INTERNATIONAL STANDARD

ISO 22600-3

First edition
2014-10-01

Health informatics — Privilege management and access control —

Part 3: Implementations

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

Partie 3: Mises en oeuvre

Reference number
ISO 22600-3:2014(E)

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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **13**
5 Structures and services for privilege management and access control **15**
6 Interpretation of ISO 22600-2 formal models in healthcare settings **18**
7 Concept representation for health information systems **18**
7.1 Overview 18
7.2 Domain languages 19
7.3 OCL constraint modelling 20
7.4 Other constraint representations 20
8 Consent **22**
8.1 Overview 22
8.2 Patient consent 22
8.3 Patient consent management 22
9 Emergency access **22**
10 Refinement of the control model **23**
11 Refinement of the delegation model **23**
Annex A (informative) **Privilege management infrastructure** **24**
Annex B (informative) **Attribute certificate extensions** **60**
Annex C (informative) **Terminology comparison** **62**
Annex D (informative) **Examples for policy management and policy representation** **63**
Bibliography **66**

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This first edition of ISO 22600-3 cancels and replaces ISO/TS 22600-3:2009, which has been technically revised.

ISO 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

The distributed architecture of shared care information systems supporting service-oriented architecture (SOA) is increasingly based on corporate networks and virtual private networks. For meeting the interoperability challenge, the use of standardized user interfaces, tools, and protocols, which ensures platform independence, but also the number of really open information systems, is rapidly growing during the last couple of years.

As a common situation today, hospitals are supported by several vendors providing different applications, which are not able to communicate authentication and authorization since each has its own way of handling these functions. For achieving an integrated scenario, it takes a remarkable amount of money, time, and efforts to get users and changing organizational environments dynamically mapped before starting communication and cooperation. Resources required for the development and maintenance of security functions grow exponentially with the number of applications, with the complexity of organizations towards a regional, national, or even international level, and with the flexibility of users playing multiple roles, sometimes even simultaneously.

The situation becomes even more challenging when inter-organizational communications happens, thereby crossing security policy domain boundaries. Moving from one healthcare centre to another or from country to country, different rules for privileges and their management can apply to similar types of users, both for execution of particular functions and for access to information. The policy differences between these domains have to be bridged automatically or through policy agreements, defining sets of rules followed by the parties involved, for achieving interoperability.

Another challenge to be met is how to improve the quality of care by using IT without infringing the privacy of the patient. To provide physicians with adequate information about the patient, a virtual electronic health care record is required which makes it possible to keep track of all the activities belonging to one patient regardless of where and by whom they have been performed and documented. In such an environment, a generic model or specific agreement between the parties for managing privileges and access control including the patient or its representative is needed.

Besides a diversity of roles and responsibilities, typical for any type of large organization, also ethical and legal aspects in the healthcare scenario due to the sensitivity of person-related health information managed and its personal and social impact have to be considered.

Advanced solutions for privilege management and access control are required today already, but this challenge will even grow over the next couple of years. The reason is the increase of information exchanged between systems in order to fulfil the demands of health service providers at different care levels for having access to more and more patient-related information to ensure the quality and efficiency of patient's diagnosis and treatment, however combined with increased security and privacy risks.

The implementation of this International Standard might be currently too advanced and therefore not feasible in certain organizational and technical settings. For meeting the basic principle of best possible action, it is therefore very important that at least a policy agreement is written between the parties stating to progress towards this International Standard when any update/upgrade of the systems is intended. The level of formalization and granularity of policies and the objects these policies are bound to defines the solution maturity on a pathway towards the presented specification.

The policy agreement also has to contain defined differences in the security systems and agreed solutions on how to overcome the differences. For example, the authentication service and privileges of a requesting party at the responding site have to be managed according to the policy declared in the agreement. For that reason, information and service requester, as well as information and service provider on the one hand, and information and services requested and provided on the other hand, have to be grouped and classified in a limited number of concepts for enabling the specification of a limited number of solution categories. Based on that classification, claimant mechanisms, target sensitivity mechanisms, and policy specification and management mechanisms can be implemented. Once all parties have signed the policy agreement, the communication and information exchange can start with the existing systems if the parties can accept the risks. If there are unacceptable risks which have to be eliminated before the information exchange starts, they also have to be recorded in the policy agreement

together with an action plan stating how these risks have to be removed. The policy agreement also has to contain a time plan for this work and an agreement on how it has to be financed.

The documentation of the negotiation process is very important and provides the platform for the policy agreement.

Privilege management and access control address security and privacy services required for communication and cooperation, i.e. distributed use of health information. It also implies safety aspects, professional standards, and legal and ethical issues. This International Standard introduces principles and specifies services needed for managing privileges and access control. Cryptographic protocols are out of the scope of this International Standard.

This three-part International Standard references existing architectural and security standards as well as specifications in the healthcare area such as ISO, CEN, ASTM, OMG, W3C, etc., and endorses existing appropriate standards or identifies enhancements or modifications or the need for new standards. It comprises of:

— ISO 22600-1: describes the scenarios and the critical parameters in information exchange across policy domains. It also gives examples of necessary documentation methods as the basis for the policy agreement.

— ISO 22600-2: describes and explains, in a more detailed manner, the architectures and underlying models for privilege management and access control which are necessary for secure information sharing including the formal representation of policies.

— ISO 22600-3: describes examples of implementable specifications of application security services and infrastructural services using different specification languages.

It accommodates policy bridging. It is based on a conceptual model where local authorization servers and cross-border directory and policy repository services can assist access control in various applications (software components). The policy repository provides information on rules for access to various application functions based on roles and other attributes. The directory service enables identification of the individual user. The granted access will be based on four aspects:

— the authenticated identification of principals (i.e. human users and objects that need to operate under their own rights) involved;

— the rules for access to a specific information object including purpose of use;

— the rules regarding authorization attributes linked to the principal provided by the authorization manager;

— the functions of the specific application.

This International Standard supports collaboration between several authorization managers that can operate over organizational and policy borders.

This International Standard is strongly related to other ISO/TC 215 works such as ISO 17090 (all parts), ISO 22857, ISO 21091, and ISO 21298.

This International Standard is meant to be read in conjunction with its complete set of associated standards.

Based on the 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 being 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 shortly summarizing the basics of ISO 22600-2, 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 22600 introduces examples for specializing and implementing the formal high-level models for architectural components based on ISO/IEC 10746 and defined in ISO 22600-2. These examples and related services are grouped in different Annexes.

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

This International Standard has been harmonized in essential parts with ASTM E2595-07.

Health informatics — Privilege management and access control —

Part 3: Implementations

1 Scope

This multi-part International Standard defines principles and specifies services needed for managing privileges and access control to data and/or functions.

It focuses on communication and use of health information distributed across policy domain boundaries. This includes healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members, and trading partners by both individuals and application systems ranging from a local situation to a regional or even national situation.

It specifies the necessary component-based concepts and is intended to support their technical implementation. It will not specify the use of these concepts in particular clinical process pathways.

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

This part of ISO 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 International Standards such as e.g. 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 (ITU-T X.509), ISO/IEC 9796 (all parts), ISO/IEC 9797 (all parts), and ISO/IEC 9798 (all parts).

2 Normative references

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

ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

ISO/IEC 10181-3, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework — Part 3*

ASTM E2084-00, *Standard Specification for Authentication of Healthcare Information Using Digital Signatures*

3 Terms and definitions

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

[SOURCE: 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
information used for access control purposes, including contextual information

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

[SOURCE: 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

[SOURCE: ISO/IEC 10181-1:1996]

3.7
attribute authority
AA

authority which assigns privileges by issuing attribute certificates

[SOURCE: ISO/IEC 9594-8:2008]

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

[SOURCE: ISO/IEC 9594-8:2008]

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
provision of assurance of the claimed identity of an entity by securely associating an identifier and its authenticator

[SOURCE: ISO/IEC 15944-5:2008, 3.5]

Note 1 to entry: See also *data origin authentication* (3.49) and peer entity authentication.

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 1 to entry: Two types are defined in this part of ISO 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

[SOURCE: ISO/IEC 9594-8:2008, modified]

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 privileges to access data and functions

[SOURCE: ISO 7498-2:1989, modified]

3.17
authority certificate
certificate issued to an authority (e.g. either to a certification authority or to an attribute authority)

3.18
authorization credential
signed assertion of a user's permission attributes

3.19
availability
property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO 7498-2:1989]

3.20
base CRL
CRL that is used as the foundation in the generation of a dCRL

3.21
business partner agreement
document used to demarcate the legal, ethical, and practical responsibilities between subscribers to a PMI and between cooperating PMI implementations

3.22
CA certificate
certificate for one CA issued by another CA

3.23
certificate
public key certificate

3.24
certificate distribution
act of publishing certificates and transferring certificates to security subjects

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

Note 1 to entry: For example, a particular certificate policy might indicate 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 anymore whereas it is unexpired

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

Note 1 to entry: 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 (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 part of ISO 22600 that are used by a certificate user

3.33
certificate validation
process of ensuring that a certificate was valid at a given time, including possibly 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
verifying that a certificate is authentic

3.35
certification authority
CA
certificate issuer; an authority trusted by one or more relying parties to create, assign, and manage certificates

[SOURCE: ISO 9594-8:2008]

Note 1 to entry: Optionally, the certification authority can create the relying parties' keys.

Note 2 to entry: Entity that issues certificates by signing certificate data with its private signing key.

Note 3 to entry: Authority in the CA term does not imply any government authorization, only that it is trusted. Certificate issuer can 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, that 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 1 to entry: The semantic content of the resulting data is not available.

[SOURCE: 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 that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: 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
prerequisite issued evidence for the entitlement of, or the eligibility for, a role; information describing the security attributes (identity or privilege or both) of a principal

Note 1 to entry: 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 1 to entry: A CRL distributed through a CRL distribution point can contain revocation entries for only a subset of the full set of certificates issued by one CA or can 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

[SOURCE: 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

[SOURCE: 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 1 to entry: 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 1 to entry: 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

[SOURCE: ISO 7498-2:1989]

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

[SOURCE: ISO 7498-2:1989]

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

[SOURCE: ISO/IEC 2382-8:1998]

Note 1 to entry: A ciphertext can be enciphered a second time, in which case a single decipherment does not produce the original plaintext.

3.51
delegation
conveyance of privilege from one entity that holds such 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

3.54
digital signature
data appended to, or a cryptographic transformation [see *cryptography* (3.44)] of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[SOURCE: ISO 7498-2:1989]

3.55
encipherment
encryption
cryptographic transformation of data [see *cryptography* (3.44)] to produce ciphertext

[SOURCE: ISO 7498-2:1989]

3.56
end entity
certificate subject that uses its private key for purposes other than signing certificates or an entity that is a relying party

3.57
end-entity attribute certificate revocation list
EARL
revocation list containing a list of attribute certificates that are no longer considered valid by the certificate issuer and that were issued to certificate holders that were not also AAs

3.58
end-entity public key certificate revocation list
EPRL
revocation list containing a list of public key certificates issued to subjects that are not also CAs, that are no longer considered valid by the certificate issuer

3.59
environmental variables
aspects of policy required for an authorization decision that are not contained within static structures, but are available through some local means to a privilege verifier (e.g. time of day or current account balance)

3.60
full CRL
complete revocation list that contains entries for all certificates that have been revoked for the given scope

3.61
functional role
role which is bound to an act

Note 1 to entry: Functional roles can be assigned to be performed during an act.

Note 2 to entry: Functional roles correspond to the ISO/HL7 21731 RIM participation.