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.

Copyright © ASTM International, 100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA 19428-2959, United States.

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:

5.6.4.1 The claimant shall encrypt or seal the health information with his or her key. A separate exchange with the authentication server shall be used for verification. The verifier and the authentication server shall use a shared key.

5.6.4.2 The claimant shall first conduct an exchange with the authentication server to obtain a ticket which is then passed to the verifier. The exchange between the claimant and authentication server shall be protected using a shared key. The ticket shall be constructed in such a way that will be acceptable only to an entity knowing the shared key between the verifier and the authentication server. An example of this is the Kerberos system.

5.6.5 When using the public key cryptography, an off-line server may be used for authentication. Verifiers shall need to obtain the certified public keys of principals and certificate revocation lists.

6. Authorization

6.1 *Requirements*:

6.1.1 Three types of authorization are required based on organizational policy:

6.1.1.1 Users shall be authorized to access (read or write) healthcare information documents;

6.1.1.2 Users shall be authorized to perform application-specific actions on a document (for example, physician review); and

6.1.1.3 Users shall be able to determine whether all necessary actions have been performed on the document, and whether the users performing these actions were allowed to do so, according to any rules and limits agreed to by the parties involved. For example, it may be a requirement that documents shall be reviewed by a physician prior to inclusion in the medical record.

6.1.2 A user's application-specific action on a document will be indicated using an electronic signature, as defined in Guide E 1762. Particular actions are indicated using signature purposes. Thus, signatures are applied in 6.1.1.2, and verified in 6.1.1.3. Generic access as described in 6.1.1.1 may be indicated using signatures, but this is not a requirement. This type of access may be needed to perform the specific actions of 6.1.1.2.

6.2 *Access Control*:

6.2.1 In a distributed environment, the following entities can be identified: the *initiator* wishes to access some object: the *target*. Access is mediated by an *access control enforcement function* (AEF), that uses an *access control decision function* (ADF) to determine whether access is to be granted. This decision is based on *access control decision information* (ADI) associated with the initiator, the target, the access request, and the context within which access is taking place. In a single system, access control is typically provided by the operating system, using standard process separation mechanisms. In a distributed environment, each of the four entities above may actually reside on a different system. Furthermore, each entity may be under the control of a different security domain or policy, so that translation of access control information (for example, user identities or roles) may be required. Although this guide does not dictate where each entity resides, it may be possible to make use of existing operating system access control mechanisms if the AEF and ADF reside on the same system as the target.

6.2.2 A variety of access control mechanisms have been defined, each of which is appropriate for particular environments. These include:

6.2.2.1 *Access control lists* (ACLs) are associated with a target and list the initiators which may access the target. ACLs might list individual user identities, as well as names of groups of users, and roles. Using groups and roles can minimize the size of the ACL. Many operating systems support ACLs. In a distributed environment, some method for verifying the identity of a remote initiator (for example, a public key certificate) is needed in order to provide remote access. ACLs are particularly appropriate when the number of targets is very large compared to the number of initiators.

6.2.2.2 *Capabilities* are associated with an initiator and specify the targets that may be accessed. Targets might be combined into groups in order to minimize the size of capabilities. In some cases (for example, a patient record), targets are hierarchically structured so that a capability might grant access to the "root" object and all subordinates. In other cases, independent targets (for example, all patients on a ward) can be combined into a group, as discussed below. Few operating systems implement capabilities. However, in a distributed environment, there is a great deal of work using certificates to bind access control and other information to a user's identity (see, for example, ANSI X9.45). Such certificates can be used to specify such capabilities.

6.2.2.3 *Security labels* are associated with both the initiator and the target and are compared by the ADF to determine if access is allowed. Labels were developed for the military environment and typically contain a security classification. An initiator may, then, read a target if the initiator's classification dominates (is greater than) that of the target. Labels are useful if there are many initiators and targets, but only a coarse granularity of access (that is, a classification) is needed.

6.2.2.4 The mechanisms in 6.2.2.1-6.2.2.3 may, of course, be combined, so that, for example, a user shall have an appropriate classification, and be on an ACL, in order to access a file.

6.2.3 Access control policies may be rule-based, in which case the policy is specified and enforced by the authority responsible for a security domain, or identity-based, in which case individual users control access to their own information. Rule-based policies may be automatically enforced; one example is a multi-level security policy using classifications. Non-hierarchical policies may be constructed by assigning initiators and targets to compartments. Note that in either case, only a coarse granularity of access is provided. Identity-based policies may be implemented with ACLs and capabilities, and provide a much finer granularity of access. A policy might also take into account the value of the data being protected or might require multiple users to agree to grant access.

6.2.4 Regardless of the access control policy or mechanism, the ADF bases its decision on the following data:

6.2.4.1 *Privilege attributes* are associated with the initiator. The most common privilege attribute is the initiator identity.

Other attributes might include user roles or groups of which the user is a member. Rule-based policies would associate a security label with the initiator. The following attributes from ECMA-219 are useful in labels, and in capabilities, for grouping initiators and targets together.

6.2.4.2 The *compartment attribute* controls access as follows: the initiator and target each have an associated list of compartments; and the initiator is granted access if all of the target's compartments are in the initiator's list as well.

6.2.4.3 The *need-to-know attribute* controls access as follows: the initiator and target each have an associated list of need-to-know attributes; and the initiator is granted access if any of the target's compartments are in the initiator's list as well.

6.2.4.4 *Control attributes* are associated with the target. These include ACLs and labels, as well as compartment and need-to-know attributes.

6.2.4.5 ADI retained from previous accesses, for example, the user identity retained from login.

6.2.4.6 Attributes of the access request itself, for example, the type of operation requested.

6.2.4.7 The context of the transaction, for example, time of day, location of initiator, and level of authentication of initiator.

6.2.5 In all cases, it is necessary to allow emergency access by initiators that may not currently have access to the target. If the appropriate ACI cannot be immediately updated, the access shall, at a minimum, be recorded in the audit trail.

6.2.6 While this guide does not require a particular policy or mechanism for access control, the following controls are easily implemented using current technology: Access control (both ADF and AEF) are performed on the target system, and implemented using ACLs (generally supported by the operating system). Groups and roles should be used to minimize the size of the ACLs, and compartments may be used to partition the targets into groups. Additionally, the natural hierarchy of the patient record should be used when constructing the access control policy.

6.3 *Authorization of User Actions*:

6.3.1 User actions can be authorized using the same sorts of techniques as described in the previous section. Rather than authorizing simple actions such as read or write, the mechanisms authorize complex actions of some semantic significance to the application. Since these actions are application-specific, it is usually not feasible to use the underlying operating system functionality for this purpose; rather, specific mechanisms shall be constructed for each application. Note that different mechanisms (for example, capabilities versus ACLs) might be better suited for different applications.

6.3.2 User actions typically can be decomposed into application-specific functionality that requires generic access to certain objects. For example, updating a patient record in a database would require write access to the file containing the database. This may, depending on the implementation, require the user to have the types of generic access rights to underlying objects that were described in 6.2.

6.3.3 Electronic signatures are used to indicate a specific action was performed. This provides an audit capability and also allows document authorization to be performed as described in 6.4. The actual action performed is indicated by the signature purpose (a signature attribute), as defined in Guide E 1762. Other signature attributes may indicate the role the user was exercising, the time the action was performed, etc.

6.4 *Document Authorization*:

6.4.1 Document authorization refers to the determination by a recipient of whether a signed document can be considered authorized according to the rules and limits agreed to by the parties. This includes assurance that all necessary actions have been performed on the document and that the users performing these actions were authorized to do so. Electronic signatures are used to indicate the actions being performed. Electronic signatures are described in Guide E 1762 and a particular implementation is specified in Guide PS 100. Document authorization mechanisms shall meet the following requirements:

6.4.1.1 Authorization may be based document contents, identity or role of the signer(s), intent (purpose) of the signer(s), transaction context, or any combination thereof.

6.4.1.2 A user may fill one or more roles, and may exercise multiple roles for a given document.

6.4.1.3 A user may delegate portions of authority to another user, on a short-term or long-term basis based on a risk assessment and organizational policy.

6.4.1.4 Multiple signatures may be required to authorize a document.

6.4.1.5 It shall be possible to timestamp documents using the signatures of trusted third parties.

6.4.2 Document authorization mechanisms associate a set of restrictions with each user. These include, but are not limited to, the types of documents a user may act on; the actions (purposes) a user need perform; the roles that may exercise; and limits on the contents of the document (expressed in terms of document attributes, as defined in Guide E 1762).

6.4.3 Document authorization mechanisms shall also allow specification of co-signature requirements, in terms of which other users, roles, or purposes shall sign a document for a given user's signature to be considered valid. These requirements may allow more complex constructions, for example, assigning weight to individual signers, requiring *k* of *n* signatures, etc.

ASTM International takes no position respecting the validity of any patent rights asserted in connection with any item mentioned in this standard. Users of this standard are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard is subject to revision at any time by the responsible technical committee and must be reviewed every five years and if not revised, either reapproved or withdrawn. Your comments are invited either for revision of this standard or for additional standards and should be addressed to ASTM International Headquarters. Your comments will receive careful consideration at a meeting of the responsible technical committee, which you may attend. If you feel that your comments have not received a fair hearing you should make your views known to the ASTM Committee on Standards, at the address shown below.

This standard is copyrighted by ASTM International, 100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA 19428-2959, United States. Individual reprints (single or multiple copies) of this standard may be obtained by contacting ASTM at the above address or at 610-832-9585 (phone), 610-832-9555 (fax), or service@astm.org (e-mail); or through the ASTM website (www.astm.org).