Designation: E 1985 – 98

An American National Standard

Standard Guide for User Authentication and Authorization[1]

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[2]

PS 100 Provisional Specification for Authentication of Healthcare Information Using Digital Signatures[2]

2.2 *ANSI Standard:*

X9.45 Enhanced Management Controls Using Digital Signatures and Attribute Certificates[3]

2.3 *ISO Standard:*

ISO 10181-3 1994: Security Frameworks in Open Systems—Access Control Framework[4]

2.4 *Other Standards:*

ECMA1-219 Authentication and Privilege Attribute Security Applications with Related Key Distribution Functions[5]

FIPS PUB 112 Password Usage[6]

FIPS PUB 181 Automated Password Generator[6]

FIPS PUB 190 Guideline for Use of Advanced Authentication Technology Alternatives[6]

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

[1] 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.

[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, Geneve, Switzerland.

[5] Available from ECMA.

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

4.1.3 To be a consensus standard on the design, implementation, and use of authentication and authorization mechanisms.

4.2 Additional standards will define interoperable protocols and message formats that can be used to implement these mechanisms in a distributed environment, using specific commercial technologies such as digital signatures.

5. User Authentication

5.1 Authentication ensures the identity of a user. The legitimate owner of an identity is known as a *principal*. Authentication occurs when a *claimant* has presented a principal's identity and claims to be that principal. Authentication allows the other party (*verifier*) to verify that the claim is legitimate.

5.2 *Requirements*:

5.2.1 Users shall be authenticated for access to health information.

5.2.2 Users may be authenticated at the system, subsystem, application, or medical record level.

5.2.3 Users shall be authenticated by one or more of the following methods based on organizational policy:

5.2.3.1 Claimant demonstrates knowledge of a password, or the like,

5.2.3.2 Claimant demonstrates possession of a token, or something similar,

5.2.3.3 Claimant exhibits some physical characteristic, like a fingerprint, and

5.2.3.4 Cryptographic techniques.

5.2.4 Remote access to health information shall be mutually authenticated.

5.2.5 Determination of which method or methods to use for authentication shall be based on a risk assessment and organizational policy.

5.2.6 For accountability purposes, authentication shall be based upon an individual principal rather than upon a role.

5.3 *Knowledge*:

5.3.1 *Password or Personal Identification Number*:

5.3.1.1 In any environment, a user can be authenticated using a password or a personal identification number (PIN). The claimant shall enter a password or PIN for authentication purposes. The verifier shall then verify the password or PIN of the claimant.

5.3.1.2 The password or PIN shall be protected against disclosure. For guidelines on password generation and usage see FIPS PUB 112.

5.3.1.3 In a multiple system environment, a single password or PIN may be used for authentication.

5.3.2 *Challenge-Response*—Password or PIN-based schemes may be augmented by the challenge-response mechanism. In challenge-response, as part of the authentication protocol, the verifier sends the claimant a non-repeating value (challenge) in advance. The claimant sends a response to the verifier based on the challenge.

5.4 *Possession*:

5.4.1 The user or claimant shows possession by presenting a physical object or token that is unique to the principal or claimant. The token shall contain information unique to the principal or claimant. The claimant shall present the token as proof of identity. A password or PIN may be used to access information on token. The verifier shall then verify the token of the claimant.

5.4.2 The information shall be protected against duplication or theft.

5.4.3 Determination of which type of form factor may be used is based on risk assessment and organizational policy.

5.4.4 The form factors may include but are not limited to the following:

5.4.4.1 Smart Card,

5.4.4.2 PCMCIA,

5.4.4.3 Diskettes, and

5.4.4.4 Hand held password or challenge response generators.

5.4.5 The form factors may also be used for cryptographic techniques.

5.5 *Physical Characteristic*:

5.5.1 Certain physical features of the human body are relatively unique to an individual. These features are called biometrics. Biometric authentication is the measurement of a unique biological features used to verify the claimed identity of a principal. The claimant shall present the biometric as proof of identity. The biometric may be stored on a token. A password or PIN may be used to access the biometric. The verifier shall then verify the biometric of the claimant.

5.5.2 The biometric shall be protected against duplication or theft.

5.5.3 Determination of which type of biometric may be used is based on risk assessment and organizational policy.

5.5.4 These biometrics include but are not limited to the following:

5.5.4.1 Fingerprints,

5.5.4.2 Voice recognition,

5.5.4.3 Retinal scan,

5.5.4.4 Hand geometry,

5.5.4.5 Signature dynamics or recognition, and

5.5.4.6 Facial characteristics.

5.6 *Cryptographic Techniques*:

5.6.1 Authentication using cryptographic techniques are based on the principle of convincing a verifier that because a claimant possesses some secret key, the claimant is the principal claimed. Symmetric or public key techniques may be used.

5.6.2 *Symmetric Key*— The principal and the verifier shall share a symmetric key. The claimant shall either encrypt or seal the information using that key. If the verifier can successfully decrypt or verify that the seal is correct, then the claimant is the principal claimed to be. A non-repeating value may also be used as part of the information encrypted.

5.6.3 *Public Key*—The principal shall have a public/private key pair. The claimant digitally signs a challenge using his private key. The verifier checks the digital signature, using the public key of the principal. If the signature checks correctly, then the claimant is the principal that he claimed to be. A non-repeating value may also be used as part of the information signed. See also 5.3.2.

5.6.4 A trusted on-line server may be used for authentication. One of the following methods may be used: