



Standard Guide on Security Framework for Healthcare Information¹

This standard is issued under the fixed designation E 2085; 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 a framework for the protection of healthcare information. It addresses both storage and transmission of information. It describes existing standards used for information security which can be used in many cases, and describes which (healthcare-specific) standards are needed to complete the framework. Appropriate background information on security (and particularly cryptography) is included. The framework is designed to accommodate a *very large* (national or international), *distributed* user base, spread across many organizations, and it therefore recommends the use of certain (scaleable) technologies over others.

1.2 Electronic information exchange and sharing of data in has been the backbone of industries such as financial institutions for several years. Cost cutting measures and a real need for sharing of information are driving healthcare services toward increased use of computer-based information systems. One of the requirements for the ability to share and exchange healthcare information is that the information be protected.

1.3 Selection of standards was performed using the following criteria, which are described in more detail in 4.2.

1.3.1 Security requirements are defined in this framework, and (in some cases) in additional ASTM guidelines.

1.3.2 ASTM standard specifications are used to define protocols and message formats in support of interoperability.

1.3.3 Existing standards will be reused or extended whenever possible.

1.3.4 This framework does not address policy issues. ASTM Subcommittee E31.17 is writing standards that address these issues.

2. Referenced Documents

2.1 ASTM Standards:

E 1238 Specification for Transferring Clinical Observations Between Independent Computer Systems²

E 1384 Guide for Content and Structure of the Computer-Based Patient Record²

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 Management, Security, Confidentiality, and Privacy.

Current edition approved Oct. 10, 2000. Published November 2000. Originally published as E 2085-00. Last previous edition E 2085-00.

² *Annual Book of ASTM Standards*, Vol 14.01.

E 1762 Guide for Electronic Authentication of Healthcare Information²

E 1985 Guide for User Authentication and Authorization²

E 1986 Guide for Information Access Privileges to Health Information²

E 2084 Specification for Authentication of Healthcare Information Using Digital Signatures²

E 2086 Guide for Internet and Intranet Healthcare Security²
2.2 *IETF Standards*:³

RFC 1510 Kerberos Authentication Service

RFC 1777 Lightweight Directory Access Protocol (v2)

RFC 2251 Lightweight Directory Access Protocol (v3)

RFCs 1901–1910 Simple Network Management Protocol

RFC 1945 Hypertext Transfer Protocol

RFC 1964 Kerberos v5 GSS-API Mechanism

RFC 2025 GSS-API Simple Public Key Mechanism (SPKM)

RFC 2078 Generic Security Services Application Program Interface

RFC 2246 The TLS Protocol Version 1.0

RFC 2401 Security Architecture for the Internet Protocol

RFC 2402 IP Authentication Header

RFC 2403 The Use of HMAC-MD5-96 within ESP and AH

RFC 2404 The Use of HMAC-SHA-196 within ESP and AH

RFC 2406 IP Encapsulating Security Payload (ESP)

RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP

RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)

RFC 2409 The Internet Key Exchange (IKE)

RFC 2440 OpenPGP Message Format

RFC 2451 The ESP CBC-Mode Cipher Algorithms

RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

RFC 2259 Internet X.509 Public Key Infrastructure Operational Protocols—LDAPv2

RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol

RFC 2630 Cryptographic Message Syntax

RFC 2631 Diffie-Hellman Key Agreement Method

³ Available online at ftp://ds.internic.net.

RFC 2632 S/MIME Version 3 Certificate Handling
RFC 2633 S/MIME Version 3 Message Specification
RFC 2634 Enhanced Security Services for S/MIME

2.3 ISO Standards:⁴

ISO 8824-1 Specification of Abstract Syntax Notions One (ASN.1)
ISO 8825-1 Specification of Basic Encoding Rules for Abstract Syntax Notions One (ASN.1)
ISO/IEC 7498-2 Security Architecture
ISO/IEC 8879 Standard Generalized Markup Language (SGML)
ISO/IEC 9735 Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)—Application Level Syntax Rules (Parts 5–10)
ISO/IEC 9595 Information Technology—Open Systems Interconnection—Common Management Information Service Definition
ISO/IEC 9596 Information Technology—Open Systems Interconnection—Common Management Information Protocol Specification
ISO/IEC 10164-7 Information Technology—Open Systems Interconnection—Systems Management: Security Alarm Reporting Function
ISO/IEC 10164-8 Information Technology—Open Systems Interconnection—Systems Management: Security Audit Trail Function
ISO/IEC 11586 Generic Upper Layers Security (4 parts)
ISO/IEC 11577 Network Layer Security Protocol
ISO/IEC 10736 Transport Layer Security Protocol
ITU-T X.509 Directory Authentication

2.4 ANSI Standards:⁵

X3.92 Data Encryption Standard
X9.30 Part 1 Public Key Cryptography Using Irreversible Algorithms: Digital Signature Algorithm
X9.30 Part 2 Public Key Cryptography Using Irreversible Algorithms: Secure Hash Algorithm (SHA-1)
X9.31 Reversible Digital Signature Algorithms
X9.42 Management of Symmetric Keys Using Diffie-Hellman
X9.44 Key Establishment Using Factoring-Based Public Key Cryptography for the Financial Services Industry
X9.57 Certificate Management
X9.55 Extensions to Public Key Certificates and CRLs
X9.52 Triple DES Modes of Operation
X9.62 Elliptic Curve Digital Signature Algorithm
X12 Electronic Data Interchange
X12.58 Security Structures (version 2)
X.25 Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) Operating in the Packet Mode and Connected to Public Networks by Dedicated Circuits
X.500 Open Systems Interconnection: The Directory

2.5 Other Standards and Publicly Available Specifications:⁶

FIPS PUB 46-3 Data Encryption Standard
FIPS PUB 74 Guidelines for Implementing and Using the NBS Data Encryption Standard
FIPS PUB 81 DES Modes of Operation
FIPS 140-1 Security Requirements for Cryptographic Modules
FIPS PUB 180-1 Secure Hash Algorithm
FIPS PUB 186 Digital Signature Standard
IEEE 802.10 *Interoperable LAN/MAN Security (SILS)*, 1992–1996 (multiple parts)
NIST MISPC Minimum Interoperability Specification for PKI Components Version 1

3. Terminology

3.1 Definitions:

3.1.1 *algorithm*—a clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

3.1.2 *asymmetric cryptography*—cryptographic algorithm that uses two related keys, a public key and a private key; the two algorithm keys have the property that, given the public key, it is computationally infeasible to derive the private key.

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

3.1.4 *authorization*—the granting of rights.

3.1.5 *cipher text*—data in its enciphered form.

3.1.6 *clear text*—data in its original, unencrypted form.

3.1.7 *confidentiality*—the property that information is not made available to or disclosed to unauthorized individuals, entities, and processes.

3.1.8 *cryptography*—the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use, or a combination thereof.

3.1.9 *data integrity*—a property whereby data has not been altered or destroyed.

3.1.10 *decryption*—a process of transforming ciphertext (unreadable) into plain text (readable).

3.1.11 *digital signature*—a cryptographic transformation of data which, when associated with a data unit, provides the services of origin authentication, data integrity, and signer non-repudiation.

3.1.12 *encryption*—a process of transforming plain text (readable) into cipher text (unreadable) for the purpose of security or privacy.

3.1.13 *encryption key*—a binary number used to transform plain text into cipher text.

3.1.14 *gateway*—a computer system or other device that acts as a translator between two systems that do not use the same communications protocols, data formatting, structures, languages, or architecture, or a combination thereof.

⁴ Available from ISO, 1 Rue de Varembe, Case Postale 56, CH 1211, Geneva, Switzerland.

⁵ Available from American National Standards Institute, 11 W. 42nd St., 13th Floor, New York, NY 10036.

⁶ National Technical Information Service, U.S. Department of Commerce, Springfield, VA. <http://src.nist.gov> or www.ntis.gov



3.1.15 *non-repudiation*—this service provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party.

3.1.16 *plain text*—data in its original, unencrypted form.

3.1.17 *repudiation*—the denial by a user of having participated in part or all of a communication (see *non-repudiation*, which has the opposite meaning).

3.1.18 *replay*—the process of sending a previously sent message as a method of perpetrating a fraud.

3.1.19 *security association*—the relationship between two entities which allows the protection of information communicated between the entities.

3.1.19.1 *Discussion*—This relationship includes a shared symmetric key and security attributes describing the relationship. The security association is used to negotiate the characteristics of these protection mechanisms, but does not include the protection mechanisms themselves.

3.1.20 *session*—a logical relationship between two network endpoints that supports a user or network application.

3.1.21 *subnetwork*—a network segment usually with its own address.

3.1.22 *symmetric encryption*—encryption using a single key to encrypt and decrypt which both the sender and receiver hold privately.

3.1.23 *virtual private network*—a network using public data network or the Internet as a carrier that acts as if a dedicated point to point network.

3.1.23.1 *Discussion*—Cryptography is normally used to protect data.

3.2 *Acronyms: Acronyms:*

3.2.1 *AH*—Authentication Header

3.2.2 *API*—Application Programming Interface

3.2.3 *ASTM*—American Society for Testing and Materials

3.2.4 *ATM*—Asynchronous Transfer Mode

3.2.5 *CA*—Certificate Authority

3.2.6 *CMIP*—Common Management Information Protocol

3.2.7 *CMS*—Cryptographic Message Syntax

3.2.8 *CORBA*—Common Object Request Broker Architecture

3.2.9 *DSA*—Digital Signature Algorithm

3.2.10 *DES*—Data Encryption Standard

3.2.11 *EDI*—Electronic Data Interchange

3.2.12 *ESP*—Encapsulating Security Payload

3.2.13 *FTP*—File Transfer Protocol

3.2.14 *GSS*—Generic Security Services

3.2.15 *HMAC*—Hashed Message Authentication Code

3.2.16 *HTTP*—HyperText Transfer Protocol

3.2.17 *IDUP*—Independent Data Unit Protection

3.2.18 *IETF*—Internet Engineering Task Force

3.2.19 *IP*—Internet Protocol

3.2.20 *IPS*—Internet Protocol Suite

3.2.21 *IPSEC*—Internet Protocol Security

3.2.22 *KRA*—Key Release Agent

3.2.23 *LAN*—Local Area Network

3.2.24 *LDAP*—Lightweight Directory Access Protocol

3.2.25 *MD*—Message Digest

3.2.26 *MIME*—Multipurpose Internet Mail Extension

3.2.27 *MSP*—Message Security Protocol

3.2.28 *NLSP*—Network Layer Security Protocol

3.2.29 *OSI*—Open Systems Interconnection

3.2.30 *PCT*—Private Communications Technology

3.2.31 *PIN*—Personal Identification Number

3.2.32 *PKI*—Public Key Infrastructure

3.2.33 *PRNG*—Pseudo Random Noise Generator

3.2.34 *RFC*—Requests for Comment

3.2.35 *RSA*—Rivest, Shamir, and Adelman

3.2.36 *SHA-1*—Secure Hash Algorithm

3.2.37 *S-HTTP*—Secure HyperText Transfer Protocol

3.2.38 *S/MIME*—Secure/Multipurpose Internet Mail Extension

3.2.39 *SMTP*—Simple Mail Transfer Protocol

3.2.40 *SSL*—Secure Socket Layer

3.2.41 *TCP*—Transmission Control Protocol

3.2.42 *TLSP*—Transport Layer Security Protocol

3.2.43 *VPN*—Virtual Private Network

3.2.44 *WAN*—Wide Area Network

3.2.45 *WWW*—World Wide Web

4. Significance and Use

4.1 This guide presents a framework for securing healthcare information of all kinds. Specific existing standards are identified which accommodate many cases, and requirements for new standards are identified. An organization's security policy will determine when these standards are to be used, based on risk analysis.

4.2 Many standards have been defined by other standards bodies such as ISO, ITU, and the IETF. There are also a variety of de facto standards and publicly available specifications such as the PKCS documents from RSA Laboratories.⁷ This framework recommends appropriate existing standards where possible, using the following criteria:

4.2.1 High level requirements for security are defined in this framework. In some cases, guidelines defining additional requirements will be needed. Guide E 1762 is an example of such a guideline for authentication of healthcare information.

4.2.2 Formal standards (for example, ASTM "standard specifications") are only required where information is exchanged between systems, to ensure interoperability. These standards define protocols and message formats.

4.2.3 If there are no healthcare specific requirements for some security service, one or more existing standards will be recommended, as is.

4.2.4 Where existing healthcare standards (for example, HL7) use specific underlying protocols and technologies, security mechanisms already defined for those protocols will be identified and recommended.

4.2.5 Healthcare specific requirements will be met, if possible, by extending existing standards. Specification E 2084 is an example of this approach.

4.2.6 Preference is given to standards which have the greatest market acceptance and maturity.

4.2.7 Standards which involve the use of cryptography shall be, to the extent possible, algorithm-independent. This can be

⁷ Available from RSA Data Security, 100 Marine Parkway, Redwood City, CA 94065. <http://www.rsa.com>.



accomplished by, for example, signaling the algorithms used within the protocol or message format.

4.2.8 The total number of security standards needed will be minimized, subject to the previous requirements.

4.2.9 Policy issues are not addressed, although these technical standards shall accommodate any potential variations in policy allowed by other standards. Policy may be the subject of security standards produced by other groups, such as ASTM Subcommittee E31.17.

4.3 This guide assumes the standard distributed environment, including multiple heterogeneous systems, interconnected by a network. Regardless of the network protocols used, it is useful to separate functionality into the following three components:

4.3.1 *Semantics*—This includes the application data and behavior model. At this level, security is viewed as a pervasive service provided by the application's infrastructure. An application's security policy would define access rules for the data, as well as constraints on its behavior. These would be implemented using security mechanisms provided by the infrastructure, such as access control lists and secure communications protocols.

4.3.2 *Syntax*—This includes rules for encoding data for transport between systems (for example, ASN.1 basic encoding rules (ISO/IEC 8824 and 8825), HL7 message and field formats). Security mechanisms generally require some additional syntax. In many cases, an entire message or document can be encapsulated in a security envelope, leaving the original structure intact inside the envelope. While standardized encoding rules are also required for performing some cryptographic operations (such as digital signature), applications generally are free to use any syntax internally.

4.3.3 *Transport*—This includes movement of data (encoded using some syntax) between systems. This typically involves adding more data elements related to the communications, for example, message headers and session identifiers.

4.4 This document is divided into several parts. Section 5 presents a security overview including threats and security services. Section 6 presents Communication Security. Local Security is presented in Section 7.

5. Security Overview

5.1 This section presents an overview of the threats addressed by a security architecture, as well as the services and mechanisms used to counter these threats. Many of these threats attack information in transit between systems (particularly those connected using open networks), and we use the generic term *message* to refer to any such data.⁸ A description of the security services and mechanisms used to counter various threats and the placement of these security services in the OSI model is provided in the OSI Security Architecture (ISO/IEC 7498-2).

5.2 The following subsections discuss threats to a system, and appropriate security services to counter these threats.

Detailed discussions of two particularly important security tools (access control mechanisms and cryptography) are also included.

5.3 *Threats*—This section describes the principal threats to a system. In some cases, security services can prevent an attack; in other cases, they merely detect an attack.

5.3.1 *Masquerade* occurs when an entity successfully pretends to be another entity. This includes impersonation of users or system components, as well as falsely claiming origination or acknowledging receipt of a message or transaction. For example, an adversary might masquerade as a hospital employee to gain access to medical records. Masquerade, then, facilitates the following described attacks:

5.3.2 *Modification of Information* can include modification of message or data content, as well as destruction of messages, data, or management information. The adversary in 5.3.1 could potentially modify medical records.

5.3.3 *Message Sequencing* threats occur when the order of messages is altered. Such threats include replay, pre-play, and delay of messages, as well as reordering of messages. The adversary might capture a password message when a legitimate user logs on, and later replay it to masquerade as that user.

5.3.4 *Unauthorized Disclosure* threats include revealing message contents or other data, as well as information derived from observing traffic flow, as well as revealing information held in storage on an open system. While masquerading as a legitimate user, the adversary can access information for which he is not authorized.

5.3.5 *Repudiation* occurs when a user or the system denies having performed some action, such as origination or reception of a message. For example, a user might deny having modified a portion of the medical record.

5.3.6 *Denial of Service* threats prevent the system from performing its functions. This may be accomplished by attacks on the underlying communications infrastructure, attacks on the underlying applications, or by flooding the system with extra traffic.

5.4 *Security Services*—The following services protect against the threats described in 5.3.1-5.3.6:

5.4.1 *Peer Entity Authentication* provides proof of the identity of communicating parties. On a single system, users are authenticated during logon. For distributed environments, various types of authentication exchanges have been discussed in the literature; most are based on digital signatures or other cryptographic mechanisms.

5.4.2 *Data Origin Authentication* counters the threat of masquerade, and is provided using digital signatures or other cryptographic integrity mechanisms.

5.4.3 *Access Control* counters the threat of unauthorized disclosure or modification of data. This is particularly appropriate on an end system. A variety of access control strategies can be found in Guide E 2086, Ford,⁸ and Menezes et al.⁹

5.4.4 *Confidentiality* counters the threat of unauthorized disclosure, particularly during the transfer of information. Confidentiality can be applied to entire messages or to selected

⁸ Ford, Warwick, *Computer Communications Security: Principles, Standard Protocols and Techniques*, Prentice Hall, 1994.

⁹ Menezes, Alfred, van Oorschot, Paul C., Vanstone, Scott A., *Handbook of Applied Cryptography*, CRC Press, 1997.