, then the timestamps received from different servers are incomparable unless a method is used to synchronize the servers. This can be accomplished by having servers that mutually trust each other correct for drift of one or more faulty servers. By adding authentication mechanisms, it is also possible to add protection against malicious machines attempting to masquerade as legitimate servers.

X3.2 *Systems with Multiple Timestamp Servers:*

X3.2.1 Network time agreement protocols are accomplished by having machines exchange messages about their local notion of time and measure the round-trip time to exchange these messages. If one machine trusts the time of another machine, then it can calculate to high accuracy the time of the other machine and adjust its own clock accordingly. By continuing to exchange messages at irregular intervals, very high accuracy can be achieved between the two. One standard for such a protocol is described in Ref (**3**). Another alternative, based on a simplification of the Network Time Protocol discussed below, is described in Ref (**4**).

X3.2.2 The most widespread method of synchronizing clocks between computers is the Network Time Protocol (NTP), which is used by many machines connected to the Internet. A detailed definition and discussion of this standard protocol is given in Ref (**3**). NTP is a hierarchical protocol, in which several root servers are linked to very accurate clocks, and the information from them is fed out through the Internet in a relay fashion. Among the advantages of NTP are:

X3.2.2.1 It provides exceptional accuracy. For most sites on the Internet (a network comprising millions of machines), NTP provides accuracy within 50 milliseconds.

X3.2.2.2 NTP timestamps are sufficient to distinguish times over a period of 136 years. External mechanisms will need to be added in the year 2036 in order to extend the range of timestamps.

X3.2.2.3 The intrinsic limitation on the accuracy of NTP timestamps is 200 picoseconds, which should be sufficient for any foreseeable use.

X3.2.2.4 NTP is an open standard that allows machines of different architectures to synchronize clocks with each other.

X3.2.2.5 Implementations exist for all TCP/IP based networks, as well as Appletalk and Novell networks.

X3.2.2.6 It can be used to maintain consistent and accurate times over extremely large networks, where clients can be many hops from the servers.

X3.2.2.7 It includes provisions for optional rudimentary authentication between peers.

X3.2.2.8 Synchronization may be initiated by either clients or servers.

X3.2.2.9 The National Institute of Standards and Technology (NIST) in the USA operates three radio services for the dissemination of time information. Radio clocks are available for modest cost to sample one of these frequencies with accuracies to within about ten milliseconds (the others require more sophisticated technology). These systems are used as root servers to maintain time on the Internet. NIST also offers time services via modem dialup. Even higher accuracies of within about 100 nanoseconds can be achieved using Global Positioning Systems.

X3.3 *Authentication of Timestamp Information:*

X3.3.1 One disadvantage of NTP is that the optional authentication method specified in the standard uses DES encryption. This may cause problems with exportability from the US of implementations that support authentication. A more serious concern is that this method of authentication requires very inconvenient key management, since systems need to share common secret keys that are distributed by some external mechanism. It is relatively simple to apply digital signatures to NTP messages, however, greatly simplifying the problem of key management. Further analysis of NTP security considerations appears in Ref (**5**).

X3.3.2 A more secure global timestamp "notary" service is being offered as a proprietary technology by Surety Technologies of Chatham, New Jersey. They offer a service in which individual machines need not contact the central server for each timestamp, but a timestamp certificate is created that relates the one-way hash value of the document to a tree of hash values maintained by the timestamp server. The tree is maintained such that it is impossible to insert a document in the middle of the tree without detection, and the timestamps of documents from different sites are tied to each other in order to maintain a global notion of time. Trees are currently being closed off at resolutions of a few seconds, so that very accurate and reliable global sequencing of events can be maintained by this method. See (**6-8**) for more details.

X4. ORGANIZATIONAL POLICY ISSUES

X4.1 This appendix discusses the types of information that shall be determined by organizational policy and communicated between the originator and recipient of a signed document. The information might be dictated in some contractual form such as bilateral agreements or system rules. It also discusses the issue of the signer's accountability for various portions of the document and associated attributes.

X4.2 *Attribute Support*—The following document and signature characteristics shall be determined:

X4.2.1 Mandatory document attributes, which shall be present in every document,

X4.2.2 Optional document attributes, which may be present in a particular document,

X4.2.3 Prohibited document attributes, which shall never be present in a document,

X4.2.4 Mandatory signature attributes, which shall be present in every signature,

X4.2.5 Optional signature attributes, which may be present in a particular signature, and

X4.2.6 Prohibited signature attributes, which shall never be present in a signature.

X4.3 *Accountability:*

X4.3.1 As discussed in Section 6, the signer might not be accountable for all document and signature attributes. If these vary from document to document, the list of accountable attributes might be conveyed as part of the signer's signature attributes.

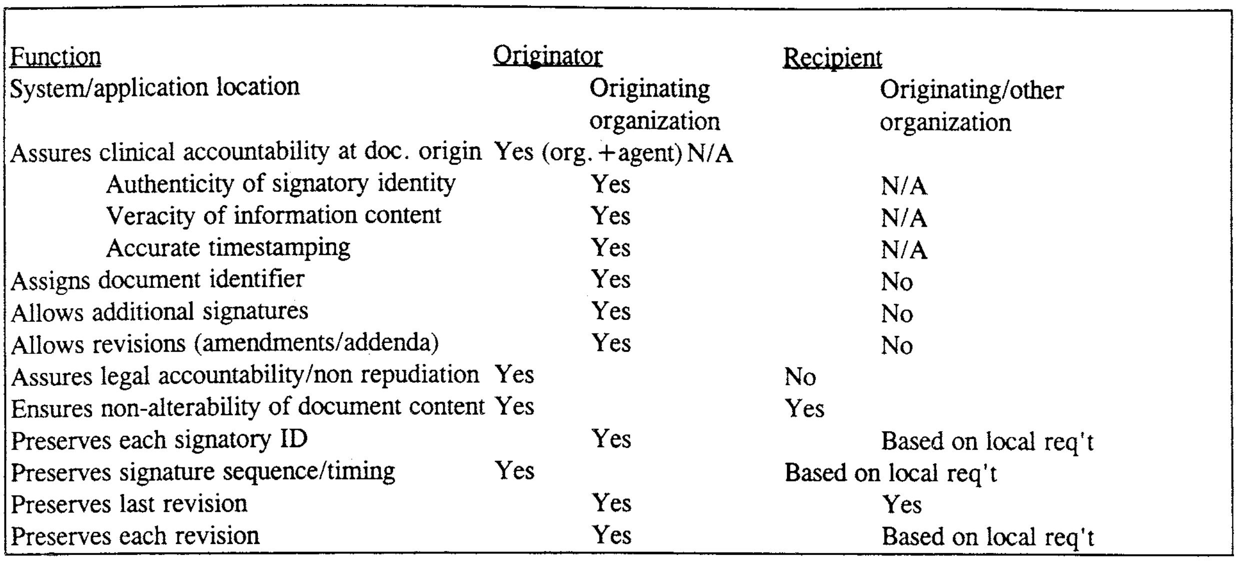
X4.3.2 Accountability for various functions typically varies with the role of the system or application. For example, in a traditional originator/recipient scenario, one might have the accountability characteristics illustrated in Fig. X4.1.

X4.3.3 To afford such individual accountability, the user shall be able to modify or denote document content, document attributes, and signature attributes to match their personal knowledge of relevant facts. Immediately prior to, or during the act of, signing the document, the user shall be able to:

X4.3.3.1 Directly modify document content, document attributes, and signature attributes (to match their knowledge of relevant facts),

X4.3.3.2 Note discrepancies in non-modifiable document content and attributes (for example, where the system clock is showing an incorrect date/time), and

X4.3.3.3 Note refusal to sign based on disagreement with previously recorded and signed document content (for example, where a countersignature is required, such as with verbal orders).



Function	Originator	Recipient
System/application location	Originating organization	Originating/other organization
Assures clinical accountability at doc. origin	Yes (org.+agent)	N/A
Authenticity of signatory identity	Yes	N/A
Veracity of information content	Yes	N/A
Accurate timestamping	Yes	N/A
Assigns document identifier	Yes	No
Allows additional signatures	Yes	No
Allows revisions (amendments/addenda)	Yes	No
Assures legal accountability/non repudiation	Yes	No
Ensures non-alterability of document content	Yes	Yes
Preserves each signatory ID	Yes	Based on local req't
Preserves signature sequence/timing	Yes	Based on local req't
Preserves last revision	Yes	Yes
Preserves each revision	Yes	Based on local req't

FIG. X4.1 Accountability Example

REFERENCES

(1) CEN TC251 WG6, "Secure User Identification and Authentication of Passwords."

(2) Holmes, J., Wright, L., and Maxwell, R., "A Performance Evaluation of Biometric Identification Devices," Sandia National Laboratories Technical Report #91-0276, June 1991.

(3) Postel, J., and Harrenstien, K., "Time Protocol," RFC 868, May 1983.

(4) Mills, D., "Simple Network Time Protocol (SNTP)," RFC 1361, August 1993.

(5) Bishop, M., "A Security Analysis of the NTP Protocol," Dartmouth College, June 1990. A shorter version was published as "A Security Analysis of the NTP Protocol Version 2," pp. 20–29, Proceedings of the Sixth Annual Computer Security Application Conference, December 1990.

(6) Haber, S., and Stornetta, S., "How to Timestamp a Digital Document," Proceedings of Crypto '90, Lecture Notes in Computer Science, Springer-Verlag, New York, Vol 357, 1991 , pp. 437–455.

(7) Cipra, B., "Electronic Time-Stamping: The Notary Public Goes Digital," *Science* , Vol 261, 9 July 1993, pp. 162–163.

(8) Bayer, D., Haber, S., and Stornetta, S., "Improving the Efficiency and Reliability of Digital Timestamping," in Sequences '91: Methods in Communication, Security, and Computer Science, ed. R. M. Capocelli, Springer-Verlag, 1991.

RELATED MATERIAL

AAMT, Position Paper on Providers' Signatures, 1993.

AHIMA, Position Statement on Authorship, 1993.

AIM, "SEISMED (Secure Environment for Information Systems in Medicine)."

American Bar Association, Science and Technology Section, Information Security Committee, "[Global] Digital Signature Guidelines with Model Legislation," March 1995 (draft).

ANSI, "X12.58 version 2: EDI Security Structures," July 1994 (draft).

ASTM E31.12, "Guide for Minimal Data Security Measures for the Protection of Medical Records," (in progress).

ASTM E31.17, "Standard for Access, Privacy and Confidentiality of Medical Records," (in progress).

ASTM E31.18, "Standard Specification for Health Data Cards" (in progress).

Baum, M., "Federal Certification Authority Liability and Policy—Law and Policy of Certificate-Based Public Key and Digital Signatures," NIST Pub. No. NIST-GCR-94-654; NTIS Pub. No. PB94-191-202 147-59 (1994).

CEN TC251 WG6, "User Authentication and Access Control," (in progress).

CEN TC251 WG6, "Security for Health Care Information Systems," (in progress).

FDA," Report on Electronic/Identification Signatures," 1994.

Health Care Financing Administration (HCFA), "42 CFR Ch. IV (10/1/91 Edition) Subchapter E—Standards and Certification," Section 482.24 (c)(1)(i) and (ii).

ISO/IEC, "ISO 7498-2 Information technology—Open systems interconnection—Security architecture," 1986.

ISO/IEC, "ISO 10181-2: Information technology—Open systems interconnection—Security framework in open systems—Part 2: Authentication framework," 1994.

JCAHO, "IM 7.9: 1995 Accreditation Manual for Hospitals."

JCAHO, "IM 7.1.2: 1995 Accreditation Manual for Home Care."

JCAHO, "IM 7.8: 1995 Accreditation Manual for Mental Health, Chemical Dependency, and Mental Retardation/Developmental Disabilities Services."

JCAHO, "IM 6.5: 1994 Accreditation Manual for Health Care Networks."

JCAHO," IM 2.4: 1994 Accreditation Manual for Long Term Care."

JCAHO," MR.1.9.10: 1994 Accreditation Manual for Ambulatory Health Care."

JCAHO, "PA.4.1: 1994 Accreditation Manual for Pathology and Clinical Laboratory Services."

Network Time Protocol (Version 3) Specification, Implementation, and Analysis. David L. Mills, University of Delaware. Network Working Group Request for Comments #1305, March 1992.

NIST, "FIPS PUB 140-1: Security Requirements for Cryptographic Modules," 1993.

Rivest, R., Shamur, A., and Adelman, L., "A Method for Obtaining Digital Signatures and Public Key Crypto Systems," Committee of the ACM, Vol 21, No. 2, February 1978, pp. 120–126.

RSA Laboratories, "PKCS #5: Password-Based Encryption Standard," 1993.

RSA Laboratories, "PKCS #9: Selected Attribute Types," 1993.

Trusted Health Information Systems, "Management Summary," November 30, 1994.

ASTM International takes no position respecting the validity of any patent rights asserted in connection with any item mentioned in this standard. Users of this standard are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard is subject to revision at any time by the responsible technical committee and must be reviewed every five years and if not revised, either reapproved or withdrawn. Your comments are invited either for revision of this standard or for additional standards and should be addressed to ASTM International Headquarters. Your comments will receive careful consideration at a meeting of the responsible technical committee, which you may attend. If you feel that your comments have not received a fair hearing you should make your views known to the ASTM Committee on Standards, at the address shown below.