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

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.

The common directory service to be used for inter-domain access control shall provide the necessary information on all entities that are covered by the policy agreement. This will include information on role assignment and authentication.

4.2.7 Authentication

There are different levels for principal authentication. Due to the sensitivity of health information and the related security requirements, the highest level of both the requesting and the responding principals within a communication and co-operation relationship shall be provided through strong mutual authentication. Strong authentication should be realized in a token-based way (e.g. by smartcards).

The authentication framework has been specified in ISO 9798-3 and ISO 10181-1. The authentication procedure is based on a PKI. The PKI framework is given in ISO/TS 17090-1. The authentication certificate follows the X.509V3 specification.

4.2.8 Process

Care processes are changing rapidly. It is therefore very important to create solutions that will allow making the necessary changes in communication processes without any disturbances in the care process. Many of the routines for allocation and withdrawal of roles and authorization shall be made as automatic as possible without losing the control. There are situations where persons involved in the care of a patient shall have the ability to override authorization assigned to roles and to be prepared to justify it later.

The process will vary from site to site but the following process describes the guiding process for this part of ISO/TS 22600.

It consists of two security domains with one application in each domain.

An example scenario is that a person in security domain 1 needs information about a patient under his care from security domain 2, where the patient has been treated at an earlier stage.

Under certain circumstances the applications need to deliver to, and/or retrieve information from, each other. The users of the applications govern the need. User access is controlled by each security domain but can also be granted upon a request from a user in another security domain. The foreign request is approved after it has been checked, with a positive result, against the agreed rules in the policy repository. All these rules shall be specified in the policy agreement.

Both domains have their authorization system with roles according to their needs and different rules for granting access to different information for the different roles.

The process model is illustrated in Figure 1.

The steps in the process are as follows:

1) A new employee gets his/her role defined and assigned by the manager for the organizational unit in which he or she is going to work as described in 4.2.4.

2) The new employee will then be registered in the authorization system that belongs to the appropriate domain with the restrictions and authorization relevant for this role. This implies that the employee is authenticated as described in 4.2.7.

3) Users in the two security domains, which fulfil the rules as defined in the policy agreement, can then be found through the common directory service. The directory is reached from any application in the domains covered by the policy agreement. See 4.2.6.

4) When an employee belonging to security domain 1 starts to use application 1, in system 1, in security domain 1, the first the application has to do is to check his authorization in access control service 1 (see Figure 1).

5) Access to application 1 in security domain 1 is granted to the employee. The rules for intra- and inter-domain communication of information are described in 5.1 of ISO/TS 22600:2006.

6) The employee using application 1 starts a request for information from application 2 in security domain 2. The request contains the identity and role of the requester and a reference to the relevant rule in the common policy repository.

7) In this situation both systems will look in the policy repository to check if the requirements for the information exchange are fulfilled. It is therefore necessary that security domains 1 and 2 have agreed upon a policy for this type of information exchange and that the rules are available for verification in the policy repository. If the qualifications are fulfilled the procedure continues according to point 8 below. Otherwise application 1 will notify the user that the request has been denied.

8) Application 1 then sends a request for that information to application 2 in security domain 2.

9) The result of the request is then sent to application 1 where the employee can read and store it together with the other information about that patient.

10) All transactions in application 1, application 2, the directory and policy repository, and all communication between the two domains shall be logged. Routines for monitoring the log shall be defined in the policy agreement.

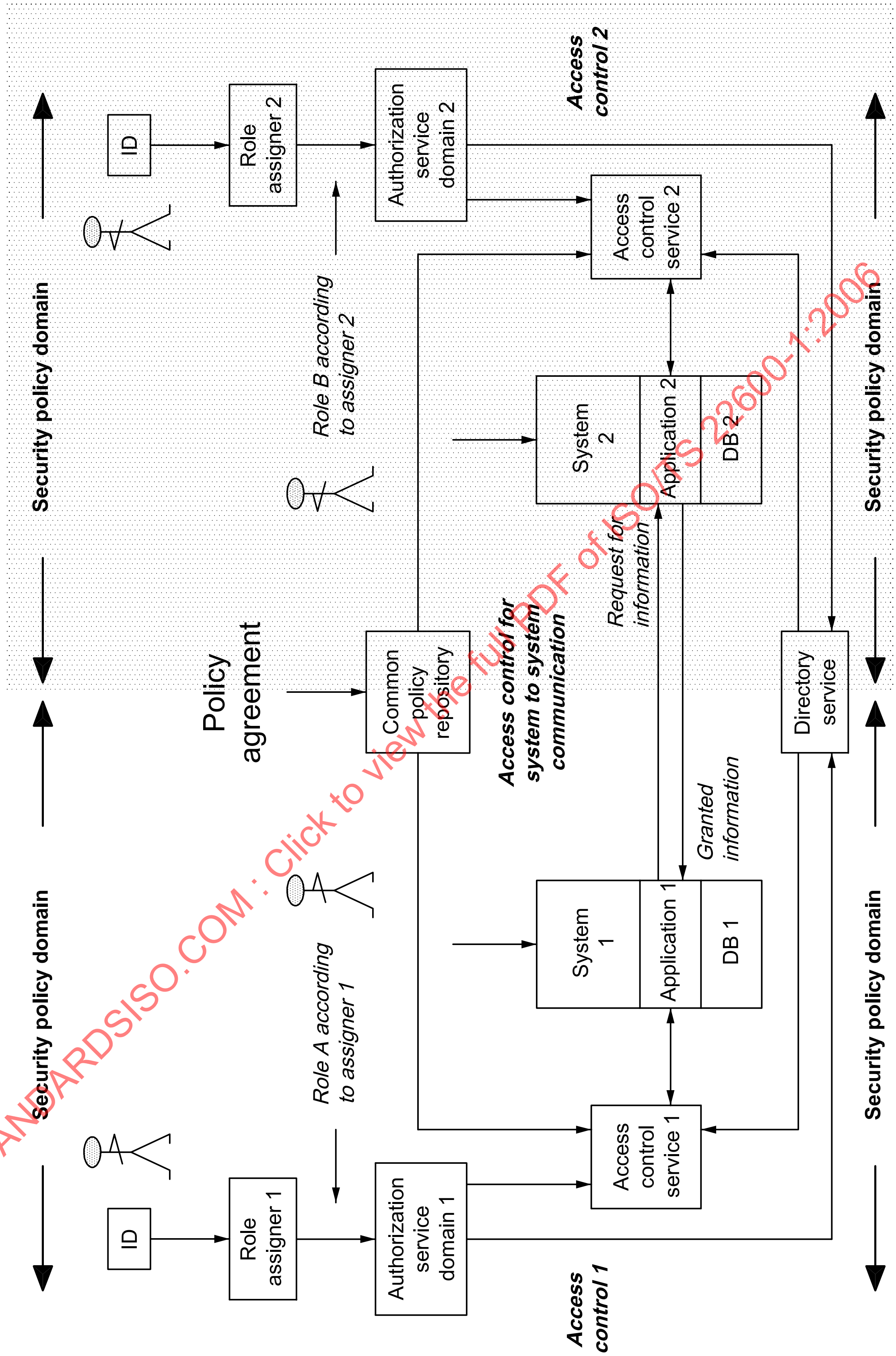

Figure 1 — Process model

5 Policy agreement

5.1 Overview

The basic part of the policy agreement shall contain descriptions of the actual legal framework including rules and regulations. The organizational and administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties and penalties are defined as well as the technological solution implemented for collecting, recording, processing and communicating data in the applications in the domains.

The policy agreement shall also contain a standardized document, the purpose of which is to make it easier to write an agreement that covers the necessary functions for the information interchange. A standard template for the policy agreement is presented in Annex A of this part of ISO/TS 22600.

Steps shall be taken to ensure that the Policy Agreement is understood by everybody using the communication between the domains. The responsibility for the observance of the agreement lies with the main managers for the domains.

The functions are described in 5.2 to 5.22.

5.2 Identification

The policy agreement shall define the identification methods used in the domains including identification of persons (patient, healthcare professionals, health professionals, etc.), organizations, systems, devices, applications, components, etc. If different identification systems are used, the system has to be defined. Linking, mapping or conversion mechanisms shall also be defined. In that context the use of a unique patient ID as well as namespace related master patient indexes and the use of a patient identification service shall be considered and specified.

5.3 Patient consent

The rules for patient consent shall be harmonized or agreements defined on how differences shall be bridged when harmonization is not possible. Both parties shall agree to this in the policy agreement.

5.4 Patient privacy

Patient privacy is a key issue in trans-border information exchange.

In order to gain a patient's full confidence with the information transactions, it is of utmost importance that the rules be clear and easily understood by the patients.

5.5 Information identification

The policy agreement shall identify the procedure for how to reach the data over the domain borders. There are many ways to bring this about and it is therefore very important that this be specified in the agreement.

For read-only, the foreign user can obtain the right to access the application in another domain as a normal domain user. If the user wants to transfer information it shall be possible to specify/identify and limit the information that shall be transferred.

5.6 Information location

In order to secure the information retrieval, the data structure in the applications shall be specified and understood by all parties. The policy agreement shall therefore contain detailed information and structure descriptions.

5.7 Information integrity

The integrity of the data shall be checked in order to detect corruption of data during transfer between the domains. The rules and techniques for this shall be agreed upon and specified in the policy agreement.

5.8 Security

It is most likely that each domain will have its own security rules. It would be ideal, of course, if the involved domains could commit themselves to one and the same security model. This is the primary goal and the security standards defined in both CEN and ISO shall be the primary tools to achieve this.

If this is not possible, it shall be specified in the agreement which security level in one domain corresponds with which security level in another domain and authority for the users shall be designed for the various levels in both domains.

NOTE The security aspects are dealt with in ISO/TS 22600-2.

5.9 Authorization

The authorization process shall be defined in the policy agreement both internally in the domain and externally in the other jurisdiction domains. Authorization is further described in Clause 5 of ISO/TS 22600-2:2006.

5.10 Role structures

Roles are defined within each domain. Rights and responsibilities in specific contexts are defined in policies that are bound to one or more roles. Role assignments are a very important part of the solution for the final standard for policy bridging. The role model is explained in 5.6 to 5.9 of ISO/TS 22600-2:2006.

5.11 Attestation rights

The policy agreement shall name the individuals in the organization who have the right to assign roles and attestation authority to employees. An employee with attestation authority has the right to attest medical information.

5.12 Delegation rights

Delegation is often necessary in daily operations. In order to be able to keep this under control, delegation rights shall be specified in the agreement since it is particularly difficult to know who has which rights inside and between the domains. Delegation shall be well structured in order for it to be possible to follow up and is explained in 5.7 of ISO/TS 22600-2:2006.

5.13 Validity time

Authorization, roles, attestation rights and delegation rights shall have a well-defined and specified time period for the access rights to information both within the domain and across domain borders. These time periods shall be notified in the agreement.

5.14 Authentication of users/roles

PKI is recommended as the authentication method. For cases where the domains cannot agree upon a common standardized authentication system this part of ISO/TS 22600 will specify a number of stipulations to be fulfilled.

5.15 Access

The circumstances allowing access to the information in the other domain are described in 5.8 of ISO/TS 22600-2:2006.

Rules for access rights shall be agreed and specified in the agreement.

5.16 Agreement validity period

The time period for which the agreement is valid shall be specified in the agreement. The agreement shall also include a clause defining the procedure for termination of the agreement both at the end of the agreement period and within the agreement period. Legitimate reasons for cancellation of the agreement shall be defined. Economic compensations for extra costs if the agreement is cancelled between the agreed time periods shall also be defined in the agreement.

5.17 Ethics

The rules and regulations will never cover all possible situations. Therefore ethics shall be taken into consideration and a memorandum shall be formulated to give everybody a good understanding of the framework for responsibility within which everyone has to work.

5.18 Secure audit trail

As mentioned above, all transactions shall be logged. How this will be done and to what extent, shall be agreed in the agreement. Logging is a key issue for ensuring patients have trust in the system.

In order to be able to ensure high quality logging, time stamping is necessary. All information transactions shall have a time stamp. This may require substantial reprogramming of older systems and therefore may not be possible, for economical reasons. In this case the parties signing the agreement shall decide what can be done under existing circumstances and what measures shall be taken for improving the situation. An implementation plan is part of the agreement.

5.19 Audit check

The agreement shall stipulate when, by whom and how the log files shall be checked and appropriate action taken.

5.20 Risk analysis

If risks are observed, all parties have jointly to evaluate them and decide whether the risks can be accepted or not. The risks shall be documented in the policy agreement. If the risks can be accepted all parties shall approve that policy agreement. If the risks are not acceptable, a plan detailing resource requirements for risk reduction shall be included in the policy agreement.

5.21 Continuity and disaster management

Detailed procedures for maintaining business continuity, recovery and disaster management in the event of failure shall be specified in the policy agreement.

5.22 Future system developments

The policy agreement shall commit all parties to develop their future system according to this and other accepted standards in order to facilitate future co-operation for information transfer between their systems.

All these functions shall be specified in the policy agreement. The standardized layout of the policy agreement is described in Annex B and shall be used as a guide when policy agreements are established.

All information exchange functions shall be specified in the policy agreement.

6 Documentation

A policy agreement is founded on the documentation of the security of the involved systems. The documentation needs to be done in a standardized way by all parties in order to get comparable documentation. The documentation consists of two parts.

The first part is administrative and defines the involved systems and who the responsible persons are. It also takes care of the version of the documentation and when it was established and when it has been changed.

The second part is a normalization of the documentation of the system and consists of a number of questions about the systems involved in the information exchange. Each question is divided into two parts. The first part asks for the present situation and the second part asks how it is supposed to be in order to fulfil the security requirements. The documentation proposes a list of answers to every question, ranging from totally fulfilled requirement to no fulfilment. The person who completes the document can then choose the answer that is most applicable to the questions. It is of the utmost importance that the standardized multiple-choice answers are clearly defined and understood by both parties.

Any difference in the answers as to how it is now and how it is supposed to be, is an indication of a security risk. An analysis of what risks such differences might give rise to shall be carried out. These risks shall be documented and measures for how they shall be taken care of shall be described.

An example of a standard documentation template is shown in Annex A.

Annex A
(informative)

Example of a documentation template

A.1 General

The parties involved in the information sharing need to work together to set up a common documentation template which covers all security aspects of the systems and other components.

In order to visualize this work this documentation template shall be regarded as an example of how a documentation template can be constructed.

A.2 Systems and information exchange descriptions

The aim and the way the information is to be exchanged shall be declared in this section. All parties shall, in this section, describe the systems and other components involved in the information exchange.

A.3 Administrative section of the document template

The layout of the documentation may vary due to the environment in which it will be used. In some instances it might be presented on the web and in other cases as paper documentation. The present layout, with inserted comments and explanations, is only meant to illustrate the parts needed to obtain effective documentation supporting the agreement document.

Document template version No: ....

Date: ....

Domain 1

Person responsible for completing the documentation: ....

Systems involved: ....

....

....

Applications involved: ....

....

....

Scope of shared access and constraints to access to information:

....

....

Domain 2

Person responsible for completing the documentation: ....

Systems involved: ....

....

....

Applications involved: ....

....

....

Scope of shared access and constraints to access to information:

....

....

A.4 Evaluation section of documentation template

A.4.1 Classification scheme

Examples of classifications, which will assist in the documentation of the systems involved in the exchange of information.

Examples of questions, for control of specific details concerning this specific information exchange.

It is important that both parties use the same classifications and the same set of questions when dealing with information exchange in accordance with this part of ISO/TS 22600. This makes it easier to harmonize the documentation between all parties.

It is also important to document both the present situation and the expected/needed level of security for the transfer of information.

This way of documentation will highlight weaknesses and other problems with the configuration. It also constitutes the basis for the mutual agreement between the parties about what has to be done to obtain a secure transfer of information or the grounds on which the parties can agree to run information-sharing whilst knowing the problems.

Each party completes the questionnaire. In the template there are two categories of answer columns to each question. One column is marked Present and the second is marked Agreed. In the column marked Present the parties shall answer yes or no to the question whether or not their system fulfils the qualification or which alternative, given in the question, that is the adequate for their system. In the column marked Agreed the parties mark if their system fulfils the policies for secure information exchange according to the agreed policy for both domain 1 and domain 2.

Security class

0 Unlabelled

1 Unclassified

2 Restricted

3 Confidential

4 Secret

5 Top-secret

Security classification of the information to be exchanged:

A.4.2.1 Patient identification method	Present	Agreed
1. Patient name		
2. Patient identification number		
3. Patient name and identification number		
4. Other (describe):		

A.4.2.2 Healthcare professionals identification method	Present	Agreed
1. Name		
2. Identification number		
3. Name and identification number		
4. Other (describe):		

A.4.2.3 Patient consent method	Present	Agreed
1. Patient consent not used		
2. Patient consent is requested		
3. Patient consent is requested and verified by patient		
4. Other (describe):		

A.4.2.4 Patient privacy	Present	Agreed
1. Patient is not informed about the data exchange		
2. Patient gets oral information about the data exchange		
3. Patient gets written information about the data exchange		
4. Other (describe):		

A.4.2.5 Information identification	Present	Agreed
1. Is the technique for the data exchange specified?		

A.4.2.6 Information location	Present	Agreed
1. Is the procedure specified to locate the data to be exchanged?		

A.4.2.7 Information integrity

Transmission identification	Present	Agreed
1. Is the id of the responsible sender sent with the message?		
2. Does each message have a unique identifier?		
3. Is the data encrypted during transmission?		
4. Is the id of the responsible receiver registered?		

Protection against information distortion and/or modification

The proposed groups shown below are just some examples from a case study and may be adjusted to the circumstances at the site were the documentation is made. The combinations can also be grouped together in order to mirror the situation at the site.

Transmission verification	Present	Agreed
1. Is there a log of sender id?		
2. Is there a return transmission of data for comparison?		
3. Is there a checksum verification test?		
4. Is there a log of id of person acknowledging receipt?		
5. Is there a log of id of person acknowledging receipt and a notifying message retransmitted to the sender?		

Class of traceability	Present	Agreed
1. No log of data transmission.		
2. Log, showing that data transmission has taken place, without possibility to recover transmitted data if lost.		
3. Log, showing that data transmission has taken place, with possibility of recovering the transmitted data if lost.		
4. Verification of identity of transmitting system.		
5. Verification of identity of receiving system.		

A.4.3 Security checklists

A.4.3.1 Examples of questions to the Information Security Department	Present	Agreed
1. Do documented demands of security and secrecy for this data exchange exist?		
2. Do documented rules for access rights for this type of data exchange exist?		

A.4.3.2 Examples of questions to the system operating department	Present	Agreed
1. Does a graphical diagram of the system and the involved co-operating components for this information exchange exist?		
2. Does protection against inappropriate access to the information exist?		
3. Do protection tools against viruses exist?		
4. Do agreements exist which clearly describe the responsibility of each party in the support chain?		
5. Do documented routines on how to report disturbances and other divergences in the information exchange exist?		
6. Do documented rules for escalation in case of no action after reported disturbances exist?		
7. Do documented routines for management of innovation or alteration of the system and its process exist?		
8. Do documented routines for backup, restore and archiving exist?		
9. Do documented tools and procedures on how to trace incidents exist?		
10. Do documented rules for installation of patches and how to handle new versions of software exist?		
11. Do documented rules for installation of patches and how to handle new versions of software exist?		
12. Do documented alternative routines exist for long lasting failures?		

A.4.3.3 Examples of questions to the system owner	Present	Agreed
1. Does documentation of user used functions in the system exist?		
2. Does a well-arranged description of the data flow between different processes and descriptions of transaction formats to other systems exist?		
3. Does a user manual for the user of the system exist?		
4. Do documented follow-up routines for evaluation of the benefit of the system and for suggestions about improvements exist?		
5. Do test protocols, rules for acceptance and documented routines exist for how to take new or new versions of the systems in production?		
6. Do specific rules for treatment of especially sensitive information exist?		

A.4.4 Administration checklists

A.4.4.1 Authorization	Present	Agreed
1. Do both parties use the same authorization structure?		
2. If not, does a complete mapping schema exist?		

A.4.4.2 Role structures	Present	Agreed
1. Do both parties use the same authorization structure?		
2. If not, does a complete mapping schema exist?		

A.4.4.3 Delegation rights	Present	Agreed
1. Do the organizations have the same delegation rights?		
2. If not, do the organizations have a complete mapping schema for the delegation rights?		

A.4.4.4 Validity time	Present	Agreed
1. Do the organizations have the same validity time structure?		
2. Do the organizations have synchronization of the validity time periods?		

A.4.4.5 Authentication of users/roles	Present	Agreed
1. Do both organizations have authentication of users/roles?		
2. If yes, are the authentication systems identical?		
3. If not, is there a mapping schema for the authentication of the systems?		

A.4.4.6 Access	Present	Agreed
1. Do the same roles for access rights to information exist in both systems?		
2. If not, is there a complete mapping schema between the roles for access rights between the systems?		

A.4.4.7 Agreement validity period (see B.3.14)

A.4.4.8 Ethics	Present	Agreed
1. Are the same rules for ethics used in both organizations?		
2. If not, is there a mapping schema between the ethic rules of the organizations?		

A.4.4.9 Secure audit trail	Present	Agreed
1. Are the same rules for audit trails used in both organizations?		

A.4.4.10 Audit control	Present	Agreed
1. Do both organizations have the same rules for when, by whom and how the log files shall be checked?		

A.4.4.11 Risk analysis	Present	Agreed
1. Do both organizations use the same system to detect and manage risks?		
2. If not, is there an agreement between the organizations on how risk detection and management shall be done?		

A.4.4.12 **Continuity and disaster management**	Present	Agreed
1. Are common rules and routines for management/administration in case of failure worked out and agreed upon between the organizations?		

A.4.4.13 **Future system developments**	Present	Agreed
1. Does an agreement about the future development of the systems exist?		

Annex B
(informative)

Example of an information exchange policy agreement

B.1 Agreement introduction

The agreement consists of two parts.

The first part is the administrative part, which defines the information to be exchanged, the involved clinical units and the responsible persons. It also specifies those things which do not fulfil the requirements in the general agreement document, and therefore require an agreed action plan for how they shall be taken care of.

The second part consists of the general agreement (policy agreement) regarding all aspects of information exchange between the parties specified in B.2 and B.3.

B.2 Administrative part

B.2.1 Parties to this agreement

Party 1: ____

Party 2: ____

B.2.2 Scope of agreement

This agreement governs the exchange of information between the above stated parties and other matters that require to be regulated according to the description given below.

B.2.3 Information specification

The agreement concerns the following information:

____

____

____

B.2.4 Contact persons

Contact persons are:

For Party 1:

Name: ____

Telephone number: ______________________ e-mail: ______________________