TECHNICAL SPECIFICATION

ISO/TS 22600-2

First edition
2006-08-01

Health informatics — Privilege management and access control —

Part 2: Formal models

Informatique de santé — Gestion de privilèges et contrôle d'accès — Partie 2: Modèles formels

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

Reference number
ISO/TS 22600-2:2006(E)

© ISO 2006

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

© ISO 2006

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

Contents

Page

Foreword ... iv

Introduction ... v

1 Scope ... 1

2 Terms and definitions ... 2

3 Abbreviations ... 6

4 Component paradigm ... 6

5 Generic models ... 7
5.1 Framework ... 7
5.2 Domain model ... 8
5.3 Document model ... 10
5.4 Policy model ... 10
5.5 Role model ... 13
5.6 Authorization model — Role and privilege assignment ... 14
5.7 Control model ... 14
5.8 Delegation model ... 15
5.9 Access control model ... 17

Annex A (informative) **Functional and structural roles** ... 19

Annex B (informative) **Example of structural roles in healthcare** ... 24

Bibliography ... 26

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

© ISO 2006 – All rights reserved

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 normative 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2e8a5-6ba1-4b0f-b166-164df324338/iso-ts-22600-2-2006

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 22600-2 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*

 © ISO 2006 – All rights reserved

Introduction

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

If, on the other hand, one looks on authorization from the health care organization's point of view, we need a flexible bridging model due to the fact that organizations change continuously. Units close down, open and merge.

The situation becomes even more complex when communications across security policy domain boundaries are necessary. The policy differences between these domains then have to be bridged through *policy agreements* between the parties.

Another complexity is found in roles when it comes to users. A user can adopt different roles related to different periods of time and even have two or more roles simultaneously. For example, a user may work as a nurse for two months and as a midwife for the next two or have both roles within the same time period.

Moreover, different responsibilities can be identified in the healthcare organization depending on the role and activities of the users. Moving from country to country or from one healthcare centre to another, different types or levels of authorization may be applied to similar types of user, both for execution of particular functions and for access to the information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49b7c815-6bc1-4b0f-b166-164d824238/iso-ts-22600-2-2006

Another most important issue today is how to improve the quality of care by using IT, without infringing the privacy of the patient. To allow physicians to have more adequate information about the patient you need to have something like a ‘virtual electronic health care 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 specific agreement between the parties for authorization.

Besides the needs 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 two years. The reason is the increase of exchange of information between applications in order to fulfil the 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 health care and its communication and application security services has changed during the last decade. Reasons are, for example:

— moving from mainframe based proprietary legacy systems to distributed systems running in local environments;

— more data are stored in 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 person-related information and its corresponding personal and social impact. Those security services concern both communication and application security. Regarding communication security services, such as authentication, integrity, confidentiality, availability, accountability (including traceability and

© ISO 2006 – All rights reserved

non-repudiation), control of access to entities as well as notary's services, it is authentication that is of crucial importance for most of the other services. This is also true for application security such as access control to data and functions of applications running at the aforementioned entity, integrity, confidentiality, availability, accountability, audibility and the notary's services.

The implementation of this Technical Specification will be very complex since the involved parties will already have systems in operation and will not be willing to update their system immediately to newer versions or new systems. It is therefore very important that a policy agreement is written between the parties, which states that they intend to progress towards this standard when any change in the systems is intended.

The policy agreement shall also contain defined differences in the security systems and agreed solutions on how to overcome the differences. For example, the authentication service, rights 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, 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 properly. Based on that classification, claimant mechanisms, target sensitivity mechanisms and policy specification and management mechanisms, can be implemented. Once all parties have underwritten the 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 shall also be recorded in the policy agreement together with an action plan for how these risks shall be removed. The policy agreement shall also contain a time plan for this work and an agreement on how it shall be financed.

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

— 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.

ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff524338/iso-ts-22600-2-2006

Privilege management and access control address security services required for communication and distributed use of health information. This document introduces principles and specifies services needed for managing privileges and access control. Cryptographic protocols are out of the scope of this document.

This part of ISO/TS 22600 is strongly related to other corresponding International Standards such as ISO/TS 17090 and ISO/TS 21091. It is also related to work in progress on a future Technical Specification, ISO/TS 21298.

This part of 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 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, virtual private networks has been rapidly growing during the last couple of years.

ISO/TS 22600 shall define privilege management and access control services required for communication and use of distributed health information over domain and security borders. The document 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 will not specify the use of these concepts in particular clinical process pathways.

 © ISO 2006 – All rights reserved

Health informatics — Privilege management and access control —

Part 2: Formal models

1 Scope

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. It is also intended to support inquiries from both individuals and application systems.

ISO/TS 22600 defines methods for managing authorization and access control to data and/or functions. 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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

— 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 should be used in a perspective ranging from a local situation to a regional or national one. One of the key points in these perspectives is to have organizational criteria combined with authorization profiles agreed upon from both the requesting and delivering side in a written policy agreement.

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

The collaboration is defined in a policy agreement, signed by all involved organizations, and 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 of information.

This part of ISO/TS 22600 excludes platform-specific and implementation details. It does not specify technical communication security services and protocols that have been established in other standards, e.g. ENV 13608. It also excludes authentication techniques.

This part of ISO/TS 22600 introduces the underlying paradigm of formal high level models for architectural components based on ISO/IEC 10746. In that context, the Domain Model, the Document Model, the Policy Model, the Role Model, the Authorization Model, the Delegation Model, the Control Model and the Access Control Model are introduced.

© ISO 2006 – All rights reserved

The specifications are provided using the meta-languages Unified Modelling Language (UML) and Extensible Markup Language (XML). Additional diagrams are used for explaining the principles. The attributes used have been referenced to the HL7 Reference Information Model and the HL7 datatype definitions.

2 Terms and definitions

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

2.1
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, definition 08.04.01]

2.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2, definition 3.3.3]

2.3
attribute authority
AA
authority that assigns privileges by issuing attribute certificates

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.4
attribute certificate
data structure, digitally signed by an attribute authority, which binds some attribute values with identification about its holder

ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

2.5
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

NOTE See also data origin authentication and peer entity authentication.

2.6
authority
entity that is responsible for the issuance of certificates

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

2.7
authorization
process of granting rights, which includes the granting of access rights

2.8
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2, definition 3.3.17]

2.9
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

 © ISO 2006 – All rights reserved

2.10
certification authority
CA
authority trusted by one or more relying parties to create and assign certificates

[ISO/IEC 9594-8, definition 3.3.17]

NOTE 1 Optionally the certification authority may create the relying parties' keys.

NOTE 2 Authority in the CA term does not imply any government authorization only that it is trusted. Certificate issuer may be a better term but CA is used very broadly.

2.11
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

2.12
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 7498-2, definition 3.3.16]

2.13
credential
prerequisite for the entitlement of, or the eligibility for, a role

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.14
delegation
conveyance of privilege from one entity that holds such privilege, to another entity

ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

2.15
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

2.16
environmental variables
aspects of policy required for an authorization decision, which 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)

2.17
identification
performance of tests to enable a data processing system to recognize entities

2.18
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[ENV 13608-1]

2.19
integrity
property that information is not altered in any way, deliberately or accidentally

2.20
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2, definition 3.3.32]

© ISO 2006 – All rights reserved

2.21
non-repudiation
service that provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party

2.22
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

2.23
policy agreement
written agreement where all involved parties commit themselves to a specified set of policies

2.24
principal
actor able to realize specific scenarios (user, organization, system, device, application, component, object)

2.25
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, definition 3.3.10]

2.26
privilege
capacity assigned to an entity by an authority according to the entity's attribute

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.27
privilege asserter
privilege holder using their attribute certificate or public-key certificate to assert privilege

ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

2.28
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

2.29
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.

2.30
privilege verifier
entity verifying certificates against a privilege policy

2.31
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

[ISO/IEC 10181-1, definition 3.3.11]

 © ISO 2006 – All rights reserved

2.32
public key certificate
PKC
certificate that binds an identity and a public key

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

2.33
role
set of competences and/or performances which is associated with a task

2.34
role assignment certificate
certificate that contains the role attribute, assigning one or more roles to the certificate holder

2.35
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.

2.36
role specification certificate
certificate that contains the assignment of privileges to a role

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.37
sensitivity
characteristic of a resource that implies its value or importance

ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/49a2c8d5-6be1-4b0f-b166-164dff324338/iso-ts-22600-2-2006

2.38
security
combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

2.39
security policy
plan or course of action adopted for providing computer security

2.40
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, definition 3.3.51]

2.41
source of authority
SOA
attribute authority (2.3) that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges

2.42
target
resource being accessed by a claimant

NOTE Its sensitivity is modelled in this document as a collection of attributes, represented as either ASN.1 attributes or XML elements.

© ISO 2006 – All rights reserved

2.43
trust
quality by which 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 should be certain that it can trust the authority to create only valid and reliable certificates.

3 Abbreviations

AA Attribute Authority

PKC Public Key Certificate

UML Unified Modelling Language

XML eXtensible Markup Language

4 Component paradigm

The framework for a future-proof health information system architecture is based on the generic component model developed in the mid-nineties (e.g. references [1], [2], [3]). Basis of that architecture are a reference information model (RIM) and agreed vocabularies enabling interoperability. Referenced to them, domain-specific constraint models will be specified which represent domain-specific knowledge concepts, considering both structural and functional knowledge. The corresponding components have to be established according to all views of the reference model in ISO 10746-1 on open distributed processing (RM-ODP), i.e. enterprise view, information view, computational view, engineering view and technology view. A view focuses consideration on one aspect abstracting from all others. The different domain concepts and their view representation is not the task of programmers but of domain experts. For that reason, they will use appropriate expression means such as specific graphical representation (e.g. UML diagrams) or sometimes even verbal templates expressed in XML.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 22600-2:2006
https://standards.iteh.ai/catalog/standards/sist/4d2e7b6b-1d1f-4b1f-b0f6-18a8c1f0b1b6/iso-ts-22600-2-2006

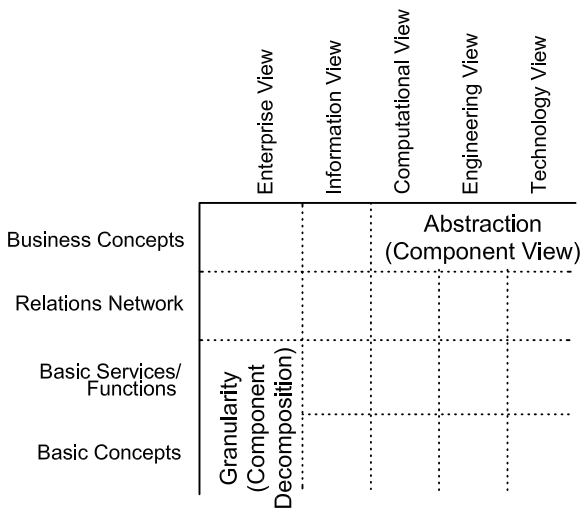

Figure 1 — Generic component model

© ISO 2006 – All rights reserved