



Standard Specification for Authentication of Healthcare Information Using Digital Signatures¹

This standard is issued under the fixed designation E 2084; 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 specification covers the use of digital signatures to provide authentication of healthcare information, as described in Guide E 1762. It describes how the components of a digital signature system meet the requirements specified in Guide E 1762. This includes specification of allowable signature and hash algorithms, management of public and private keys, and specific formats for keys, certificates, and signed healthcare documents.

1.2 This specification should be read in conjunction with Guide E 1762, which describes the scope of, and requirements for, authentication of healthcare information. This specification describes one implementation (digital signatures) that meets all of the requirements of Guide E 1762. It does not prescribe any particular policy regarding which documents shall be authenticated, and by whom.

2. Referenced Documents

2.1 ASTM Standards:

E 1762 Guide for Electronic Authentication of Healthcare Information²

2.2 ANSI Standards:³

X9.30 Part 2: Public Key Cryptography Using Irreversible Algorithms: Secure Hash Algorithm (SHA-1)

X9.31 Reversible Digital Signature Algorithms

X9.55 Extensions to Public Key Certificates and CRLs

X9.57 Certificate Management

X9.62 Elliptic Curve Digital Signature Algorithm

2.3 ISO Standards:⁴

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

ISO 8824–1 1993: Specification of Abstract Syntax Notation One (ASN.1)

ISO 8825–1 1993: Specification of Basic Encoding Rules for ASN.1

ISO 9796 1991: Digital Signature Scheme Giving Message Recovery

ISO 10166 1991: Document Filing and Retrieval (DFR)

2.4 Internet Standards:⁵

RFC 2630 Cryptographic Message Syntax

2.5 Other Documents:⁶

RSA Laboratories, “PKCS #1: RSA Encryption Standard (version 1.5),” November 1993

RSA Laboratories, “PKCS #5: Password Based Encryption (version 1.5),” November 1993

RSA Laboratories, PKCS #6: Extended Certificate Syntax Notation

RSA Laboratories, “PKCS #7: Cryptographic Message Syntax (version 1.5),” November 1993

RSA Laboratories, PKCS #9: Selected Attribute Types

ITU-T X.501 Information Technology Open Systems Interconnection—The Directory: Models

3. Terminology

3.1 Definitions:

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

3.1.2 *authentication (data origin)*—corroboration that this source of data received is as claimed.

3.1.3 *authentication (user)*—provision of assurance of the claimed identity of an entity.

3.1.4 *certificate (public key)*—digitally signed data structure that binds a user’s identity to a public key.

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

3.1.6 *digest*—result of applying a one-way hash function to a message.

3.1.7 *digital signature*—data associated with, 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.

¹ This specification 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 April 10, 2000. Published June 2000.

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

³ Available from American National Standards Institute, 11 W. 42nd St., 13th Floor, New York, NY 10036.

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

⁵ Available at <http://www.ietf.org>.

⁶ Available from RSA Data Security, 100 Marine Parkway, Redwood City, CA 94605.

