DRAFT FOR DEVELOPMENT

DD ISO/TS 22600-3:2009

Health informatics — Privilege management and access control

Part 3: Implementations

ICS 35.240.80

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards
Documents
Document Sharing Hub

Full document details: DD ISO/TS 22600-3:2009

National foreword

This Draft for Development is the UK implementation of ISO/TS 22600-3:2009.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion to an international standard. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of Update Standards.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 January 2010

© BSI 2010

ISBN 978 0 580 57694 2

Amendments/corrigenda issued since publication

Date	Comments

Documents
Document Sharing Hub

Full document details: DD ISO/TS 22600-3:2009

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)

Documents
Document Sharing Hub

© ISO 2009

Full document details: DD ISO/TS 22600-3:2009

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 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub

Full document details: DD ISO/TS 22600-3:2009

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 2
4 Abbreviations 14
5 Structures and services for privilege management and access control 15
6 Interpretation of ISO/TS 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
7.4.1 General 20
7.4.2 eXtensible Access Control Markup Language 20
7.4.3 Web Services Description Language 21
7.4.4 Business Process Execution Language 21
7.4.5 WS-policy 21
7.4.6 Web Services Policy Language 21
7.4.7 Domain-Independent Web Services Policy Assertion Language 21
7.4.8 Security Assertion Markup Language 22
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
10.1 Use of push or pull 23
10.1.1 Push 23
10.1.2 Pull 23
11 Refinement of the delegation model 23
Annex A (informative) **Privilege management infrastructure** 24
Annex B (informative) **Attribute certificate extensions** 62
Annex C (informative) **Terminology comparison** 64
Annex D (informative) **Examples of policy management and policy representation** 65
Bibliography 68

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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*

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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.

Documents
Document Sharing Hub

© ISO 2009 – All rights reserved

Full document details: DD ISO/TS 22600-3:2009

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.

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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.

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

Documents
Document Sharing Hub

Full document details: DD ISO/TS 22600-3:2009

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 2009 – All rights reserved

Documents
Document Sharing Hub

Full document details: DD ISO/TS 22600-3:2009

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]

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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.

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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.

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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.

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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]

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

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

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

3.54
digital signature
data appended to, or a cryptographic transformation (see cryptography) 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

[ISO 7498-2:1989]

3.55
encipherment
encryption
cryptographic transformation of data (see cryptography) to produce ciphertext

[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, which are no longer considered valid by the certificate issuer

3.59
environmental variables
those 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
roles bound to an act and that can be assigned to be performed during an act

NOTE 1 Functional roles correspond to the RIM participation.

NOTE 2 Adapted from ISO/TS 21298:2008.

NOTE 3 See also **structural role** (3.105).

3.62
hash function
(mathematical) function which maps values from a large (possibly very large) domain into a smaller range

NOTE A “good” hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

3.63
holder
entity to whom some privilege has been delegated either directly from the source of authority or indirectly through another attribute authority

3.64
identification
performance of tests to enable a data processing system to recognize entities

[ISO/IEC 2382-8:1998]

3.65
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[EN 13608-1:2007]

3.66
indirect CRL
iCRL
revocation list that at least contains revocation information about certificates issued by authorities other than that which issued this CRL

3.67
integrity
proof that the message content has not altered, deliberately or accidentally in any way during transmission

[ISO 7498-2:1989]

3.68
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2:1989]

3.69
key agreement
method for negotiating a key value online without transferring the key, even in an encrypted form, e.g. the Diffie-Hellman technique

NOTE See ISO/IEC 11770-1 for more information on key agreement mechanisms.

3.70
key management
generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

[ISO 7498-2:1989]

3.71
lightweight directory access protocol
LDAP
standard access protocol for directories allowing public or controlled access to certificates and other information needed in a PKI

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

3.72
non-repudiation
service providing proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party

3.73
object identifier
OID
unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class

NOTE The object identifier is a name for a certificate policy that is recorded in a field of each certificate issued in conformance with the policy.

3.74
object method
action that can be invoked on a resource

EXAMPLE A file system may have read, write and execute object methods.

3.75
one-way function
(mathematical) function f which is easy to compute, but which, for a general value y in the range, it is computationally difficult to find a value x in the domain such that $f(x) = y$

NOTE There may be a few values y for which finding x is not computationally difficult.

3.76
permission
approval for performing an operation on one or more RBAC protected objects

3.77
policy
set of legal, political, organizational, functional and technical obligations or omissions for communication and cooperation

3.78
policy agreement
written agreement where all involved parties commit themselves to a specified set of policies

3.79
policy decision point
PDP
system entity that evaluates an applicable policy and renders an authorization decision

NOTE 1 This term is defined differently in RFC 3198 [45].

NOTE 2 This term corresponds to “Access Decision Function” (ADF) in ISO/IEC 10181-3:1996.

3.80
policy enforcement point
PEP
system entity that performs access control, by making decision requests and enforcing authorization decisions

NOTE 1 This term is defined in a joint effort by the IETF Policy Framework Working Group and the Distributed Management Task Force (DMTF)/Common Information Model (CIM) in RFC 3198.

NOTE 2 This term corresponds to “Access Enforcement Function” (AEF) in ISO/IEC 10181-3:1996.

Documents
Document Sharing Hub
© ISO 2009 – All rights reserved
Full document details: DD ISO/TS 22600-3:2009

3.81
policy mapping
recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent to (but not necessarily identical to in all respects) a particular certificate policy in the first domain

3.82
principal
actor able to realise specific scenarios (user, organization, system, device, application, component, object)

3.83
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

[ISO/IEC 10181-1:1996]

3.84
privilege
capacity assigned to an entity by an authority according to the entity's attribute

3.85
privilege asserter
privilege holder using their attribute certificate or public key certificate to assert privilege

3.86
privilege management infrastructure
PMI
infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a public key infrastructure

3.87
privilege policy
policy that outlines conditions for privilege verifiers to provide/perform sensitive services to/for qualified privilege asserters

NOTE Privilege policy relates attributes associated with the service, as well as attributes associated with privilege asserters.

3.88
privilege verifier
entity verifying certificates against a privilege policy

3.89
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

[ISO/IEC 10181-1:1996]

3.90
public key certificate
X.509 public key certificates (PKCs) [X.509], binding an identity and a public key

NOTE The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC.

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

3.91
public key infrastructure
PKI
infrastructure used in the relation between a key holder and a relying party that allows a relying party to use a certificate relating to the key holder for at least one application using a public-key-dependent security service

NOTE PKI includes a certification authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy and methods to validate the certification practice.

3.92
relying party
recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate

3.93
role
set of competences and/or performances that are associated with a task

NOTE For managing role relationships between the entities, structural and functional roles can be defined.

[ISO/TS 21298:2008].

3.94
role assignment certificate
certificate that contains the role attribute, assigning one or more roles to the certificate holder

3.95
role certificate
certificate that assigns privileges to a role rather than directly to individuals

NOTE Individuals assigned to that role, through an attribute certificate or public key certificate with a subject directory attributes extension containing that assignment, are indirectly assigned the privileges contained in the role certificate.

3.96
role specification certificate
certificate that contains the assignment of privileges to a role

3.97
sensitivity
characteristic of a resource that implies its value or importance

3.98
security
combination of availability, confidentiality, integrity and accountability

3.99

3.99.1
security policy
plan or course of action adopted for providing computer security

[ISO/IEC 2382-8:1998]

3.99.2
security policy
set of rules laid down by the security authority governing the use and provision of security services and facilities

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

3.100
security service
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[ISO 7498-2:1989]

3.101
simple authentication
authentication by means of simple password arrangements

3.102
source of authority
SoA
attribute authority that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges, or a special type of attribute authority upon which a verifier endows unlimited privilege

NOTE The verifier trusts the source of authority to delegate that privilege to certificate holders, some of which may further delegate that privilege to other certificate holders.

3.103
strong authentication
authentication by means of cryptographically derived credentials

3.104
structural role
structural roles specify relations between entities in the sense of competence (RIM roles), often reflecting organizational or structural relations (hierarchies)

[ISO/TS 21298:2008]

NOTE See also **functional role** (3.61).

3.105
target
resource being accessed by a claimant

NOTE Its sensitivity is modelled in this part of ISO/TS 22600 as a collection of attributes, represented as either ASN.1 attributes or XML elements.

3.106
trust
an entity can be said to “trust” a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects

NOTE This trust may apply only for some specific function. The key role of trust in this framework is to describe the relationship between an authenticating entity and an authority; an entity shall be certain that it can trust the authority to create only valid and reliable certificates.

3.107
third party
party other than the data originator, or data recipient, required to perform a security function as part of a communication protocol

3.108
trusted third party
TTP
third party which is considered to be trusted for purposes of a security protocol

[EN 13608-1:2007]

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

NOTE This term is used in many ISO/IEC standards and other documents describing mainly the services of a CA. The concept is, however, broader and includes services like time stamping and possibly escrowing. TTPs provide basic services, infrastructural services and value-added services.

3.109
verifier
entity responsible for performing or providing a sensitive service for/to qualified claimants

NOTE The verifier enforces the privilege policy. When validating certification paths, a verifier is a type of relying party.

4 Abbreviations

This list of abbreviations includes all the abbreviations used in the three parts of ISO/TS 22600.

AA	Attribute Authority
AARL	Attribute Authority Revocation List
ACI	Access Control Information
ACRL	Attribute Certificate Revocation List
ADF	Access Decision Function
ADI	Access Control Decision Information
AEF	Access Enforcement Function
ANSI	American National Standards Institute
ARL	Authority Revocation List
CA	Certification Authority
CARL	Certification Authority Revocation List
CIM	Common Information Model
CORBA	Common Object Request Broker Architecture
CRL	Certificate Revocation List
dCRL	Delta Certificate Revocation List
DAP	Directory Access Protocol
DEA	Drug Enforcement Administration
DIB	Directory Information Base
DIT	Directory Information Tree
DMTF	Distributed Management Task Force
DSA	Directory System Agent
DTD	Data Type Definition
DUA	Directory User Agent
EARL	End-entity Attribute Certificate Revocation List
EHR	Electronic Health Record
EPRL	End-entity Public Key Certificate Revocation List
HL7	Health Level Seven
iCRL	Indirect Certificate Revocation List
IETF	Internet Engineering Task Force
IT	Information Technology

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

LDAP	Lightweight Directory Access Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OMG	Object Management Group
PA	Privilege Allocator
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKC	Public Key Certificate
PKCS	Public Key Cryptosystem
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PPS	Permission Policy Set
RA	Registration Authority
RBAC	Role-Based Access Control
RPS	Role Policy Set
S/MIME	Secure Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SOA	Service-Oriented Architecture
SoA	Source of Authority
SPML	Service Provisioning Markup Language
TTP	Trusted Third Party
UDDI	Universal Description, Discovery and Integration
UHID	Universal Healthcare Identifier
UML	Unified Modeling Language
URI	Uniform Resource Identifier
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

5 Structures and services for privilege management and access control

Privilege management and access control are ruled by policies, which should be formally expressed for enabling interoperability. In reference to the Generic Component Model, the base class structure of policies has been defined in ISO/TS 22600-2 (see Figure 1). As mentioned in ISO/TS 22600-2, policies can be represented differently. For example, OASIS WS-policy provides a general-purpose model and syntax to describe and communicate the policies of a web service. It specifies a set of common message policy assertions within a policy and attachment mechanisms for using policy expressions with existing XML service technologies. This part of ISO/TS 22600 does not enforce a policy representation language.

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009

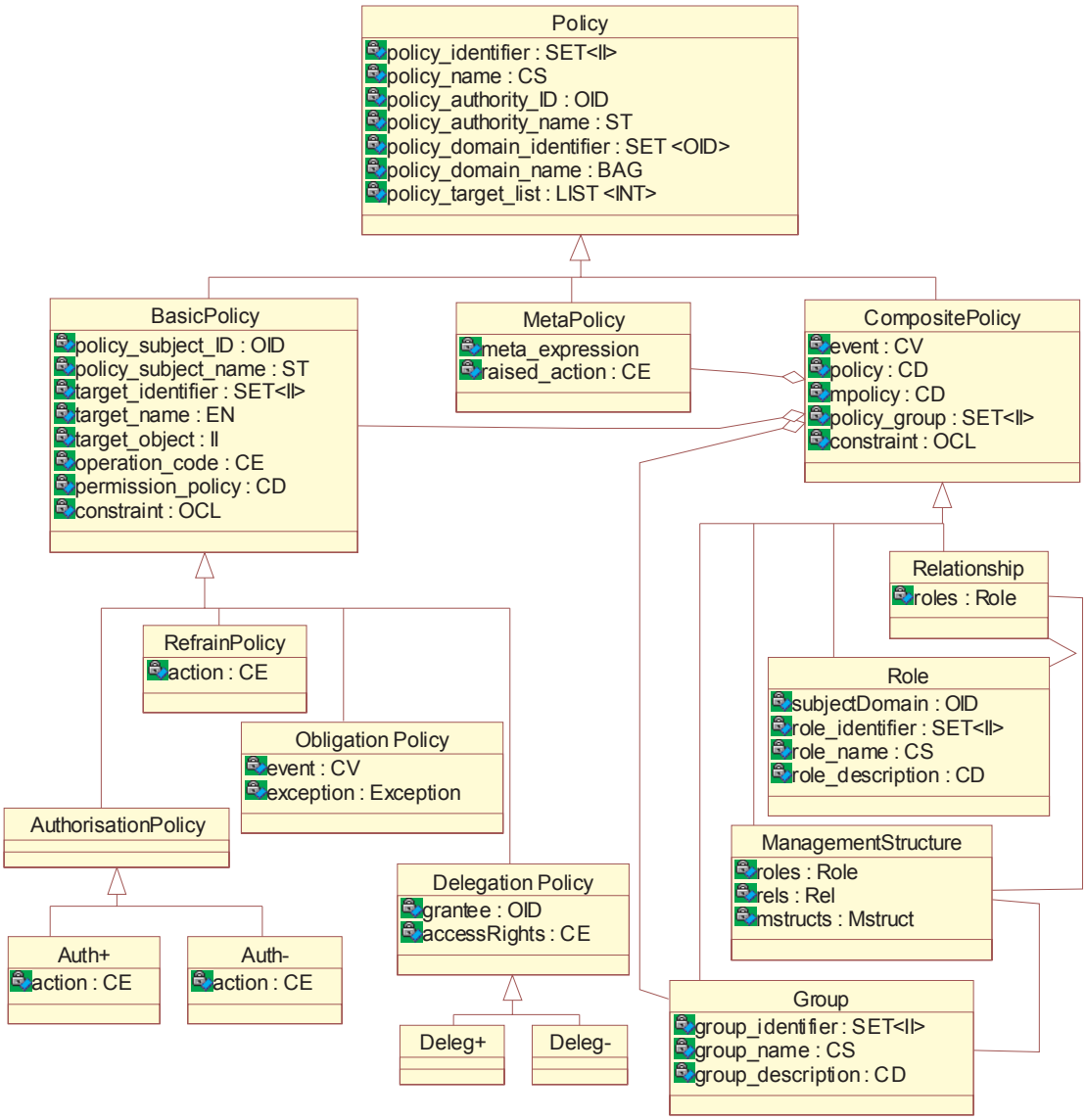

Figure 1 — Policy base class diagram

Privilege management and access control are based on a series of infrastructural services directly or indirectly related to security and privacy services. In that context, a series of PKI services and trusted third party services have to be mentioned, such as ID management, role management, privilege management, policy management, object management, etc. Additionally, services such as audits, LDAPs, intrusion detection, etc., have to be discussed. Instantiations including the services' mechanisms or encoding definitions are dynamically changing or informative issues deferred to the annexes. This part of ISO/TS 22600 has been harmonized as much as possible with ASTM E2595-07.

Regarding the specific requirements and conditions of healthcare, the underlying security model shall consider the whole spectrum of security services and mechanisms that can be accomplished by secure micro-domains.

a) Interaction between security domains

Separate security domains in the domain model can exchange privilege information by agreement of the parties concerned. This interaction between security domains shall be coordinated on both a technical and documentary level. The creating and exchange of privilege sets should take the organizational structure into consideration.

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 22600-3:2009