NORME INTERNATIONALE

ISO 22600-3

Première édition
2014-10-01

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

Partie 3: Mises en oeuvre

Health informatics — Privilege management and access control —

Part 3: Implementations

Numéro de référence
ISO 22600-3:2014(F)

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

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 utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les 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 concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou sur la liste ISO des déclarations de brevets reçues (voir www.iso.org/patents).

Les éventuelles appellations commerciales utilisées dans le présent document sont données pour information à l'intention des utilisateurs et ne constituent pas une approbation ou une recommandation.

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: Foreword - Supplementary information.

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

Cette première édition de l'ISO 22600-3 annule et remplace l'ISO/TS 22600-3:2009, qui a fait l'objet d'une révision technique.

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

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

— *Partie 2: Modèles formels*

— *Partie 3: Mises en œuvre*

Introduction

L'architecture répartie des systèmes d'informations de soins partagés prenant en charge l'architecture orientée service 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 vendeurs 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 que les parties concernées doivent respecter, pour assurer l'interopérabilité.

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.

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 qui lui sont délivrés, 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.

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 peuvent en accepter 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.

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: décrit les scénarios et les paramètres cruciaux de l'échange d'informations d'un domaine de politique à un autre. 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'application 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.

La présente Norme internationale prend en charge une collaboration entre plusieurs gestionnaires d'autorisation qui peuvent fonctionner au-delà des 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.

Sur la base du processus unifié, un modèle de référence architectural en trois dimensions a été obtenu en vue d'une définition des modèles de contrainte nécessaires. Les dimensions du modèle de composante général utilisé sont l'axe «domaine», l'axe «décomposition/composition» et l'axe décrivant les points de vue sur un système et ses composantes. Afin d'obtenir un système à l'épreuve du temps, durable, souple, portable et évolutif, seul le processus de contrainte et les métamodèles associés à la sécurité résultants sont présentés. L'instanciation et la mise en œuvre, par exemple la spécification de mécanismes et de définitions de codage, forment un processus de longue haleine, dédié à d'autres normes et projets ou à la communauté de vendeurs/fournisseurs, respectivement.

Après un bref résumé des concepts de base de l'ISO 22600-2, les différentes façons de représenter des niveaux différents de maturité avec des niveaux différents d'interopérabilité en dessous de la situation idéale valable d'un point de vue sémantique sont décrites.

Pour ces différents environnements et niveaux, la présente partie de l'ISO 22600 introduit des exemples de spécialisation et de mise en œuvre des modèles formels de haut niveau pour les composantes architecturales, basés sur l'ISO/IEC 10746 et définis dans l'ISO 22600-2. Ces exemples et les services associés sont regroupés dans des annexes différentes.

Les spécifications sont fournies via des dérivés du langage XML, en particulier les langages SAML et XACML spécifiés par l'organisation OASIS. Des spécifications supplémentaires sont également présentées dans la syntaxe ASN.1 traditionnelle.

La présente Norme internationale a été harmonisée dans ses parties essentielles avec l'ASTM E2595-07.

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

Partie 3:
Mises en oeuvre

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 réparties au-delà des limites d'un domaine de politique. Cela inclut le partage d'informations de santé entre prestataires de soins de santé non affiliés, organisations de soins 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 venir à l'appui de leur mise en œuvre technique. Elle ne spécifiera pas l'utilisation de ces concepts pour des cheminements de processus cliniques particuliers.

La présente partie de l'ISO 22600 instancie les exigences applicables aux répertoires de politiques de contrôle d'accès et les exigences applicables aux infrastructures de gestion des privilèges. Elle fournit des exemples de mise en œuvre des modèles formels spécifiés dans l'ISO 22600-2.

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 de sécurité, les techniques d'authentification ni les protocoles de communication techniques qui ont été établis dans d'autres Normes internationales telles que, par exemple, l'ISO 7498-2, l'ISO/IEC 10745 (ITU-T X.803), l'ISO/IEC/TR 13594 (ITU-T X.802), l'ISO/IEC 10181-1 (ITU-T X.810), l'ISO/IEC 9594-8 (ITU-T X.509), l'ISO/IEC 9796 (toutes les parties), l'ISO/IEC 9797 (toutes les parties) et l'ISO/IEC 9798 (toutes les parties).

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application du présent document. 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/IEC 9594-8, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire — Partie 8: Cadre général des certificats de clé publique et d'attribut*

ISO/IEC 10181-3, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre de contrôle d'accès — Partie 3*

ASTM E2084-00, *Standard Specification for Authentication of Healthcare Information Using Digital Signatures*

3 Termes et définitions

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
fonction de prise de décision concernant le contrôle d'accès
ADF
fonction spécialisée prenant des décisions concernant le contrôle d'accès par l'application des règles de la politique de contrôle d'accès à une action demandée

3.3
fonction d'application de contrôle d'accès
AEF
fonction spécialisée qui fait partie du chemin d'accès entre un demandeur et une ressource protégée, qui applique les décisions prises par la fonction de prise de décision concernant le contrôle d'accès

3.4
informations de contrôle d'accès
informations utilisées à des fins de contrôle d'accès, incluant les informations contextuelles

3.5
imputabilité
propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité

[SOURCE: ISO 7498-2:1989]

3.6
algorithme asymétrique de cryptographie
algorithme pour réaliser le chiffrement ou le déchiffrement correspondant dans lequel les clés utilisées pour le chiffrement et le déchiffrement sont différentes

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

3.7
autorité d'attribut
AA
autorité qui assigne des privilèges par l'émission de certificats d'attribut

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

3.8
liste de révocation d'autorité d'attribut
AARL
liste de révocation contenant une liste de références à des certificats d'attribut qui ont été délivrés à des autorités d'attribut mais ne sont plus considérés comme étant valides par l'autorité d'émission de certificat

3.9
certificat d'attribut
structure de données, ayant été signée électroniquement par une autorité d'attribut, qui lie certaines valeurs d'attribut à une identification de son détenteur

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

3.10
liste de révocation de certificat d'attribut
ACRL
liste de révocation contenant une liste de références à des certificats d'attribut qui ne sont plus considérés comme étant valides par l'autorité d'émission de certificat

3.11
authentification
moyen pour une entité d'assurer la légitimité d'une identité revendiquée par l'association sécurisée d'un identifiant et de son authentifiant

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

Note 1 à l'article: Voir aussi *authentification de l'origine des données (3.49)* et «authentification de l'entité homologue».

3.12
jeton d'authentification
informations acheminées au cours d'un strict échange d'authentification, qui peuvent être utilisées pour authentifier son expéditeur

3.13
autorité
entité responsable de l'émission des certificats

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

3.14
certificat d'autorité
certificat délivré à une autorité de certification ou à une autorité d'attribut

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

3.15
liste de révocation d'autorité
ARL
liste de révocation contenant une liste de certificats de clé publique qui ont été délivrés à des autorités mais ne sont plus considérés comme étant valides par l'émetteur de certificat

3.16
autorisation
attribution de privilèges comprenant la délivrance de privilèges donnant accès à des données et fonctions

[SOURCE: ISO 7498-2:1989, modifié]

3.17
certificat d'autorité
certificat délivré à une autorité (par exemple, à une autorité de certification ou à une autorité d'attribut)

3.18
justificatif d'identité d'autorisation
déclaration signée d'attributs de permission d'un utilisateur

3.19
disponibilité
propriété d'être accessible et utilisable sur demande par une entité autorisée

[SOURCE: ISO 7498-2:1989]

3.20
liste de révocation de certificat de base
liste de révocation de certificat qui sert de fondement à la génération d'une liste de révocation de certificat delta

3.21
accord entre partenaires métier
document utilisé pour délimiter les responsabilités légales, éthiques et pratiques entre des abonnés d'une infrastructure de gestion des privilèges et entre des implémentations d'infrastructures de gestion des privilèges qui coopèrent

3.22
certificat d'autorité de certification
certificat qu'une autorité de certification a délivré à une autre autorité de certification

3.23
certificat
certificat de clé publique

3.24
distribution de certificat
acte consistant à publier des certificats et à les délivrer à des sujets de sécurité

3.25
gestion des certificats
procédures se rapportant aux certificats: génération de certificat, distribution de certificat, archivage de certificat et révocation

3.26
politique de certificat
ensemble nommé de règles qui indique l'applicabilité d'un certificat à une communauté d'application et/ou à une classe d'application particulières ayant des exigences de sécurité communes

Note 1 à l'article: Par exemple, une politique de certificat particulière peut indiquer l'applicabilité d'un type de certificat à l'authentification de transactions d'échange de données électroniques pour la commercialisation de biens au sein d'une gamme de prix donnée.

3.27
révocation de certificat
acte consistant à supprimer tout lien fiable entre un certificat et son détenteur du fait que le certificat n'est plus approuvé alors qu'il n'a pas expiré

3.28
liste de révocation de certificat
CRL
liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme étant valides par l'émetteur de certificat

Note 1 à l'article: Outre le terme de liste CRL général, certains types de listes CRL spécifiques sont définis pour des listes CRL qui couvrent des portées particulières. Liste publiée des certificats suspendus et révoqués (signée électroniquement par l'autorité de certification).

3.29
numéro de série de certificat
entier unique au sein de l'autorité d'émission, qui est associé de manière univoque à un certificat émis par cette autorité de certification

3.30
liste de suspension de certificat
CSL
liste publiée des certificats suspendus (signée électroniquement par l'autorité de certification)

3.31
utilisateur de certificat
entité qui a besoin de connaître, avec certitude, la clé publique d'une autre entité

3.32
système utilisateur de certificat
implémentation des fonctions définies dans la présente partie de l'ISO 22600 qui sont utilisées par un utilisateur de certificat

3.33
validation de certificat
processus garantissant qu'un certificat était valide à un instant donné, incluant éventuellement la construction et le traitement d'un chemin de certification, et garantissant que tous les certificats de ce chemin étaient valides au même instant, c'est-à-dire qu'ils n'avaient pas expiré ou qu'ils n'avaient pas été révoqués

3.34
vérification de certificat
vérification de l'authenticité d'un certificat

3.35
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

[SOURCE: ISO 9594-8:2008]

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

Note 2 à l'article: Entité qui émet des certificats en signant les données de certificat à l'aide de sa clé de signature privée.

Note 3 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.

3.36
liste de révocation d'autorité de certification
CARL
liste de révocation contenant une liste de certificats de clé publique qui ont été délivrés à des autorités de certification mais ne sont plus considérés comme étant valides par l'émetteur de certificat

3.37
chemin de certification
séquence ordonnée de certificats d'objet dans l'arbre d'informations d'annuaire (ou arbre DIT) qui, lorsqu'ils sont associés à la clé publique de l'objet initial dans le chemin, peuvent être traités pour obtenir le certificat de l'objet final dans le chemin

3.38
cryptogramme
données obtenues par l'utilisation du chiffrement

Note 1 à l'article: Le contenu sémantique des données résultantes n'est pas compréhensible.

[SOURCE: ISO 7498-2:1989]

3.39
prétendant
entité demandant qu'un service sensible soit effectué ou fourni par un vérificateur, sur la base des privilèges du prétendant identifiés dans son certificat d'attribut ou dans l'extension d'attributs d'annuaire de sujet de son certificat de clé publique

3.40
confidentialité
propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés

[SOURCE: ISO 7498-2:1989]

3.41
consentement
politique particulière qui définit un accord entre une entité qui joue le rôle du sujet d'un acte et une entité qui agit

3.42
justificatif d'identité
preuve émise à des fins de conditions préalables concernant l'habilitation ou l'éligibilité à un rôle; informations décrivant les attributs de sécurité (identité et/ou privilège) d'un acteur principal

Note 1 à l'article: Les justificatifs d'identité sont revendiqués par l'authentification ou la délégation et utilisés par le contrôle d'accès.

3.43
point de répartition de liste CRL
entrée d'annuaire ou autre source de répartition pour les listes de révocation de certificat

Note 1 à l'article: Une liste CRL répartie par l'intermédiaire d'un point de répartition de liste CRL peut contenir des entrées de révocation pour un seul sous-ensemble de l'ensemble complet des certificats émis par une même autorité de certification ou peut contenir des entrées de révocation pour plusieurs autorités de certification.

3.44
cryptographie
discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée

[SOURCE: ISO 7498-2:1989]

3.45
algorithme cryptographique
chiffrement
méthode de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée

[SOURCE: ISO 7498-2:1989]

3.46
système cryptographique
système de chiffrement
recueil de transformations faisant passer un texte en clair en cryptogramme et vice versa, la ou les transformations particulières à utiliser étant sélectionnées par des clés

Note 1 à l'article: Les transformations sont habituellement définies par un algorithme mathématique.

3.47
confidentialité des données
service qui peut être utilisé pour assurer la protection des données vis-à-vis d'une divulgation non autorisée

Note 1 à l'article: Le service de confidentialité des données est pris en charge par le cadre d'authentification. Il peut être utilisé pour empêcher l'interception des données.

3.48
intégrité des données
propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[SOURCE: ISO 7498-2:1989]

3.49
authentification de l'origine des données
confirmation que la source des données reçues est telle que déclarée

[SOURCE: ISO 7498-2:1989]

3.50
déchiffrement
reconstitution, à partir d'un cryptogramme, des données originales correspondantes

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

Note 1 à l'article: Un cryptogramme peut être chiffré une deuxième fois; dans ce cas, un déchiffrement unique ne restitue pas le texte en clair original.

3.51
délégation
transmission d'un privilège détenu par une entité à une autre entité

3.52
chemin de délégation
séquence ordonnée de certificats qui, lorsqu'ils sont associés à l'authentification de l'identité d'un déclarant qui revendique un privilège, peuvent être traités pour vérifier l'authenticité du privilège que ce déclarant revendique

3.53
liste de révocation de certificat delta
dCRL
liste de révocation partielle qui ne contient que les entrées pour les certificats qui ont vu leur statut de révocation évoluer suite à l'émission de la liste de révocation de certificat de base référencée

3.54
signature numérique
données ajoutées à une unité de données, ou transformation cryptographique [voir *cryptographie (3.44)*] d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)

[SOURCE: ISO 7498-2:1989]

3.55
chiffrement
transformation cryptographique [voir *cryptographie (3.44)*] de données produisant un cryptogramme

[SOURCE: ISO 7498-2:1989]

3.56
entité finale
sujet de certificat qui utilise sa clé privée à d'autres fins que pour signer des certificats ou entité qui constitue une partie utilisatrice

3.57
liste de révocation de certificat d'attribut d'entité finale
EARL
liste de révocation contenant une liste de certificats d'attribut qui ne sont plus considérés comme étant valides par l'émetteur de certificat et qui ont été délivrés à des détenteurs de certificat qui ne sont pas également des autorités d'attribut