NORME INTERNATIONALE

**ISO 22600-1**

Première édition
2014-10-01

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

## Partie 1: Vue d'ensemble et gestion des politiques

*Health informatics — Privilege management and access control — Part 1: Overview and policy management*

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

Numéro de référence
ISO 22600-1:2014(F)

© ISO 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

**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO 2014

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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

Publié en Suisse

# Sommaire

Page

**Avant-propos** ..... **iv**
**Introduction** ..... **v**
**1 Domaine d'application** ..... **1**
**2 Références normatives** ..... **1**
**3 Termes et définitions** ..... **1**
**4 Abréviations** ..... **4**
**5 Objectif et structure de la gestion des privilèges et du contrôle d'accès** ..... **4**
5.1 Objectif de la gestion des privilèges et du contrôle d'accès ..... 4
5.2 Structure de la gestion des privilèges et du contrôle d'accès ..... 5
**6 Accord de politique** ..... **10**
6.1 Vue d'ensemble ..... 10
6.2 Identification ..... 10
6.3 Consentement du patient ..... 10
6.4 Respect de la vie privée du patient ..... 10
6.5 Identification d'informations ..... 10
6.6 Localisation d'informations ..... 11
6.7 Intégrité d'informations ..... 11
6.8 Sécurité ..... 11
6.9 Autorisation ..... 11
6.10 Structures de rôle ..... 11
6.11 Autorités d'attribution et d'attestation ..... 11
6.12 Droits de délégation ..... 11
6.13 Durée de validité ..... 12
6.14 Authentification d'utilisateurs/rôles ..... 12
6.15 Accès ..... 12
6.16 Période de validité de l'accord de politique ..... 12
6.17 Éthique ..... 12
6.18 Journal d'audit de sécurité ..... 12
6.19 Contrôle d'audit ..... 13
6.20 Analyse de risque ..... 13
6.21 Continuité et gestion des incidents ..... 13
6.22 Futurs développements de système ..... 13
**7 Documentation** ..... **13**
**Annexe A** (informative) **Exemple d'un modèle de formulaire de documentation** ..... **14**
**Annexe B** (informative) **Exemple d'un accord de politique sur l'échange d'informations** ..... **22**
**Bibliographie** ..... **29**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 22600-1:2014
https://standards.iteh.ai/catalog/standards/sist/826ed851-32b9-4429-80c0-cd0db037d1a2/iso-22600-1-2014

# Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures employées pour l'élaboration du présent document et celles destinées à son suivi sont décrites dans les Directives ISO/IEC, Partie 1. Il convient de noter les différents critères d'approbation nécessaires aux différents types de documents ISO. Le présent document a été rédigé conformément aux règles rédactionnelles des Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails relatifs à tous droits de propriété identifiés au cours de l'élaboration du document figureront en Introduction et/ou dans la liste ISO des déclarations de brevets reçues (voir www.iso.org/patents).

Tout nom commercial utilisé dans le présent document est une information donnée à des fins de commodité pour l'utilisateur et ne bénéficie d'aucun appui particulier.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, aussi bien que pour des informations au sujet de l'adhésion de l'ISO aux principes de l'OMC concernant les obstacles techniques au commerce (OTC) voir le lien suivant: Avant-propos — Informations supplémentaires.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Le comité chargé de l'élaboration du présent document est l'ISO/TC 215, *Informatique de santé*.

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

Cette première édition de l'ISO 22600-1 annule et remplace l'ISO/TS 22600-1:2006, qui a fait l'objet d'une révision technique.

L'ISO 22600, présentée sous le titre général *Informatique de santé — Gestion de privilèges et contrôle d'accès*, comprend les parties suivantes:

— *Partie 1: Vue d'ensemble et gestion des politiques*

— *Partie 2: Modèles formels*

— *Partie 3: Mises en œuvre*

 © ISO 2014 – Tous droits réservés

# Introduction

L'architecture répartie des systèmes d'informations de soins partagés s'appuie de plus en plus sur des réseaux d'entreprise et des réseaux privés virtuels. Afin de relever le défi de l'interopérabilité, le recours à des interfaces utilisateur, outils et protocoles normalisés qui garantissent l'indépendance d'une plateforme s'est généralisé, tout comme le nombre de systèmes d'informations réellement ouverts a rapidement augmenté au cours des dernières années.

À l'heure actuelle, il est très fréquent que des hôpitaux aient recours à plusieurs fournisseurs qui leur installent des applications qui ne sont pas en mesure de communiquer une authentification et une autorisation, puisque chaque application a sa propre manière de gérer ces fonctions. Aboutir à un scénario intégré demanderait d'investir beaucoup d'argent, de temps et d'efforts pour faire correspondre dynamiquement des utilisateurs et des environnements organisationnels changeants, avant même de démarrer une communication et une coopération. Les ressources requises pour le développement et la maintenance des fonctions de sécurité augmentent de façon exponentielle, parallèlement au nombre d'applications, à l'évolution toujours plus complexe des organisations vers un niveau régional, national, voire international et à la flexibilité des utilisateurs jouant des rôles multiples, parfois même simultanément.

La situation s'avère même encore plus compliquée lorsqu'il s'agit de communications inter-organisationnelles qui, comme leur nom le laisse entendre, excèdent les limites d'un domaine de politique de sécurité. D'un centre de soins à un autre ou d'un pays à un autre, les règles régissant les privilèges et leur gestion peuvent différer pour des types d'utilisateurs similaires, aussi bien pour l'exécution de fonctions particulières que pour l'accès aux informations. Les différences de politiques entre ces domaines doivent être comblées automatiquement ou via des accords de politique définissant des ensembles de règles à respecter par les parties concernées, pour assurer l'interopérabilité.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Améliorer la qualité des soins grâce aux technologies de l'information (TI) sans pour autant violer la vie privée du patient constitue un autre défi à relever. Afin que les médecins puissent disposer d'informations pertinentes sur leurs patients, il est nécessaire de mettre en place un dossier informatisé de soins de santé, permettant de garder une trace de toutes les activités associées à un patient donné, quels que soient le lieu où ces activités ont été menées et la personne qui les a effectuées ou documentées. Dans ce contexte, il est nécessaire de disposer d'un modèle général ou d'un accord spécifique passé entre les parties pour pouvoir gérer les privilèges et le contrôle d'accès aux informations incluant le patient ou son représentant.

ISO 22600-1:2014
https://standards.iteh.ai/catalog/standards/sist/826ed891-7289-4429-8069-cd0d6037d1a2/iso-22600-1-2014

Outre la diversité des rôles et responsabilités qui caractérise tout type de grande organisation, il est important de prendre également en considération les questions éthiques et légales qui se posent dans le cadre d'un scénario de soins de santé, en raison de la sensibilité des informations gérées, liées à la santé de la personne, et de leur impact personnel et social.

Même si la gestion des privilèges et le contrôle d'accès requièrent d'ores et déjà la mise en œuvre de solutions perfectionnées, ce besoin se fera davantage ressentir dans les prochaines années. Cela est dû à l'augmentation du nombre d'informations échangées entre systèmes afin de répondre aux exigences des prestataires de services de santé à différents niveaux de soins, qui veulent pouvoir accéder à toujours plus d'informations sur le patient afin de garantir la qualité et l'efficacité des diagnostics et traitements délivrés aux patients, même si cela implique des risques accrus en termes de sécurité et de respect de la vie privée.

La présente Norme internationale constitue une avancée technologique telle que certains établissements techniques et organisationnels peuvent juger son application infaisable dans l'état actuel des choses. Par conséquent, afin de satisfaire au principe de base qui consiste à entreprendre la meilleure action possible, il est très important que les différentes parties impliquées rédigent au moins un accord de politique explicitant la volonté d'évoluer dans le sens de la présente Norme internationale si des mises à jour/mises à niveau sont prévues. Le niveau de formalisation et de granularité des politiques et les objets auxquels ces politiques sont liées définissent la maturité de la solution par rapport à la spécification présentée.

© ISO 2014 – Tous droits réservés 

L'accord de politique doit également mentionner les différences qui ont été identifiées entre les systèmes de sécurité ainsi que les solutions retenues pour pallier ces différences. Par exemple, le service d'authentification et les privilèges d'un demandeur au niveau du site de réponse doivent être gérés conformément à la politique déclarée dans l'accord. Pour cette raison, le demandeur d'informations et de services ainsi que le fournisseur d'informations et de services d'une part, et les informations et services demandés et fournis d'autre part, doivent être regroupés et classés selon un nombre limité de concepts afin de pouvoir spécifier un nombre limité de catégories de solutions. Il est alors possible, sur la base de cette classification, de mettre en œuvre des mécanismes d'ayants droits, de sensibilité des cibles ainsi que de spécification et de gestion des politiques. Une fois l'accord de politique signé par la totalité des parties impliquées, la communication et l'échange d'informations peuvent débuter en s'appuyant sur les systèmes existants, si les parties en acceptent les risques. En cas de risques inacceptables devant être éliminés avant de débuter l'échange d'informations, ces risques doivent également être enregistrés dans l'accord de politique, tout comme le plan d'actions explicitant la façon de supprimer ces risques. L'accord de politique doit également inclure les échéances d'application du plan d'actions et ses moyens de financement.

La documentation du processus de négociation est très importante et fournit la plateforme de l'accord de politique.

La gestion des privilèges et le contrôle d'accès couvrent les services de sécurité et de respect de la vie privée nécessaires à la communication et à la coopération, c'est-à-dire l'utilisation répartie des informations de santé. Cela couvre également les aspects de sécurité et les normes professionnelles ainsi que les questions légales et éthiques. La présente Norme internationale constitue une introduction aux principes de gestion des privilèges et de contrôle d'accès et spécifie les services nécessaires à ces activités. Les protocoles cryptographiques ne sont pas couverts par la présente Norme internationale.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

La présente Norme internationale en trois parties comporte des références à des normes existantes relatives à l'architecture et à la sécurité de même qu'à des spécifications dans le domaine des soins de santé, comme des spécifications ISO, CEN, ASTM, OMG, W3C, etc., et est conforme à d'autres normes pertinentes existantes ou sinon identifie les améliorations ou les modifications ou encore le besoin d'élaborer de nouvelles normes. Elle se subdivise ainsi:

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

— ISO 22600-1: décrit les scénarios et les paramètres cruciaux de l'échange d'informations d'un domaine de politique à un autre. Elle donne également des exemples des méthodes de documentation nécessaires pouvant servir de base à l'établissement d'un accord de politique.

— ISO 22600-2: décrit et explique de manière plus détaillée les architectures et les modèles sous-jacents de la gestion des privilèges et du contrôle d'accès nécessaires à la sécurisation du partage de données incluant la représentation formelle des politiques.

— ISO 22600-3: donne des exemples détaillés de spécifications pouvant être mises en œuvre pour les services de sécurité et les services d'infrastructure d'applications dans différents langages de spécification.

Elle prend en compte la mise en relation des politiques. Elle est fondée sur un modèle conceptuel dans lequel des serveurs d'autorisation locaux et des services d'annuaires et de répertoires de politiques trans-domaines peuvent faciliter le contrôle d'accès dans diverses applications (composants logiciels). Le répertoire de politiques fournit des informations sur les règles d'accès à diverses fonctions d'application sur la base des rôles et d'autres attributs. Le service d'annuaire permet une identification de l'utilisateur individuel. L'accès sera accordé ou non sur la base des quatre aspects suivants:

— l'identification authentifiée des acteurs principaux (c'est-à-dire utilisateurs humains et objets qui ont besoin de fonctionner avec leurs propres droits);

— les règles d'accès à un objet d'information particulier, notamment le but de l'utilisation;

— les règles applicables aux attributs d'autorisation associés à l'acteur principal, fournies par le gestionnaire d'autorisation;

— les fonctions de l'application spécifique.

 © ISO 2014 – Tous droits réservés

La présente Norme internationale prend en charge une collaboration entre plusieurs gestionnaires d'autorisation qui peuvent fonctionner au-delà de limites organisationnelles et de politique.

La présente Norme internationale est en relation étroite avec d'autres documents élaborés par le comité technique ISO/TC 215 tels que l'ISO 17090 (toutes les parties), l'ISO 22857, l'ISO 21091 et l'ISO 21298.

Les personnes qui liront la présente Norme internationale devront également lire toutes les normes associées.

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

© ISO 2014 – Tous droits réservés

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

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

## Partie 1:
## Vue d'ensemble et gestion des politiques

### 1 Domaine d'application

La présente Norme internationale, subdivisée en plusieurs parties, définit les principes de gestion des privilèges et de contrôle d'accès aux données et/ou aux fonctions et spécifie les services nécessaires à ces activités.

Elle se concentre sur la communication et l'utilisation des informations de santé distribuées au-delà des limites d'un domaine de politique. Cela inclut le partage d'informations de santé entre professionnels de santé non affiliés, établissements de santé, sociétés d'assurance-maladie, patients, membres du personnel et partenaires commerciaux, par des individus tout comme par des systèmes d'application utilisés dans un contexte local, voire régional ou même national.

Elle spécifie les concepts nécessaires pour chaque composante et est destinée à faciliter leur mise en œuvre technique. Elle ne spécifiera pas l'utilisation de ces concepts pour des cheminements de processus cliniques particuliers.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

La présente partie de l'ISO 22600 propose un modèle d'accord de politique, qui permet d'obtenir de toutes les parties impliquées dans l'échange d'informations une documentation comparable.

ISO 22600-1:2014
https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-ed0db057d1a2/iso-22600-1-2014

La présente partie de l'ISO 22600 exclut les détails propres à une plateforme ainsi que les détails de mise en œuvre. Elle ne spécifie pas les services et protocoles de communication techniques qui ont été établis dans d'autres normes. Elle exclut également les techniques d'authentification.

### 2 Références normatives

Les documents suivants, en totalité ou en partie, sont référencés de manière normative dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 17090 (toutes les parties), *Informatique de santé — Infrastructure de clé publique*

ISO 21091, *Informatique de santé — Services d'annuaires pour les fournisseurs de soins de santé, les sujets de soins et autres entités*

ISO 21298:—[1)], *Informatique de santé — Rôles fonctionnels et structurels*

### 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

1) À publier. (Révision de l'ISO/TS 21298.)

© ISO 2014 – Tous droits réservés

**3.1**
**contrôle d'accès**
ensemble des moyens garantissant que seules les entités autorisées peuvent accéder aux ressources d'un système informatique, et seulement d'une manière autorisée

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

**3.2**
**imputabilité**
propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité

[SOURCE: ISO 7498-2:1989]

**3.3**
**certificat d'attribut**
structure de données, ayant été signée électroniquement par une autorité de gestion d'attribut qui lie certaines valeurs d'attribut à une identification de son détenteur

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

**3.4**
**authentification**
moyen pour une entité d'assurer la légitimité d'une identité revendiquée par l'association sécurisée d'un identifiant et de son authentifiant

Note 1 à l'article: Voir aussi authentification de l'origine des données et authentification de l'entité homologue.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

**3.5**
**autorité**
entité responsable de l'octroi des certificats

ISO 22600-1:2014
https://standards.iteh.ai/catalog/standards/sist/82bed851-32b9-4429-80c0-c4d0db037d1a3/iso-22600-1-2014

Note 1 à l'article: Deux types d'autorité sont définis dans la présente partie de l'ISO 22600, à savoir l'autorité de certification qui octroie des certificats de clé publique et l'autorité de gestion d'attribut qui octroie des certificats d'attribut.

**3.6**
**autorisation**
attribution de privilèges comprenant la délivrance de privilèges afin d'avoir accès à des données et fonctions

[SOURCE: ISO 7498-2:1989, modifiée]

**3.7**
**disponibilité**
propriété d'être accessible et utilisable sur demande par une entité autorisée

[SOURCE: ISO 7498-2:1989]

**3.8**
**autorité de certification**
**CA**
émetteur de certificat; autorité de confiance déclarée compétente par une ou plusieurs parties utilisatrices en matière de création, de délivrance et de gestion de certificats

Note 1 à l'article: L'autorité de certification peut éventuellement créer les clés de parties utilisatrices.

Note 2 à l'article: La notion d'autorité incluse dans le terme « autorité de certification » n'implique en rien une autorisation gouvernementale, mais véhicule simplement une notion de confiance. Le terme « émetteur de certificat » est peut-être moins ambigu, mais le terme « autorité de certification » est très largement employé.

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


© ISO 2014 – Tous droits réservés

**3.9**
**confidentialité**
propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés

[SOURCE: ISO 7498-2:1989]

**3.10**
**délégation**
transmission d'un privilège détenu par une entité à une autre entité

**3.11**
**identification**
exécution de tests permettant à un système de traitement des données de reconnaître des entités

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

**3.12**
**clé**
série de symboles commandant les opérations de chiffrement et de déchiffrement

[SOURCE: ISO 7498-2:1989]

**3.13**
**politique**
ensemble d'obligations légales, politiques, organisationnelles, fonctionnelles et techniques applicable à une communication et à une coopération

iTeh STANDARD PREVIEW
(standards.iteh.ai)

**3.14**
**accord de politique**
accord écrit par le biais duquel toutes les parties impliquées s'engagent à respecter un ensemble de politiques préalablement spécifié

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

**3.15**
**acteur principal**
utilisateurs humains et objets qui doivent fonctionner avec leurs propres droits

[SOURCE: Spécification de l'OMG relative aux services de sécurité (OMG Security Services Specification): 2001]

**3.16**
**clé privée**
clé qui est utilisée avec un algorithme asymétrique de cryptographie et dont la possession est limitée (habituellement à une seule entité)

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

**3.17**
**privilège**
capacité assignée par une autorité à une entité selon son attribut

**3.18**
**clé publique**
clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique

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

**3.19**
**rôle**
ensemble de compétences et/ou de comportements associés à une tâche

© ISO 2014 – Tous droits réservés

**3.20**
**sécurité**
combinaison de propriétés de sécurité (telles que disponibilité, confidentialité, intégrité et imputabilité)

[SOURCE: ENV 13608-1:2000]

**3.21**
**politique de sécurité**
plan ou programme d'action adopté pour assurer la sécurité informatique

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

**3.22**
**service de sécurité**
service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données

[SOURCE: ISO 7498-2:1989]

**3.23**
**stricte authentification**
authentification à partir d'un justificatif d'identité à multiples facteurs obtenu de manière cryptographique

**3.24**
**cible**
ressource à laquelle un ayant droit accède

iTeh STANDARD PREVIEW
(standards.iteh.ai)

## 4 Abréviations

La liste d'abréviations ci-dessous inclut toutes les abréviations employées dans la présente partie de l'ISO 22600.

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

CA Certification Authority (autorité de certification)

PKI Public Key Infrastructure (infrastructure de clé publique)

## 5 Objectif et structure de la gestion des privilèges et du contrôle d'accès

### 5.1 Objectif de la gestion des privilèges et du contrôle d'accès

Les objectifs sont les suivants:

a) Donner des orientations pour le partage d'informations. Cela inclut le modèle de formulaire d'accord de politique, qui définit et détermine la structure et le contenu du document d'accord.

b) Constituer une pratique normalisée pour la gestion des privilèges et le contrôle d'accès, qui régit l'échange sécurisé d'informations entre domaines de sécurité. De manière à atteindre cet objectif, un processus de base d'échange d'informations est défini. La pratique normalisée de gestion des privilèges et de contrôle d'accès définit également la méthode de sécurisation du processus d'échange d'informations trans-domaines.

c) Établir la manière de passer de systèmes existants aux futurs systèmes qui satisferont à tous les critères d'échange d'informations trans-domaines selon la présente Norme internationale.

Le processus d'échange d'informations de privilège et de contrôle d'accès prend en compte les situations existantes et vise à aboutir à une normalisation de l'échange d'informations d'un domaine de politique à un autre dans des systèmes existants. L'accord de politique, le répertoire de politiques et l'annuaire sont des éléments capitaux dans la présente partie de l'ISO 22600.

 © ISO 2014 – Tous droits réservés