



# Standard Guide for User Authentication and Authorization<sup>1</sup>

This standard is issued under the fixed designation E 1985; 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 mechanisms that may be used to authenticate healthcare information (both administrative and clinical) users to computer systems, as well as mechanisms to authorize particular actions by users. These actions may include access to healthcare information documents, as well as specific operations on those documents (for example, review by a physician).

1.2 This guide addresses both centralized and distributed environments, by defining the requirements that a single system shall meet and the kinds of information which shall be transmitted between systems to provide distributed authentication and authorization services.

1.3 This guide addresses the technical specifications for how to perform user authentication and authorization. The actual definition of who can access what is based on organizational policy.

## 2. Referenced Documents

### 2.1 ASTM Standards:

E 1762 Guide for Electronic Authentication of Healthcare Information<sup>2</sup>

PS 100 Provisional Specification for Authentication of Healthcare Information Using Digital Signatures<sup>2</sup>

### 2.2 ANSI Standard:

X9.45 Enhanced Management Controls Using Digital Signatures and Attribute Certificates<sup>3</sup>

### 2.3 ISO Standard:

ISO 10181-3 1994: Security Frameworks in Open Systems—Access Control Framework<sup>4</sup>

### 2.4 Other Standards:

ECMA1-219 Authentication and Privilege Attribute Security Applications with Related Key Distribution Functions<sup>5</sup>

FIPS PUB 112 Password Usage<sup>6</sup>

FIPS PUB 181 Automated Password Generator<sup>6</sup>

FIPS PUB 190 Guideline for Use of Advanced Authentication Technology Alternatives<sup>6</sup>

## 3. Terminology

### 3.1 Definitions:

3.1.1 *access control list*—a piece of access control information, associated with a target, that specifies the initiators who may access the target.

3.1.2 *capability*—a piece of access control information, associated with an initiator, which authorizes the holder to access some target.

3.1.3 *claimant*—party requesting authentication; may be a person or a device.

3.1.4 *initiator*—an entity (for example, a user) who requests access to some object.

3.1.5 *principal*—legitimate owner of an identity.

3.1.6 *security label*—access control information bound to initiators and targets. The initiator and target labels are compared to determine if access is allowed.

3.1.7 *target*—an entity (for example, a file or document) that may be accessed by an initiator.

3.1.8 *verifier*—another party seeking to authenticate principal.

### 3.2 Acronyms:

3.2.1 *ACI*—Access Control Information

3.2.2 *ACL*—Access Control List

3.2.3 *ADF*—Access Control Decision Function

3.2.4 *ADI*—Access Control Decision Information

3.2.5 *AEF*—Access Control Enforcement Function

3.2.6 *PIN*—Personal Identification Number

## 4. Significance and Use

4.1 This guide has three purposes:

4.1.1 To serve as a guide for developers of computer software that provides or makes use of authentication and authorization processes,

4.1.2 To serve as a guide to healthcare providers who are implementing authentication and authorization mechanisms, and

<sup>1</sup> This guide is under the jurisdiction of ASTM Committee E-31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.20 on Data System Security for Health Information.

Current edition approved Oct. 10, 1998. Published November 1998.

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

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

<sup>4</sup> Available from ISO, 1 Rue de Varembe, Case Postale 56, CH 1211, Geneve, Switzerland.

<sup>5</sup> Available from ECMA.

<sup>6</sup> Available from National Technical Information Service, U.S. Department of Commerce, Springfield, VA. <http://csrc.nist.gov> or [www.ntis.gov](http://www.ntis.gov).