



## Standard Practice for Healthcare Certificate Policy<sup>1</sup>

This standard is issued under the fixed designation E 2212; 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 practice covers a policy (“the policy”) for digital certificates that support the authentication, authorization, confidentiality, integrity, and nonrepudiation requirements of persons and organizations that electronically create, disclose, receive, or otherwise transact health information.

1.2 This practice defines a policy for three classes of certificates: (1) entity certificates issued to computing components such as servers, devices, applications, processes, or accounts reflecting role assignment; (2) basic individual certificates issued to natural persons involved in the exchange of health information used for healthcare provisioning; and (3) clinical individual certificates issued to natural persons and used for authentication of prescriptive orders relating to the clinical treatment of patients.

1.3 The policy defined by this practice covers: (1) definition of healthcare certificates, healthcare certification authorities, healthcare subscribers, and healthcare relying parties; (2) appropriate use of healthcare certificates; (3) general conditions for the issuance of healthcare certificates; (4) healthcare certificate formats and profile; and (5) requirements for the protection of key material.

1.4 The policy establishes minimum responsibilities for healthcare certification authorities, relying parties, and certificate subscribers.

### 2. Referenced Documents

#### 2.1 ASTM Standards:

E 2084 Specification for Authentication of Healthcare Information Using Digital Signatures<sup>2</sup>

E 2086 Guide for Internet and Intranet Healthcare Security<sup>2</sup>

#### 2.2 Other Documents:

Public Law 104-191, Aug. 21, 1996, Health Insurance Portability and Accountability Act of 1996<sup>3</sup>

RFC 2527—Internet X.509 Public Key Infrastructure Cer-

tificate Policy and Certification Practices Framework, P-KIX Working Group Internet Draft, January 3, 2002<sup>4</sup>  
RFC 2560—Internet X.509 Public Key Infrastructure Online Certificate Status Protocol, OCSP, June 1999<sup>5</sup>

### 3. Terminology

3.1 *Certificate and Related Terms*—A certificate, also referred to as a digital certificate or public key certificate, binds a public key value to information identifying the entity associated with the use of a corresponding private key. An entity may be an individual, organization, account, role, computer process, or device. The entity identified within the certificate is referred to as the certificate subject. The certificate is typically used to verify the digital signature of the certificate subject or to encrypt information for that subject. The reliability of the binding of a public key to a certificate subject is asserted by the certification authority (CA) that creates, issues, and distributes certificates. Certification authority is synonymous with certificate authority. Parties that depend on the accuracy of information in the certificate are referred to as relying parties. Certificate users are the collective relying parties and subscribers.

#### 3.2 Certificate Policy:

3.2.1 The X.509 standard defines a certificate policy (CP) as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.” For example, a particular certificate policy might indicate the type of certificate applicable for authenticating electronic data interchange transactions for the trading of goods within a specified price range. In contrast, Practice E 2212 addresses rules for certificates that support the authentication, authorization, confidentiality, integrity, and nonrepudiation requirements of persons and organizations that electronically create, disclose, receive, or otherwise transact health information.

3.2.2 Certificates contain a registered certificate policy object identifier (OID) that the relying party may use to decide whether a certificate may be trusted for a particular purpose. The OID registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the OID

<sup>1</sup> This practice 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 Nov. 10, 2002. Published January 2003. Originally approved in 2002. Last previous edition approved in 2002 as E 2212-02.

<sup>2</sup> *Annual Book of ASTM Standards*, Vol 14.01.

<sup>3</sup> Available at <http://aspe.hhs.gov/admsimp/pl104191.htm>.

<sup>4</sup> Available at [www.ietf.org/html.charters/pkix-charter.html](http://www.ietf.org/html.charters/pkix-charter.html).

<sup>5</sup> Available at <http://www.ietf.org/rfc/rfc2560.txt>.