TECHNICAL SPECIFICATION

ISO/TS 22600-1

First edition
2006-08-01

Health informatics — Privilege management and access control —

Part 1: Overview and policy management

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

Partie 1: Vue d'ensemble et gestion des politiques

Reference number
ISO/TS 22600-1:2006(E)

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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 22600-1 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*

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.

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 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.

- 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.

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.

Technical Specification ISO/TS 22600 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.

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.

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, which ensure platform independence, is growing and consequently the number of really open information systems based on corporate networks and virtual private networks has also been rapidly growing during the last couple of years.

ISO/TS 22600 defines 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.

Health informatics — Privilege management and access control —

Part 1: Overview and policy management

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:

- 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.

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

2.4
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.

2.5
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.

2.6
authorization
process of granting rights, which includes the granting of access rights

2.7
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2, definitioin 3.3.11]

2.8
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.

2.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 7498-2, definition 3.3.16]

2.10
delegation
conveyance of privilege from one entity that holds such privilege, to another entity

2.11
identification
performance of tests to enable a data processing system to recognize entities

2.12
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2, definition 3.3.32]

2.13
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

2.14
policy agreement
written agreement where all involved parties commit themselves to a specified set of policies

2.15
principal
actor able to realize specific scenarios (user, organization, system, device, application, component, object)

2.16
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]

2.17
privilege
capacity assigned to an entity by an authority according to the entity’s attribute

2.18
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]

2.19
role
set of competences and/or performances which is associated with a task

2.20
security
combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

2.21
security policy
plan or course of action adopted for providing computer security

2.22
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]

2.23
strong authentication
authentication by means of cryptographically derived credentials

2.24
target
resource being accessed by a claimant

3 Abbreviations

This list of abbreviations includes all abbreviations used in this part of ISO/TS 22600.

CA	Certification Authority
PKI	Public Key Infrastructure

4 Goal and structure of privilege management and access control

4.1 Goal of privilege management and access control

The goals are listed under a) to c).

a) To give directions for sharing information. This includes the policy agreement document template, which defines and determines the structure and the contents of the agreement document.

b) To be a standard for privilege management and access control, which govern secure exchange of information between security domains. In order to achieve this, a basic process for the information exchange is defined. The standard for privilege management and access control also defines the method for the secure trans-border information exchange process.

c) To establish a route for transformation of existing systems to future systems, which fulfils all criteria for the cross-border information exchange according to this part of ISO/TS 22600.

The privilege and access control information exchange process takes into account existing situations and takes care of standardization of information exchange over domain and security borders in existing systems. The policy agreement, the policy repository and the directory are central elements in this document.

4.2 Structure of privilege management and access control

4.2.1 Structure elements

This description of the structure for the process model of the information exchange across security domain borders consists of the elements listed below. In this part of ISO/TS 22600 the structure is explained in a broad sense.

The structure consists of the following elements:

- domain;
- policy;
- roles;
- directory;
- authentication;
- process.

The rules for these elements, agreed by the involved domains, are stored in a repository and can be considered as a part of this structure.

4.2.2 Domain

To keep information systems that support shared care, manageable and operating, principal-related components of the system are grouped by common organizational, logical and technical properties, into domains. Any kind of interoperability internal to a domain is called an intra-domain communication and co-operation, whereas interoperability between domains is called an inter-domain communication and co-operation. For example, communication could be realized between departments of a hospital internal to the domain hospital (intra-domain communication), or externally to the domain of a special department (inter-domain communication).

A domain might consist of sub-domains (which will inherit and might specialize policies from the parent domain). The smallest-scale domain might be an individual workplace or a specific component within an information system. Domains can be extended into super-domains, by chaining a set of distinct domains and forming a common larger-scale domain for communication and co-operation.

4.2.3 Policy

4.2.3.1 Access control policy

A policy describes the framework including rules and regulations, the organizational and administrative framework, functionalities, claims and objectives, the parties involved, agreements, rights, duties and penalties defined as well as the technological solution implemented for collecting, recording, processing and communicating data in information systems.

For describing policies, methods such as policy templates or formal policy modelling might be deployed. The policy model is described in 5.4 of ISO/TS 22600-2:2006. Regarding security requirements, security policy is of special interest. The security policy is dealt with in 5.1 of ISO/TS 22600-2:2006.

The particular policy in this document regards an access control infrastructure. It specifies the requirements and conditions for trustworthy communication, creation, storage, processing and use of sensitive information. This includes legal and ethical implications, organizational and functional aspects as well as technical solutions.

Co-operation between domains requires the definition of a common set of policies, which applies to all collaborating domains. It must be derived from the relevant domain-specific policies across all of those domains. These common policies are derived (negotiated) through a process known as policy bridging. The eventual agreed policies need to be documented and signed by all of the domain authorities. Ideally this whole process will be capable of electronic representation and negotiation, to permit real-time electronic collaboration to take place within a (pre-agreed) permitted and regulated framework. The policy negotiation or verification would then take place at every service interaction.

The policy agreement is introduced in Clause 6 and is formally modelled using structured schemata and templates in ISO/TS 22600-2. An agreement process for information exchange shall precede the actual information exchange process. The next subsection describes a scenario for the agreement process. The agreement will constitute the basis for the actual information exchange process described in 4.2.7.

4.2.3.2 Agreement process

The agreement process starts with the formation of a group of persons who have good knowledge about the systems involved in the exchange process and who are mandated to take decisions about which information shall be exchanged and which security level it demands.

When the decision about the information to be exchanged has been made the next step is to look at the level of security in both systems and define the level that satisfies all parties. The way to do this is to list all the requirements both parties have and make up an evaluation form like the one described in Annex A.

The next step in this agreement process is that both parties compare their system with the evaluation criteria by completing the evaluation form. These forms then constitute the basis for the agreement between the parties for the information exchange. In each occasion where there is a situation in which one system does not reach the level of agreed security, this has to be noted in the agreement together with what action shall be taken. One example of action is that one decides that there shall not be any information exchange before this has been taken care of. Another example may be that one decides that it is possible to start the information exchange but the deficiency shall be corrected before a specified date.

The services and the level of services in the policy repository shall also be defined by the parties involved and registered in the agreement. One example of this can be the mapping of roles within these two domains if they do not agree.

Provisions for management and operations of the common directory and policy repository services shall be specified in the agreement.

4.2.4 Roles

Assignment of roles, privileges, and credentials as well as resulting resource access decisions has to be dedicated to a specific principal. Therefore, identification and authentication of principals are basic services for authorization, access control, and other application security services.

The role assignments can show great variation between healthcare establishments, both in granularity and hierarchical organization. This creates difficulties for interoperability, which policy bridging should overcome.

The generic concept of roles is described in 5.4 and Annex A of ISO/TS 22600-2:2006 and will be covered in a future Technical Specification, ISO/TS 21298.

4.2.5 Policy repository

A policy repository holds the set of rules for access control and the set of roles to which these apply. For inter-domain access control these rules and the mechanism for role mapping are stored in a common policy repository.

The common policy repository presents a formal representation of the policy agreement. It is used by an access control service in conjunction with the role information for an individual entity to grant or deny access. If all requirements are fulfilled, a user of an application in one security domain will be privileged to access or retrieve appropriate information from the other security domain.

4.2.6 Directory

A directory service provides information about entities. Directory specifications should follow ISO/TS 21091.