INTERNATIONAL STANDARD

ISO 22600-1

First edition
2014-10-01

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 22600-1:2014(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

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

This first edition of ISO 22600-1 cancels and replaces ISO/TS 22600-1:2006, which has been technically revised.

ISO 22600 consists of the following parts, under the general title *Health informatics — Privilege management and access control*:

— *Part 1: Overview and policy management*

— *Part 2: Formal models*

— *Part 3: Implementations*

Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

— the functions of the specific application.

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

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

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

Health informatics — Privilege management and access control —

Part 1:
Overview and policy management

1 Scope

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

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

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

This part of ISO 22600 proposes a template for the policy agreement. It enables the comparable documentation from all parties involved in the information exchange.

This part of ISO 22600 excludes platform-specific and implementation details. It does not specify technical communication services and protocols which have been established in other standards. It also excludes authentication techniques.

2 Normative references

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

ISO 17090 (all parts), *Health informatics — Public key infrastructure*

ISO 21091, *Health informatics — Directory services for healthcare providers, subjects of care and other entities*

ISO 21298:—[1], *Health informatics — Functional and structural roles*

3 Terms and definitions

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

3.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

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

1) To be published (revision of ISO/TS 21298).

3.2
accountability
property that ensures that the actions of an entity can be traced uniquely to the entity

[SOURCE: ISO 7498-2:1989]

3.3
attribute certificate
data structure, digitally signed by an attribute authority, that binds some attribute values with identification about its holder

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

3.4
authentication
provision of assurance of the claimed identity of an entity by securely associating an identifier and its authenticator

Note 1 to entry: See also data origin authentication and peer entity authentication.

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

3.5
authority
entity that is responsible for the issuance of certificates

Note 1 to entry: Two types are defined in this part of ISO 22600: certification authority, which issues public key certificates, and attribute authority, which issues attribute certificates.

3.6
authorization
granting of privileges, which includes the granting of privileges to access data and functions

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

3.7
availability
property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO 7498-2:1989]

3.8
certification authority
CA
certificate issuer; an authority trusted by one or more relying parties to create, assign, and manage certificates

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

Note 2 to entry: Authority in the CA term does not imply any government authorization, only that it is trusted. Certificate issuer might be a better term but CA is used very broadly.

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

3.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 7498-2:1989]

3.10
delegation
conveyance of privilege from one entity that holds such privilege to another entity

3.11
identification
performance of tests to enable a data processing system to recognize entities

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

3.12
key
sequence of symbols that controls the operations of encipherment and decipherment

[SOURCE: ISO 7498-2:1989]

3.13
policy
set of legal, political, organizational, functional, and technical obligations for communication and cooperation

3.14
policy agreement
written agreement where all involved parties commit themselves to a specified set of policies

3.15
principal
human users and objects that need to operate under their own rights

[SOURCE: OMG Security Services Specification: 2001]

3.16
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

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

3.17
privilege
capacity assigned to an entity by an authority according to the entity's attribute

3.18
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

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

3.19
role
set of competences and/or performances that is associated with a task

3.20
security
combination of availability, confidentiality, integrity, and accountability

[SOURCE: ENV 13608-1:2000]

3.21
security policy
plan or course of action adopted for providing computer security

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

3.22
security service
service provided by a layer of communicating open systems which ensures adequate security of the systems or of data transfers

[SOURCE: ISO 7498-2:1989]

3.23
strong authentication
authentication by means of cryptographically derived multi-factor credentials

3.24
target
resource being accessed by a claimant

4 Abbreviated terms

This list of abbreviated terms includes all abbreviations used in this part of ISO 22600.

CA Certification Authority

PKI Public Key Infrastructure

5 Goal and structure of privilege management and access control

5.1 Goal of privilege management and access control

The goals are:

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 that fulfils all criteria for the cross-border information exchange according to this International Standard.

The privilege and access control information exchange process takes into account existing situations and takes care of standardization of information exchange across policy domain boundaries in existing systems. The policy agreement, the policy repository, and the directory are central elements in this part of ISO 22600.

5.2 Structure of privilege management and access control

5.2.1 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 22600, the structure is explained in a broad sense. For more detailed specifications, references to ISO 22600-2 are given.

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.

5.2.2 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 internally 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 internally 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.

5.2.3 Policy

5.2.3.1 Access control policy

A policy describes the organizational, administrative, legal, and technical framework including rules and regulations, functionalities, claims and objectives, 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. In this International Standard, the policy model is described in ISO 22600-2:2014, 6.4. Regarding security requirements, security policy is of special interest. The security policy is dealt with in ISO 22600-2:2014, 6.1.

The particular policy in this part of ISO 22600 regards a privilege management and 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.

Trustworthy co-operation between policy domains requires the definition of a common set of security and privacy policies that applies to all collaborating entities. It shall be derived from the relevant domain-specific policies across all of those policy domains. Those common security and privacy policies are derived (negotiated) through a process known as policy bridging. The eventually 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 taking place within a (pre-agreed) permitted and regulated framework. The policy negotiation in the case of changing constraints, but at least identification, verification, and enforcement of the applicable policy, has to take place at every service interaction.

The policy agreement is introduced in Clause 5 and is formally modelled using structured schemata and templates in ISO 22600-2. An agreement process for information exchange shall precede the actual information exchange process. The next subclause describes a scenario for the agreement process. The agreement will constitute the basis for the actual information exchange process described in 5.2.8.

5.2.3.2 Agreement process

A successful agreement process depends upon the formation of a group of persons who have in-depth knowledge of the business process requirements and systems involved in the information exchange process and who are mandated to take decisions about the business process requirements for the information exchange including but not limited to such attributes as the type, volume, content, quality, timeliness, relevance, and currency of the data to be exchanged.

When the decision about the information to be exchanged has been made, the next step is to look at the security and privacy policy in both systems and define a common policy that satisfies all parties. This common policy can further constrain data and function permitted for communication and co-operation. Annex A exemplifies the policy evaluation process, listing all requirements of both parties to assess them using the proposed evaluation form. This International Standard offers an explicit way to express policies. In legacy systems, the constraints are frequently just attributed in security levels.

In the next step of this agreement process, both parties compare their system with the evaluation criteria by completing the evaluation form. These forms constitute the basis for the agreement between the parties for the information exchange. Every situation where one system does not reach the level of agreed security has to be noted in the agreement together with the action to be taken. A possible action is to decide that no information exchange is permitted before the problem has been solved. Another policy decided could be to constrain the communication and co-operation process in time, i.e. fixing the requirement that the deficiency shall be corrected before a specified date.

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

5.2.4 Roles

Assignment of roles, privileges, and credentials as well as resulting resource access decisions have to be dedicated to a specific principal. Therefore, identification and authentication of principals are basic services for authorization, access control, and other application security and privacy 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 ISO 22600-2:2014, 6.4 and Annex A. It will be covered in ISO 21298.

5.2.5 Policy repository

A policy repository holds the set of rules for privilege management and access control as well as 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 policy decision services, i.e. an access control service, in conjunction with the role information for an individual entity to grant or deny access. If all requirements are met, a user of an application in one security policy and privacy domain will be privileged to access or retrieve appropriate information from the other security and privacy policy domain.

5.2.6 Directory

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

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

5.2.7 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 has to be provided through strong mutual authentication. Strong authentication should be realized in a multi-factor token-based way (minimally by two factor credentials such as smartcards and passwords).

The authentication framework has been specified in ISO 9798 and ISO 10181. The authentication procedure is based on a PKI. The PKI framework is given in ISO/TS 17090. The authentication certificate follows the X.509v3 specification.

5.2.8 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 authorizations 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 authorizations 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 International Standard.

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 visualized 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 5.2.4.

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 5.2.7.

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 5.2.6.

4) When an employee belonging to security domain 1 starts to use application 1, in system 1, in security domain 1, the application has first 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 ISO 22600-2:2014, 6.1.

6) The employee using application 1 starts a request for information from application 2 in security domain 2. The request contains the identifier and role of the requestor 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 the policy repository and all communication between the two domains shall be logged. Routines for monitoring the log shall be defined in the policy agreement.

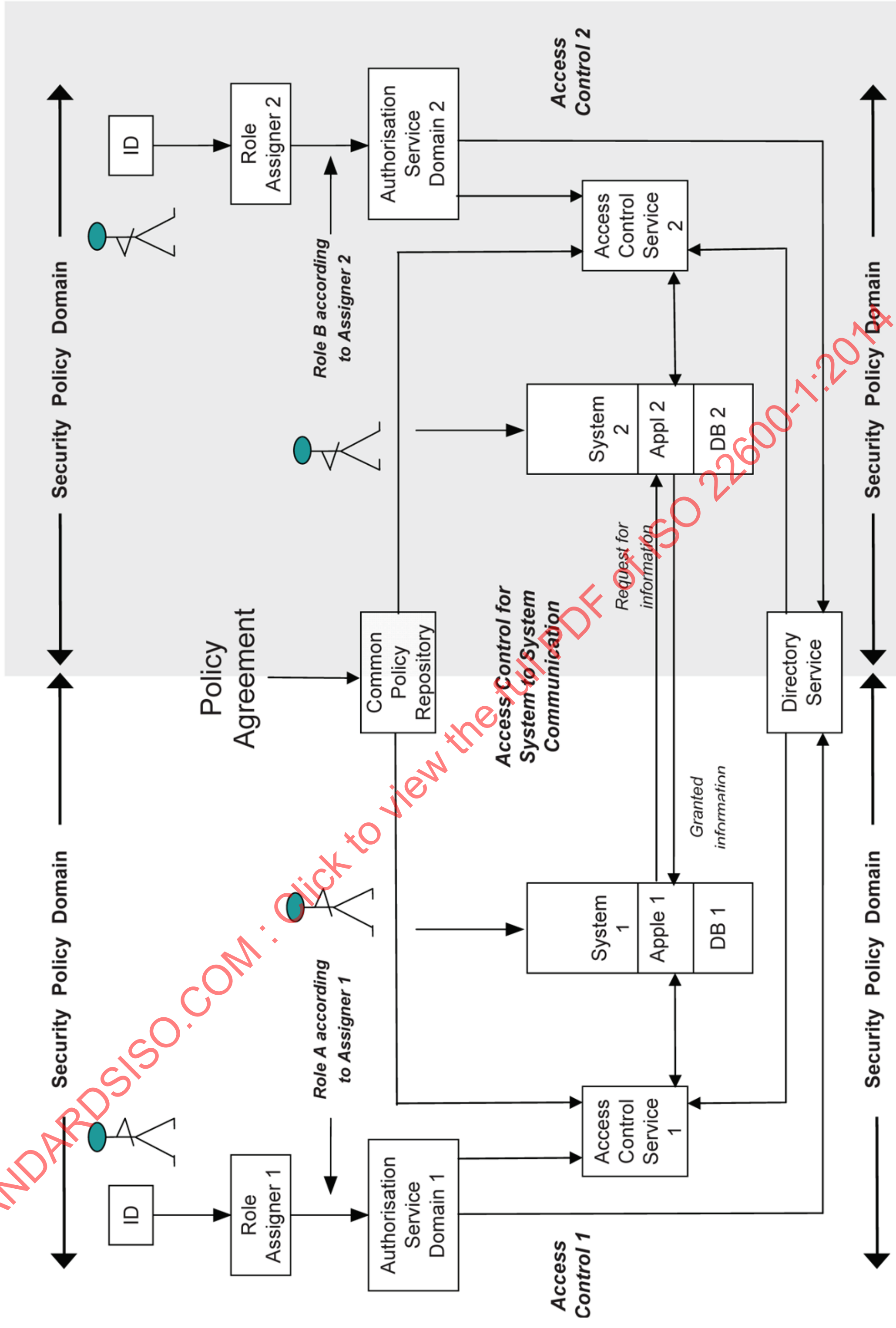

Figure 1 — Process model

6 Policy agreement

6.1 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 the creation, collection, storage, processing, disclosure, retention, transmission, and use of data in applications within the security and privacy policy domains.

The policy agreement shall also contain a standardized document, 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 B.

Steps shall be taken to ensure that the policy agreement is understood by everybody communicating and co-operating between the security and privacy policy domains. Ultimate responsibility for ensuring compliance with the policy agreement rests with those within the organization who are legally responsible for information and its appropriate use and management.

The functions are described in the following subclauses.

6.2 Identification

The policy agreement shall define the identity validation and/or verification methods used in the domains, including identity proofing for methods used in the security and privacy policy domains for the identification of principals such as persons (patients, healthcare professionals, health professionals, etc.), organizations, systems, devices, applications, components, etc. If different identification systems are used, the applied 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.

6.3 Patient consent

The rules for patient consent have to be harmonized. If harmonization is not possible, principles have to be defined ruling how differences shall be bridged. Both parties shall agree on those principles in the policy agreement.

6.4 Patient privacy

Patient privacy is a key issue in communication across policy domain boundaries, and especially 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 are clear and easily understood by the patients.

6.5 Information identification

The policy agreement shall define the procedure of accessing data across domain boundaries.

It shall be possible to specify, identify, and limit the information to be accessed by foreign users. For different access modes such as read-only, transfer, process, or communicate, accessible information might be different. Therefore, information shall be identifiable at the granularity level needed.

6.6 Information location

In order to secure the information retrieval, location and data structure of applications have to be specified and understood by all parties. The policy agreement shall therefore contain detailed information about the location and structure of data, uniquely described by identifiers such as URLs and/or object identifiers (OIDs).

6.7 Information integrity

The integrity of the data shall be checked in order to detect unauthorized modification of data during transfer between the security and privacy policy domains. The rules and techniques for such integrity check shall be agreed upon and specified in the policy agreement.

6.8 Security

Security and privacy policy domains are distinguished by their policies. Ideally, the communicating and cooperating security and privacy domains can commit to one and the same security model represented by a harmonized policy. This is the primary goal, and the security standards defined at both CEN and ISO shall be the primary tools for achieving this.

If such harmonization is not possible, it shall be specified in the policy agreement which policy can be considered equivalent for which role, information, action, and purpose. For each role, information, action, and purpose, a set of policies has to be defined. In cases where policies cannot be processed by the systems involved, security levels have to be defined including the related rules and the equivalences between them.

Details are defined in ISO 22600-2.

6.9 Authorization

The authorization process shall be defined in the policy agreement both internally to the security and privacy policy domain and between the interconnected domains. Authorization is further described in ISO 22600-2:2014, Clause 6.

6.10 Role structures

Roles are defined within each security and privacy policy domain. Privileges as well as contextual and environmental conditions are defined in policies that are bound to one or more roles. Role assignments and assertions are essential parts of the solution for the final policy bridging standard. The role model is explained in detail in ISO 22600-2:2014, 6.6 to 6.9.

6.11 Assignment and attestation authorities

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

6.12 Delegation rights

Delegation of permissions and duties is often necessary in daily operation. In order to be able to keep this under control, ways and limitations to delegate permissions and duties have to be specified in the policy agreement since it is particularly difficult to know who has which privileges inside and between the security and privacy policy domains. Delegation has to be well structured in order to enable follow-ups. It is explained in ISO 22600-2:2014, 6.7.

6.13 Validity time

Authorizations, role assignments, and attestation and delegation privileges shall have a well-defined and specified time period to create, collect, access or modify, use, disclose, retain, and destruct information both within the domain and across domain borders. These time periods shall be notified in the policy agreement.

6.14 Authentication of users/roles

Authentication of users/roles should be based on PKI according to ISO 17090. For cases where the security and privacy policy domains cannot agree upon a common standardized authentication system, this part of ISO 22600 will specify a number of stipulations to be met.

6.15 Access

The circumstances allowing access to the information in the other domain are described in ISO 22600-2:2014, 6.9.

Rules for access privileges have to be agreed and specified in the policy agreement.

6.16 Policy agreement validity period

The time period for which the policy agreement is valid shall be specified in the policy agreement. The policy agreement shall also include a clause defining the procedure for termination of the policy agreement both at the end of and within the policy agreement period. Legitimate reasons for cancellation of the policy agreement within the agreed time period as well as compensations of related extra costs shall be defined in the policy agreement.

6.17 Ethics

Formal, legally binding rules and regulations will never cover all possible situations. Therefore, an ethical framework has to be taken into consideration and a memorandum has to be formulated to give everybody a good understanding about the fair information and ethical principles everyone has to follow. Fair information principles such as openness, publicity, limitation of data collection, limitation of information disclosure, limitation of information use, security, and best practice access control have been defined by the International Medical Informatics Association. A possible ethical framework after Kluge covers autonomy and respect of person, exclusion of impossibility for realizing right, exclusion of relevant differences between right and realization (praxis), obligation for best action, assurance of priority ranges, assurance of equality, and legality.

6.18 Secure audit trail

As mentioned above, all transactions shall be logged, if anyhow possible following ISO 27789. Processes, techniques, and extension of audit trails shall be agreed in the policy 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 might require substantial reprogramming of older systems and therefore might not be possible for economic 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.

6.19 Audit check

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

6.20 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 have to be documented in the policy agreement. If the risks can be accepted, all parties shall approve it. If the risks are not acceptable, a plan detailing resource requirements for risk reduction shall be included in the policy agreement.

6.21 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.

6.22 Future system developments

The policy agreement shall commit all parties to develop their future system according to this International Standard 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.

7 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 an administrative part which defines the involved systems and who the responsible persons are. It also takes care of the version of the documentation, 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 chose the answer that is most applicable to the questions. It is of 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 of 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 might 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 get an 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

This subclause gives

1) examples of classifications, which will assist in the documentation of the systems involved in the exchange of information, and

2) 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 according to this part of ISO 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 information transfer.

This way of documentation will point up 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 information transfer or the grounds which the parties can agree to run the information sharing 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, is 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 (example):

0. Unlabelled
1. Unclassified
2. Restricted
3. Confidential
4. Secret
5. Top-secret

Security classification of the information to be exchanged: ☐

A.4.2 Basic checklists

A.4.2.1 **Patient identity proofing 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 identity proofing method**	Present	Agreed
1. Name		
2. Identification number		
3. Name and identification number		
4. Other (describe):		

A.4.2.3 **Patient consent method** (In this subclause of the Annex, only the classification schema has been specified. For describing the consent, information about role, action, purpose, contextual and environmental conditions, etc. have to be defined.)	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 notification method** (In this subclause of the Annex, only the classification schema has been specified. Notification requirements are not covered here.)	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 transmission integrity check

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 can be adjusted to the circumstances at the site where 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 to recover 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 cooperating 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?		

A.4.3.2 Examples of questions to the system operating department	Present	Agreed
10. Do documented rules for installation of patches and how to handle new versions of software exist?		
11. 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 rules	Present	Agreed
1. Do the organizations have the same delegation rules?		
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 no, is there a mapping schema for the authentication of the systems?		

A.4.4.6 Access	Present	Agreed
1. Do the same roles for privileges to information exist in both systems?		
2. If no, is there a complete mapping schema between the roles for privileges between the systems?		

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

A.4.4.8 Ethics	Present	Agreed
1. Is the same ethical framework used in both organizations?		
2. If no, is there a mapping schema between the ethical frameworks used in the organizations?		

A.4.4.9 Secure audit trail	Present	Agreed
1. Are common rules and routines for audit trails worked out and agreed upon between the organizations?		

A.4.4.10 Audit control	Present	Agreed
1. Are common rules and routines worked out and agreed upon between the organizations regarding 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 no, 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 below

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 according to the description below between the above stated parties and other matters that require to be regulated.

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:___________________________

For Party 2: