



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

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

¹ This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.20 on Data and System Security for Health Information.

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.

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