
**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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 22600-1:2014

<https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-cd0db037d1a2/iso-22600-1-2014>



iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 22600-1:2014

<https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-cd0db037d1a2/iso-22600-1-2014>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	4
5 Goal and structure of privilege management and access control	4
5.1 Goal of privilege management and access control.....	4
5.2 Structure of privilege management and access control.....	4
6 Policy agreement	9
6.1 Overview.....	9
6.2 Identification.....	10
6.3 Patient consent.....	10
6.4 Patient privacy.....	10
6.5 Information identification.....	10
6.6 Information location.....	10
6.7 Information integrity.....	11
6.8 Security.....	11
6.9 Authorization.....	11
6.10 Role structures.....	11
6.11 Assignment and attestation authorities.....	11
6.12 Delegation rights.....	11
6.13 Validity time.....	11
6.14 Authentication of users/roles.....	12
6.15 Access.....	12
6.16 Policy agreement validity period.....	12
6.17 Ethics.....	12
6.18 Secure audit trail.....	12
6.19 Audit check.....	12
6.20 Risk analysis.....	12
6.21 Continuity and disaster management.....	13
6.22 Future system developments.....	13
7 Documentation	13
Annex A (informative) Example of a documentation template	14
Annex B (informative) Example of an information exchange policy agreement	21
Bibliography	27

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.

<https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-cd0db037d1a2/iso-22600-1-2014>

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 22600-1:2014

5 Goal and structure of privilege management and access control

<https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-cd0db037d1a2/iso-22600-1-2014>

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.

<https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-cd0db037d1a2/iso-22600-1-2014>

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.

[ISO 22600-1:2014](#)

<https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-cd0db037d1a2/iso-22600-1-2014>

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.