TECHNICAL SPECIFICATION

ISO/TS 22600-3

First edition
2009-12-01

Health informatics — Privilege management and access control —

Part 3: Implementations

Informatique de santé — Gestion de privilèges et contrôle d'accès —

Partie 3: Mises en œuvre

Reference number
ISO/TS 22600-3:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;
- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 22600-3 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

ISO/TS 22600 consists of the following parts, under the general title *Health informatics — Privilege management and access control*:

- *Part 1: Overview and policy management*
- *Part 2: Formal models*
- *Part 3: Implementations*

Introduction

A common situation today is that hospitals are supported by several vendors providing different applications, which are not able to communicate authentication and authorization since they have their own way to handle these functions. In an integrated scenario, one has to spend a huge amount of money to get users and organizational information mapped before starting the communication. Resources are required for development and maintenance of security functions, which grow exponentially with the number of applications.

On the other hand, if one looks at authorization from the healthcare-organization point of view, the need for a flexible bridging model becomes obvious from the fact that organizations change continuously. Units are closed down, opened and merged.

The situation becomes even more complex when communications over security policy domain boundaries are necessary. The policy differences of these domains then have to be bridged via system changes and/or through *policy agreements* between the parties.

Another complexity is found in functional and structural roles when it comes to users. A user can be authorized to operate under multiple functional and structural roles. While a user can concurrently hold multiple structural roles, the user can only perform under a single functional role for a given information request. The policy will define the relationship among the multiple functional roles that can be held by a user, including relationships of grouping, hierarchy, composite structural roles, functional roles taken in sequence, and roles that must not be combined. For example: if a general practitioner is also a psychiatrist, the policy can specify that the psychiatrist can be grouped with other similarly privileged structural roles, that the psychiatrist inherits the privileges of the General Practitioner, that a new composite structural role is created, or that the two structural roles cannot be combined. An example of a restriction of functional roles taken in sequence would be a conflict of duties which can be restricted by law (e.g. a requester for reimbursement cannot also be the signer for the same reimbursement). Moreover, different responsibilities can be identified in the healthcare organization regarding the role and activities of the users. Moving from country to country or from one healthcare establishment to another, different types or levels of authorization can be applied to similar types of users, both for execution of particular functions and for access to information.

Another important issue today is to improve the quality of care by using Information Technology (IT), without interfering with the respect for the privacy of the patient. To allow physicians to have more adequate information about patients, you need to have something like a “virtual electronic healthcare record” which makes it possible to keep track of all the activities belonging to one patient, regardless of where and by whom they have been documented. With such an approach, we need to have a generic model or a specific agreement between the parties for authorization.

Besides the need for support of a diversity of roles and responsibilities, which are typical in any type of large organization, additional critical aspects can be identified, such as ethical and legal aspects in the healthcare scenario due to the particular type of information that is managed.

The need for restrictive authorization is already high today but is going to dramatically increase over the next couple of years. The reason for this is the increase of exchange of information between applications, in order to fulfil physicians' demands on having access to more and more patient-related information to ensure the quality and efficiency of patient treatment.

The situation with respect to healthcare and its communication and application security services has changed during the last decade. The reasons are, for example:

- moving from mainframe-based proprietary legacy systems to distributed systems running in local environments;
- more data are stored in the information systems and are therefore also more valuable to the users;
- patients are more ambulant and in need of their medical information at different locations.

From this, it follows that advanced security is required in communication and use of health information due to the sensitivity of the person-related information and its corresponding personal and social impact. Those security services concern both communication and application security. Regarding the application security services, such as authentication, integrity, confidentiality, availability, accountability (including traceability and non-repudiation) as well as the notary's services, the first service mentioned, authentication, is of crucial importance for most of the other services. This is also valid for application security, such as access control, integrity, confidentiality, availability, accountability, audibility and the notary's services.

The implementation of a Technical Specification like this is very complex since the involved parties already have systems in operation and are not immediately willing to update these to newer versions or new systems. It is therefore very important that a policy agreement is written between the parties that states that they intend to move towards ISO/TS 22600 for any changes in the systems they are going to make.

The policy agreement must also contain defined differences in the security systems and the agreed solutions on how to overcome the differences. For example, the authentication service, privileges and duties of a requesting party at the responding site have to be managed according to the agreed policy written down in the agreement. For that reason, the information and service requester, as well as the information and service provider on the one hand and the information and services requested and provided on the other hand, have to be grouped and classified properly. Based on that classification, claimant mechanisms, target sensitivity mechanisms and policy specification and management mechanisms can be implemented. With such an all parties underwritten policy agreement, the communication and information exchange can start with the existing systems if the parties do not see any risks. If there are risks which are of such importance that they have to be eliminated before the information exchange starts, they must also be recorded in the policy agreement together with an action plan for how these risks must be removed. The policy agreement must also contain a time plan for this work and an agreement on how it must be financed.

The documentation process is a very important part of a platform for the policy agreement.

ISO/TS 22600 consists of the following parts.

Part 1: Overview and policy management: describes the scenarios and the critical parameters in the cross-border information exchange. It also gives examples of necessary documentation methods as the basis for the policy agreement.

Part 2: Formal models: describes and explains, in a more detailed manner, the architectures and underlying models for the privileges and privilege management which are necessary for secure information sharing, plus examples of policy agreement templates.

Part 3: Implementations: describes examples of implementable specifications of application security services and infrastructural services using different specification languages.

ISO/TS 22600 introduces principles and specifies services needed for managing privileges and access control. Cryptographic protocols are outside the scope of ISO/TS 22600.

ISO/TS 22600 is strongly related to other corresponding International Standards and specifications, such as ISO 17090, ISO/TS 21091 and ISO/TS 21298.

ISO/TS 22600 is meant to be read in conjunction with its complete set of associated standards.

The distributed architecture of shared care information systems with the trend to personal health supporting Service Oriented Architecture (SOA) is increasingly based on networks. Due to their user friendliness, the use of standardized user interfaces, tools and protocols, and therefore their platform independence, the number of really open information systems based on corporate networks and virtual private networks has been rapidly growing during the last couple of years.

This part of ISO/TS 22600 is intended to support the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners.

This part of ISO/TS 22600 is intended to support enquiries from both individuals and application systems.

ISO/TS 22600 defines methods for managing authorization and access control to data and/or functions. It allows policy bridging. It is based on a conceptual model where local authorization manager servers and a cross-border directory server can assist access control in various applications (software components). This directory server provides information on rules for access to various application functions based on roles and other attributes of the individual user. The granted access will be based on the following aspects:

- the authenticated identification of the user;
- the rules for access connected with a specific information object;
- the rules regarding authorization attributes linked to the user provided by the authorization manager;
- the functions of the specific application.

This part of ISO/TS 22600 is used in a perspective ranging from a local situation to a regional or national situation. One of the key points in these perspectives is to have organizational criteria combined with authorization profiles, agreed upon from both the requesting and the delivering side in a written policy agreement.

This part of ISO/TS 22600 supports collaboration between several authorization managers that can operate over organizational and policy borders.

The collaboration is defined in a *policy agreement*, signed by all of the involved organizations, which constitutes the basic platform for the operation.

A documentation format is proposed as a platform for the policy agreement, which makes it possible to obtain comparable documentation from all parties involved in the information exchange.

Based on the aforementioned unified process, a three-dimensional architectural reference model has been derived for defining the constraint models needed. The dimensions of the Generic Component Model used are the domain axis, the decomposition/composition axis and the axis describing the views on a system and its components. For it to be future-proof, sustainable, flexible, portable and scalable, only the constraining process and the resulting security-related meta-models are presented. The instantiation and implementation, e.g. the specification of mechanisms and encoding definitions, is a long-term process, dedicated to other standards and projects or the vendor/provider community, respectively.

After summarizing the ISO/TS 22600-2 basics, the different ways of representing different levels of maturity with different levels of interoperability below the ideal situation of a semantically valid one are discussed.

For those different environments and levels, this part of ISO/TS 22600 introduces examples for specializing and implementing the formal high-level models for architectural components based on ISO/IEC 10746 and defined in ISO/TS 22600-2. These examples and related services are grouped in different annexes.

The specifications are provided using derivates of eXtensible Markup Language (XML), especially SAML (Security Assertion Markup Language) and XACML (eXtensible Access Control Markup Language) specified by OASIS. Additional specifications are also presented in the traditional ASN.1 syntax.

ISO/TS 22600 has been harmonized in essential parts with ASTM E2595-07.

Health informatics — Privilege management and access control —

Part 3: Implementations

1 Scope

This part of ISO/TS 22600 instantiates requirements for repositories for access control policies and requirements for privilege management infrastructures for health informatics. It provides implementation examples of the formal models specified in ISO/TS 22600-2.

This part of ISO/TS 22600 is strongly related to other ISO/TC 215 documents, such as ISO 17090, ISO 22857 and ISO/TS 21091. It is also related to ISO/TS 21298.

This part of ISO/TS 22600 excludes platform-specific and implementation details. It does not specify technical communication security services, authentication techniques and protocols that have been established in other standards such as, for example, ISO 7498-2, ISO/IEC 10745 (ITU-T X.803), ISO/IEC TR 13594 (ITU-T X.802), ISO/IEC 10181-1 (ITU-T X.810), ISO/IEC 9594-8 Authentication framework (equivalent to ITU-T X.509), ISO/IEC 9796, ISO/IEC 9797 and ISO/IEC 9798.

ISO/TS 22600 defines privilege management and access control services required for the communication and use of distributed health information over domain and security borders. ISO/TS 22600 introduces principles and specifies services needed for managing privileges and access control. It specifies the necessary component-based concepts and is intended to support their technical implementation. It does not specify the use of these concepts in particular clinical process pathways nor does it address the safety concerns, if any, associated with their use.

While ISO/TS 22600-1 is a narrative introducing the problem of policy bridging in the context of inter-organizational communication and cooperation, ISO/TS 22600-2 defines a generic development process for analysing, designing, implementing and semantically deploying health information systems. The security services needed due to legal, social, organizational, user-related, functional and technological requirements have to be embedded in the advanced and sustainable system architecture meeting the paradigms for semantic interoperability.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 8601:2004, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO/IEC 9594-8:2001, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks* (also available as ITU-T X.509: 2000)

ISO/IEC 10181-3:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework* (also available as ITU-T X.812: 1995)

ISO/TS 21298:2008, *Health informatics — Functional and structural roles*

ASTM E2595-07, *Standard Guide for Privilege Management Infrastructure*

ASTM E1762-07, *Standard Guide for Electronic Authentication of Health Care Information*

ASTM E1986-98. *Standard Guide for Information Access Privileges to Health Information*

ASTM E2212-02a, *Standard Practice for Healthcare Certificate Policy*

OASIS, *eXtensible Access Control Markup Language* (XACML) v2.0, February 2005

OASIS, *XACML Profile for Role Based Access Control* (RBAC): Committee Draft 01 (normative; 13 February 2004)

OASIS, *Security Assertion Markup Language* (SAML), Version 2.0, March 2005

OASIS 200306, *Service Provisioning Markup Language* (SPML), V1.0, October 2003

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8:1998]

3.2
access control decision function
ADF
specialized function that makes access control decisions by applying access control policy rules to a requested action

3.3
access control enforcement function
AEF
specialized function that is part of the access path between a requester and a protected resource that enforces the decisions made by the ADF

3.4
access control information
any information used for access control purposes, including contextual information

3.5
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2:1989]

3.6
asymmetric cryptographic algorithm
algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[ISO/IEC 10181-1:1996]

3.7
attribute authority
AA
authority which assigns privileges by issuing attribute certificates

[ISO/IEC 9594-8:2001]

3.8
attribute authority revocation list
AARL
revocation list containing a list of references to attribute certificates issued to AAs that are no longer considered valid by the certificate-issuing authority

3.9
attribute certificate
data structure, digitally signed by an attribute authority, that binds some attribute values with identification about its holder

[ISO/IEC 9594-8:2001]

3.10
attribute certificate revocation list
ACRL
revocation list containing a list of references to attribute certificates that are no longer considered valid by the certificate-issuing authority

3.11
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

NOTE See also **data origin authentication** (3.50).

[ISO 7498-2:1989]

3.12
authentication token
information conveyed during a strong authentication exchange, which can be used to authenticate its sender

3.13
authority
entity, which is responsible for the issuance of certificates

NOTE Two types of authority are defined in this part of ISO/TS 22600: certification authority, which issues public key certificates, and attribute authority, which issues attribute certificates.

3.14
authority certificate
certificate issued to a certification authority or an attribute authority

NOTE Adapted from ISO/IEC 9594-8:2001.

3.15
authority revocation list
ARL
revocation list containing a list of public key certificates issued to authorities, which are no longer considered valid by the certificate issuer

3.16
authorization
granting of privileges, which includes the granting of access based on access privileges or conveyance of privileges from one entity that holds higher privileges, to another entity holding lower privileges

NOTE Adapted from ISO 7498-2:1989.

3.17
authorization credential
signed assertion of a user's permission attributes

3.18
availability
property of being accessible and usable upon demand by an authorized entity

[ISO 7498-2:1989]

3.19
base CRL
CRL that is used as the foundation in the generation of a dCRL

3.20
business partner agreement
document used to demarcate the legal, ethical and practical responsibilities between subscribers to a PMI and between cooperating PMI implementations

3.21
CA certificate
certificate for one CA issued by another CA

3.22
certificate
public key certificate

3.23
certificate distribution
act of publishing certificates and transferring certificates to security subjects

3.24
certificate holder
entity that is named as the subject of a valid certificate

3.25
certificate management
procedures relating to certificates: certificate generation, certificate distribution, certificate archiving and revocation

3.26
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

EXAMPLE A particular certificate policy might indicate the applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

3.27
certificate revocation
act of removing any reliable link between a certificate and its certificate holder because the certificate is not trusted any more, whereas it is unexpired

3.28
certificate revocation list
CRL
assigned list indicating a set of certificates that are no longer considered valid by the certificate issuer

NOTE In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes. A published list of the suspended and revoked certificates exists (digitally signed by the CA).

3.29
certificate serial number
integer value, unique within the issuing authority, which is unambiguously associated with a certificate issued by that CA

3.30
certificate suspension list
CSL
published list of the suspended certificates (digitally signed by the CA)

3.31
certificate user
entity that needs to know, with certainty, the public key of another entity

3.32
certificate using system
implementation of those functions defined in this Directory Specification that are used by a certificate user

3.33
certificate validation
process of ensuring that a certificate was valid at a given time, possibly including the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e. were not expired or revoked) at that given time

3.34
certificate verification
verification that a certificate is authentic

3.35

3.35.1
certification authority
CA
certificate issuer; an authority trusted by one or more relying parties to create and assign certificates; optionally the certification authority may create the relying parties' keys

NOTE Adapted from ISO/IEC 9594-8:2001.

3.35.2
certification authority
entity that issues certificates by signing certificate data with its private signing key.

NOTE Authority in the CA term does not imply any government authorization; it only means that it is trusted. Certificate issuer may be a better term but CA is used very broadly.

3.36
certification authority revocation list
CARL
revocation list containing a list of public key certificates issued to certification authorities, which are no longer considered valid by the certificate issuer

3.37
certification path
ordered sequence of certificates of objects in the DIT which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path

3.38
ciphertext
data produced through the use of encipherment

NOTE The semantic content of the resulting data is not available.

[ISO 7498-2:1989]

3.39
claimant
entity requesting that a sensitive service be performed or provided by a verifier, based on the claimant's privileges as identified in their attribute certificate or subject directory attributes extension of their public key certificate

3.40
confidentiality
property indicating that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 7498-2:1989]

3.41
consent
special policy which defines an agreement between an entity playing the role of the subject of an act and an entity acting

3.42
credential
information describing the security attributes (identity or privilege or both) of a principal, which is a prerequisite for the entitlement of, or the eligibility for, a role

NOTE Credentials are claimed through authentication or delegation and used by access control.

3.43
CRL distribution point
directory entry or other distribution source for CRLs

NOTE A CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.

3.44
cryptography
discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2:1989]

3.45
cryptographic algorithm
cipher
method for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2:1989]

3.46
cryptographic system
cryptosystem
collection of transformations from plaintext into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys

NOTE The transformations are normally defined by a mathematical algorithm.

3.47
data confidentiality
service that can be used to provide for protection of data from unauthorized disclosure

NOTE The data confidentiality service is supported by the authentication framework. It can be used to protect against data interception.

3.48
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2:1989]

3.49
data origin authentication
corroboration that the source of data received is as claimed

[ISO 7498-2:1989]

3.50
decipherment
decryption
process of obtaining, from a ciphertext, the original corresponding data

NOTE 1 A ciphertext may be enciphered a second time, in which case a single decipherment does not produce the original plaintext.

NOTE 2 Adapted from ISO/IEC 2382-8:1998.

3.51
delegation
conveyance of privilege from one entity that holds such a privilege to another entity

3.52
delegation path
ordered sequence of certificates which, together with authentication of a privilege asserter's identity, can be processed to verify the authenticity of a privilege asserter's privilege

3.53
delta CRL
dCRL
partial revocation list that only contains entries for certificates that have had their revocation status changed since the issuance of the referenced base CRL