Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1253

(09/2011)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Gestion des identités

Lignes directrices pour la sécurité des systèmes de gestion d'identité

Recommandation UIT-T X.1253

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	**X.1250–X.1279**
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1253

Lignes directrices pour la sécurité des systèmes de gestion d'identité

Résumé

La Recommandation UIT-T X.1253 propose des lignes directrices pour la sécurité des systèmes de gestion d'identité (IdM, *identity management*). Ces lignes directrices expliquent de quelle façon les systèmes IdM devraient être mis en place et exploités en vue de sécuriser les services d'identité dans un environnement NGN (réseau de prochaine génération) ou dans le cyberespace. Elles visent principalement à donner des orientations officielles sur la façon d'utiliser les différents mécanismes de sécurité pour protéger un système IdM général; ces lignes directrices présentent en outre des procédures de sécurité spécifiques à appliquer en cas d'interfonctionnement de deux systèmes IdM.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1253	2011-09-02	17

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1253

Lignes directrices pour la sécurité des systèmes de gestion d'identité

1 Domaine d'application

La présente Recommandation porte sur les éléments suivants:

– Modèles et services de système IdM général

– Menaces et risques concernant la sécurité des systèmes IdM

– Lignes directrices pour la sécurité du déploiement de systèmes IdM

– Lignes directrices pour la sécurité de l'exploitation de systèmes IdM

– Considérations relatives à la confidentialité dans les systèmes IdM.

La présente Recommandation traite principalement des services de gestion d'identité fondée sur plusieurs domaines. Toutefois, les lignes directrices peuvent également s'appliquer à un système de gestion d'identité centralisé.

NOTE – Les personnes appliquant ou utilisant les lignes directrices décrites doivent se conformer aux législations, réglementations et politiques nationales ou régionales applicables. Certaines réglementations ou législations particulières peuvent imposer l'implémentation de mécanismes pour protéger les informations d'identification personnelle.

2 Références

La présente recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1205] Recommandation UIT-T X.1205 (2008), *Présentation générale de la cybersécurité*.

[UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

3 Termes et définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [UIT-T X.1252]: procédure utilisée pour déterminer si l'accès à des ressources, fonctionnalités, services ou informations devrait être accordé à une entité, compte tenu des règles préétablies et des droits spécifiques ou de l'autorité associés à l'entité requérante.

3.1.2 attribut [UIT-T X.1252]: information liée à une entité qui en spécifie une caractéristique.

3.1.3 authentification (d'entité) [UIT-T X.1252]: processus permettant d'obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

3.1.4 justificatif [UIT-T X.1252]: ensemble de données présentées comme preuve d'une identité déclarée et/ou de droits.

3.1.5 identité [UIT-T X.1252]: représentation d'une entité sous la forme d'un ou de plusieurs éléments d'information qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de l'IdM, le terme identité désigne l'identité contextuelle (sous-ensemble d'attributs), c'est-à-dire que la diversité des attributs est limitée par un cadre avec des frontières définies (le contexte) dans lequel l'entité existe et interagit.

NOTE – Chaque entité est représentée par une identité holistique, qui comprend tous les éléments d'information possibles caractérisant cette entité (les attributs). Toutefois, l'identité holistique est théorique et échappe à toute description et utilisation pratique, car le nombre de tous les attributs possibles est indéfini.

3.1.6 gestion d'identité [UIT-T X.1252]: ensemble de fonctions et de fonctionnalités (par exemple l'administration, la gestion et la tenue à jour, la découverte, les échanges de communication, la corrélation et les liens, l'application des politiques, l'authentification et les assertions) utilisées pour:

- garantir les informations d'identité (par exemple les identificateurs, les justificatifs, les attributs);
- garantir l'identité d'une entité (par exemple les utilisateurs/abonnés, les groupes, les dispositifs d'utilisateur, les organisations, les fournisseurs de réseaux et de services, les éléments et objets de réseaux et les objets virtuels); et
- permettre des applications commerciales et de sécurité.

3.1.7 utilisateur [UIT-T X.1252]: toute entité qui utilise une ressource, par exemple un système, un équipement, un terminal, un processus, une application ou un réseau d'entreprise.

3.1.8 centré sur l'utilisateur [UIT-T X.1252]: système IdM qui peut conférer à l'utilisateur la capacité de contrôler et d'appliquer diverses politiques de respect de la vie privée et de sécurité régissant l'échange d'informations d'identité, en particulier des informations d'identification personnelle (PII, *personally identifiable information*), entre entités.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 entité: tout élément qui a une existence séparée et distincte et peut être identifié dans un contexte.

NOTE – Une entité peut être une personne physique, un animal, une personne morale, une organisation, une chose active ou passive, un dispositif, une application logicielle, un service, etc., ou un groupe de ces éléments. Dans le contexte des télécommunications, il peut s'agir de points d'accès, d'abonnés, d'utilisateurs, d'éléments de réseau, de réseaux, d'applications logicielles, de services et de dispositifs, d'interfaces, etc.

3.2.2 client IdM: programme client qui interagit avec le serveur IdM pour extraire les informations d'identité.

3.2.3 serveur IdM: serveur qui gère la durée de vie de l'identité d'un utilisateur.

3.2.4 client IdM mobile: client IdM qui est installé et utilisé sur un dispositif mobile.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

DB base de données (*database*)

DoS déni de service (*denial of service*)

FDDI Interface de données avec distribution par fibre (*fibre distributed data interface*)

IdM gestion d'identité (*identity management*)

IdP fournisseur d'identité (*identity provider*)

IDS système de détection des intrusions (*intrusion detection system*)

IPS système de prévention des intrusions (*intrusion prevention system*)

LAN réseau local (*local area network*)

NGN réseau de prochaine génération (*next generation network*)

OS système d'exploitation (*operating system)*

PII information d'identification personnelle (*personally identifiable information*)

PIN numéro d'identification personnel (*personal identification number*)

PKI infrastructure de clé publique (*public key infrastructure*)

SP fournisseur de services (*service provider*)

SSL couche de connexion sécurisée (*secure socket layer*)

TTP tiers de confiance (*trusted third party*)

VPN réseau privé virtuel (*virtual private network*)

5 Conventions

Aucune.

6 Rappel

En dix ans, les systèmes de gestion d'identité (IdM) sont passés d'un modèle dit "en silo" à un modèle fédéré ou centré sur l'utilisateur. On s'attachait alors dans la plupart des cas à concevoir des systèmes IdM permettant d'assurer des services d'identité de façon efficace et pratique, tandis que l'on tente avec bon nombre des systèmes IdM élaborés récemment d'assurer la sécurité et la confidentialité.

Au départ, les systèmes IdM "en silo" ont été déployés dans le domaine de l'entreprise. Les différents systèmes IdM n'avaient alors aucune connexion entre eux, de telle sorte qu'il n'était pas possible de partager les informations d'identité d'un utilisateur pour assurer certains services utiles entre domaines. Par ailleurs, l'identité d'un même utilisateur pouvait être reproduite dans plusieurs systèmes IdM différents, d'où la difficulté pour l'administrateur système d'une organisation de gérer de façon sécurisée et efficace l'identité d'un utilisateur.

L'étape suivante a consisté à rassembler toutes les identités d'un utilisateur dans un système IdM unique et de les diffuser lorsque nécessaire. Cette approche était appelée modèle centralisé. Dans ce cas de figure, un volume excessif d'informations concernant un utilisateur est regroupé sur un serveur unique. Cette approche présente plusieurs inconvénients, puisque non seulement le fournisseur d'identité devient une défaillance ponctuelle, mais il risque également de ne pas avoir la confiance de toutes les parties.

On a ensuite décidé de laisser chaque fournisseur d'identité gérer sa propre identité et décentraliser sa responsabilité vers plusieurs fournisseurs d'identité pouvant être sélectionnés par un utilisateur. Cette approche est appelée modèle fédéré. Dans ce cas de figure, plusieurs fournisseurs d'identité peuvent recevoir la confiance d'un utilisateur et gèrent une partie des informations d'identité des utilisateurs si nécessaire. Il est possible de partager les informations d'identité d'un utilisateur détenues par chaque fournisseur d'identité en utilisant une partie d'un pseudonyme appelé identité fédérée. Ce modèle évite le problème de la défaillance ponctuelle.

Les questions liées à la confidentialité devenant de plus en plus importantes pour l'utilisateur, la technologie IdM privilégie les utilisateurs pour leur donner le contrôle total de leurs informations d'identité. Ce modèle est dit "centré sur l'utilisateur". Selon ce modèle, les informations d'identité

doivent passer par l'utilisateur afin que celui-ci puisse appliquer sa politique de confidentialité lorsque deux fournisseurs d'identité partagent ses informations d'identité. Ce modèle a été adapté pour de nombreux produits commerciaux et fait appel à d'autres technologies IdM existantes.

La convergence de ces systèmes IdM nécessite souvent de trouver une façon de garantir la sécurité du système issu de la convergence et de parvenir au juste équilibre entre sécurité et confidentialité pour offrir une qualité de fonctionnement optimale. En outre, la plupart des lignes directrices en matière de sécurité proposées jusqu'à présent portaient en règle générale sur les fournisseurs d'identité et les parties utilisatrices. Etant donné que les aspects se rapportant à la sécurité et à la confidentialité des données d'un utilisateur sont désormais des prescriptions obligatoires, il est nécessaire d'examiner la partie centrée sur l'utilisateur de la sécurité des systèmes IdM afin de tenir compte des inquiétudes grandissantes liées à la confidentialité des données de l'utilisateur.

7 Présentation générale des systèmes de gestion d'identité

7.1 Modèle général des systèmes IdM

7.1.1 Système IdM centré sur l'application

Dans les systèmes de gestion d'identité à grande échelle, un système IdM centré sur l'application suppose que des services et politiques d'identité sont conçus pour répondre aux prescriptions des fournisseurs d'identité et des parties utilisatrices et sont optimisés pour répondre aux prescriptions relatives aux applications, par exemple pour la configuration des informations relatives au compte de l'utilisateur. Un système IdM centré sur l'application comprend un fournisseur d'identité et une partie utilisatrice. Lorsqu'un service identité est fourni à l'utilisateur, l'échange d'identité se fait en règle générale entre ces deux entités. Traditionnellement, les technologies de gestion d'identité et d'accès se concentrent principalement sur l'authentification des utilisateurs finals pour permettre un accès fédéré aux applications et services. Par conséquent, l'exigence de sécurité est limitée au périmètre des domaines d'application concernés.

7.1.2 Système IdM centré sur l'utilisateur

Les systèmes IdM centrés sur l'utilisateur privilégient principalement les utilisateurs finals et sont optimisés pour répondre à leurs exigences. Cela signifie que l'objectif premier d'un système IdM est de fournir aux utilisateurs des services d'identité pratiques et complets. Un tel système a pour principale caractéristique de donner à l'utilisateur le contrôle total de son identité. Lorsqu'elles sont diffusées, les informations d'identité d'un utilisateur doivent passer de façon explicite par l'utilisateur pour que celui-ci ait la possibilité d'appliquer une politique personnelle si besoin est. Dans le cas d'un système IdM centré sur l'utilisateur, un programme client doit être installé dans l'environnement informatique de l'utilisateur. Par conséquent, il faut des lignes directrices simples et globales en matière de sécurité pour aider l'utilisateur à installer et déployer de façon sécurisée le logiciel correspondant. Le logiciel doit gérer certaines des informations de sécurité de l'utilisateur.

Les systèmes centrés sur l'utilisateur se distinguent des autres types de systèmes IdM en ce qu'ils insistent sur le fait que c'est l'utilisateur – et non une autorité – qui contrôle la création, la diffusion, l'actualisation et la suppression de ses attributs d'identité. Cela signifie que l'utilisateur a une autorité totale sur la durée de vie de son identité. Le niveau de contrôle peut être déterminé par les besoins de confidentialité de l'utilisateur.

7.2 Services d'identité

7.2.1 Gestion de la durée de vie d'une identité

Ce service gère l'identité qui est créée, diffusée, mise à jour et supprimée. Les données se rapportant à ce service sont stockées dans une base de données située sur un serveur ou sur une machine locale. Par conséquent, seuls les utilisateurs autorisés devraient pouvoir accéder à cette base de données.

7.2.2 Authentification

Le service d'authentification sert à vérifier l'identité des utilisateurs ou des entités légitimes qui demandent à accéder à un système ou à des ressources. L'authentification est le plus important des services que le système IdM fournit aux parties utilisatrices. Tout doit être mis en œuvre pour éviter le piratage des mots de passe et les usurpations d'identité.

7.2.3 Autorisation

Le service d'autorisation vise à traiter la prise de décisions concernant les droits d'accès de l'utilisateur et l'application des décisions en matière d'autorisation, en fonction des privilèges de l'utilisateur. Il est nécessaire pour protéger le système d'identité contre un accès ou une utilisation non autorisé.

7.2.4 Echange d'attributs

Ce service assure les échanges et la synchronisation des attributs. Il est l'un des plus importants du point de vue de la sécurité puisque l'échange d'attributs se fait par l'intermédiaire d'un réseau de communication. Différents niveaux de mécanismes de sécurité sont nécessaires car le support de communication peut être fixe ou hertzien.

7.2.5 Jeton de sécurité

Le service de jeton de sécurité permet aux entités d'échanger des informations de sécurité ou d'identité. En règle générale, les jetons de sécurité sont protégés par des mécanismes de sécurité et des mécanismes cryptographiques car ils contiennent toujours des informations hautement confidentielles qui ne devraient pas être diffusées.

8 Menaces concernant la sécurité dans les systèmes IdM

La plupart des menaces pesant sur la sécurité dans le cyberespace existent a priori également dans les systèmes IdM, ces derniers étant exploités dans le cyberespace. On trouvera dans [UIT-T X.1205] une description des menaces générales pesant sur la sécurité dans le cyberespace.

Dans les systèmes IdM, diverses menaces pour la sécurité rendent les systèmes vulnérables ou peuvent compromettre leur sécurité de telle manière qu'une organisation peut être exposée à un grand danger.

8.1 Sécurité des systèmes

En règle générale, la sécurité des systèmes consiste à protéger le matériel et les données des utilisateurs. L'objectif est que seuls les utilisateurs autorisés puissent accéder au matériel et uniquement pour les finalités recherchées par le propriétaire. En outre, le système devrait être utilisé à ces fins. Les attaquants ne devraient pas pouvoir déposséder les utilisateurs légitimes des ressources.

8.1.1 Accès et utilisation non autorisés

Les utilisateurs non autorisés ne devraient pas pouvoir accéder à la plupart des systèmes, ni les utiliser. Les systèmes IdM devraient être très stricts pour prévenir ce type de vulnérabilité sur le plan de la sécurité puisque l'accès non autorisé à une identité stockée dans un système IdM peut entraîner d'autres menaces pour la sécurité, par exemple le vol ou l'usurpation d'identité.

8.1.2 Utilisation inappropriée

L'utilisation inappropriée suppose qu'un utilisateur peut se servir d'un système IdM pour traiter ou effectuer une tâche pour laquelle le système n'a pas été conçu au départ. Un utilisateur autorisé ne devrait pouvoir utiliser que les parties du système IdM ne nécessitant pas de privilèges propres. Certains services ne sont accessibles qu'aux seuls utilisateurs autorisés, d'autres qu'à certains utilisateurs et d'autres encore sont interdits à tous, sauf aux administrateurs.

8.1.3 Déni de service

En règle générale, un système IdM est le premier point d'accès pour un utilisateur qui souhaite utiliser des services d'application. Par conséquent, il est très probable que les systèmes IdM soient la cible d'attaques visant à interrompre la fourniture de services. Il existe un large éventail d'attaques pouvant amener un système IdM à refuser le service. Les attaques par déni de service sont souvent très faciles à exécuter et difficiles à arrêter. Bon nombre d'entre elles sont conçues pour consommer des ressources informatiques énormes et, ainsi, rendre difficile ou impossible la desserte des utilisateurs légitimes.

8.2 Menaces passives concernant la sécurité

Dans le cas de menaces passives, l'attaquant lit des paquets du réseau mais ne les écrit pas. Le plus simple pour lancer une telle attaque est de se trouver sur le même réseau local que la victime. Dans la plupart des configurations habituelles de réseau local, y compris Ethernet, 802.3 et FDDI, toutes les machines connectées au réseau peuvent lire la totalité du trafic destiné à l'une quelconque des autres machines connectées au même réseau local.

Il convient d'accorder une attention spéciale aux canaux de communications hertziennes, d'autant plus que les réseaux locaux hertziens, par exemple ceux utilisant 802.11, sont depuis peu de plus en plus populaires. Dans la mesure où les données sont simplement radiodiffusées sur des fréquences connues de tous, un attaquant a juste besoin de pouvoir recevoir ces émissions. Ces canaux sont particulièrement vulnérables aux attaques passives. Un grand nombre de canaux de ce type sont associés à une protection cryptographique, mais bien souvent, cette technologie de sécurité n'est pas utilisée avec une configuration adaptée.

8.2.1 Violation de la confidentialité

Une attaque visant la confidentialité consiste à violer une conversation ou une communication privée passant par une ligne de communication. Dans le cas de l'Internet, les informations confidentielles continuent, dans de nombreux cas, d'être transmises sous une forme non codée. Tout justificatif obtenu grâce à une attaque de ce type peut être réutilisé pour d'autres attaques.

8.2.2 Reniflage de mot de passe

Le reniflage de mot de passe consiste à obtenir les mots de passe des utilisateurs transmis dans le réseau dans le but d'utiliser des ressources sans autorisation. Un attaquant qui peut lire ce trafic est donc en mesure d'intercepter un mot de passe et de le reproduire. En d'autres termes, il peut se connecter au système IdM et voler les informations d'identité d'un utilisateur.

8.3 Menaces actives concernant la sécurité

Une attaque nécessitant l'écriture de données dans le réseau ou dans le système est dite "active". Les attaques actives sont des intrusions dans un réseau informatique qui ont pour objet de supprimer ou de modifier les données stockées dans les systèmes IdM du réseau. Il s'agit de la forme d'attaque la plus grave puisque les activités de nombreuses entreprises reposent entièrement sur ces données.

8.3.1 Attaques par répétition

Dans ce cas de figure, l'attaquant enregistre une série de messages hors réseau et les "rejoue" à la partie qui les a reçus au départ. Il est à noter qu'il n'est pas nécessaire que l'attaquant comprenne les messages. Il doit simplement pouvoir les intercepter et les retransmettre.

8.3.2 Attaque de l'homme du milieu

L'attaquant compromet le flux de communication pour faire croire à l'expéditeur qu'il est le destinataire et au destinataire qu'il est l'expéditeur. Il s'agit d'une attaque grave car l'identité de l'expéditeur et celle du destinataire sont usurpées. Par conséquent, bon nombre de techniques visant à assurer l'intégrité du flux de communication ne suffisent pas pour se prémunir contre les attaques de ce type. Le risque d'attaque du milieu existe dès lors qu'un protocole ne prévoit pas d'authentification de l'entité homologue.

8.4 Menaces concernant la sécurité du système IdM

Ces menaces sont celles qui concernent en particulier les systèmes IdM. Les menaces énumérées ci-après sont les principaux points faibles sur le plan de la sécurité contre lesquels tout système IdM devrait prévoir des contre-mesures adaptées.

8.4.1 Menaces relatives aux mots de passe

L'une des menaces relatives aux mots de passe est due à l'utilisation d'un mot de passe faible. Si l'utilisateur choisit un mot de passe faible – c'est-à-dire pouvant être deviné – pour s'authentifier, une attaque de type dictionnaire est alors possible. De même, un problème surviendra si l'utilisateur choisit le même mot de passe faible pour se connecter à différents sites web. Dans ce cas, un site web présentant une faille de sécurité peut être attaqué et révéler le mot de passe d'un utilisateur; l'attaquant n'a alors plus qu'à essayer de se connecter aux autres sites web en utilisant le mot de passe volé.

La deuxième menace est le reniflage de mot de passe par un logiciel espion installé sur un ordinateur. Un ordinateur peut être infecté par un logiciel espion capable d'intercepter le mot de passe d'un utilisateur ou d'un administrateur.

8.4.2 Accès non autorisé

L'accès non autorisé renvoie à un certain nombre d'attaques de différents types. Le but ultime de l'attaquant est d'accéder de façon illégitime aux ressources [UIT-T X.1205].

Un système assurant des services d'authentification et d'identité doit être disponible et accessible pour toutes les parties qui ont besoin de connaître l'identité de l'utilisateur pour fournir des services d'application. Par conséquent, il faut un mécanisme de contrôle d'accès à granularité fine pour protéger le système contre les accès non autorisés.

8.4.3 Ecoute clandestine

L'écoute clandestine est une menace difficile à détecter. Ici, le but de l'attaquant est d'écouter ou, le plus souvent, d'enregistrer les données brutes sur le réseau local de l'entreprise. Cette attaque utilise le "mode promiscuité" des adaptateurs Ethernet en série qui sont vendus sur le marché. Ce mode permet à un attaquant de saisir chaque paquet circulant sur le réseau. Actuellement, il existe sur le web une multitude de renifleurs de réseau gratuits, qu'un attaquant peut utiliser pour procéder à des écoutes clandestines [UIT-T X.1205].

En règle générale, les systèmes IdM communiquent avec des utilisateurs et d'autres entités pour échanger des justificatifs et des informations d'identité souvent confidentielles par l'intermédiaire de réseaux filaires ou hertziens. Par conséquent, toute information obtenue au moyen d'une écoute clandestine peut aboutir à un vol d'identité.

8.4.4 Hameçonnage

L'hameçonnage consiste, pour une tierce partie, à demander des informations confidentielles à un individu, un groupe ou une organisation, en simulant ou en détournant une marque spécifique, généralement connue, avec comme finalité habituelle, le produit financier. Un intrus tente de tromper les utilisateurs en les amenant à révéler des données personnelles, par exemple un numéro de carte de crédit, un justificatif d'identité bancaire en ligne et d'autres informations à caractère sensible, qu'il pourra ensuite utiliser pour commettre des actes frauduleux. Un site web d'hameçonnage est un site conçu pour simuler le site web légitime de l'organisation dont la marque est détournée. Dans les systèmes de gestion d'identité, l'hameçonnage représente une grave menace, dans la mesure où les informations d'authentification de la victime, ou d'autres informations d'identification personnelle, peuvent être utilisées, une fois saisies par un intrus, pour usurper une identité ou commettre d'autres activités frauduleuses.

8.4.5 Vol d'identité

Il s'agit d'une question de sécurité de premier plan, en particulier pour les organisations qui stockent et gèrent un volume important d'informations d'identité personnelle. Non seulement ce type d'atteinte qui entraîne la perte de données personnelles peut entamer la confiance des clients et des institutions et nuire gravement à la réputation d'une organisation, mais la violation des données peut également avoir un coût financier élevé pour les organisations.

9 Lignes directrices pour la sécurité des systèmes IdM

Les lignes directrices pour la sécurité décrites dans les § 9.1 et 9.2 expliquent comment sécuriser le déploiement et l'exploitation d'un système IdM général. Elles définissent les prescriptions de base en matière de sécurité pour un système IdM qui peut être déployé et exploité de façon sécurisée dans différents environnements informatiques. Les paragraphes 9.3, 9.4 et 9.5 traitent des entités qui composent le système IdM (serveur IdM, client et client mobile). Le paragraphe 9.6 présente des considérations relatives à la confidentialité dans les systèmes IdM.

9.1 Lignes directrices pour la sécurité du déploiement des systèmes IdM

Le présent paragraphe expose des lignes directrices à appliquer pour sécuriser l'installation et le déploiement d'un système IdM. Dans la plupart des cas, il faudra prendre les dispositions nécessaires pour assurer la gestion de la confiance et des clés.

9.1.1 Gestion de la confiance

Pour délivrer une autorisation, un système IdM doit avoir confiance dans le fait qu'une identité et ses attributs sont authentiques et corrects. Par conséquent, une identité n'est utile que lorsqu'elle a été autorisée. L'autorité est établie sur la base de la confiance. Le plan de gestion de la confiance est la première étape pour déployer et exploiter correctement un système IdM.

L'infrastructure PKI (infrastructure de clé publique) est l'un des mécanismes de confiance essentiels pour les systèmes de gestion d'identité. Sa vocation principale est de fournir un certificat de clé publique pouvant être utilisé pour s'authentifier et sécuriser un canal. Dans un système IdM à grande échelle, il est vivement recommandé d'utiliser une infrastructure PKI pour établir un tiers de confiance. Le certificat délivré par l'infrastructure PKI peut être utilisé pour authentifier un utilisateur auprès du système IdM et crypter un canal de communication dans une couche SSL. La signature numérique est une autre application majeure du certificat.

9.1.2 Sécurité des réseaux

Il est essentiel qu'un environnement de réseau soit sécurisé de plusieurs façons. Tout d'abord, le périmètre du réseau devrait être sécurisé à l'aide d'un pare-feu. Tout système IdM doit être situé à l'intérieur du périmètre du pare-feu. En outre, des mécanismes de sécurité de réseau plus sophistiqués, par exemple VPN et IDS/IPS, peuvent être utilisés pour renforcer la sécurité des environnements de réseau.

9.1.3 Environnement d'hébergement sécurisé

On entend par environnement d'hébergement l'endroit où un système IdM est installé et exploité. Les serveurs ou les postes de travail sur lesquels on compte installer un élément du système IdM doivent être préalablement équipés de programmes antivirus et de programmes de protection du clavier. Il faudrait garantir que l'environnement d'hébergement n'a pas été compromis par une quelconque attaque visant la sécurité avant l'installation et le déploiement d'un système IdM.

9.1.4 Stockage sécurisé

De nombreuses données importantes et sensibles sont stockées dans des mémoires telles qu'une base de données ou un serveur d'annuaire. Au moment de sa mise en place, le serveur de stockage devrait être installé sur un ordinateur sécurisé et un compte d'administrateur devrait être créé sur la base des lignes directrices d'installation appropriées pour empêcher qu'un compte indésirable puisse être ouvert et utilisé par la suite pour attaquer le système.

9.2 Lignes directrices pour la sécurité de l'exploitation des systèmes IdM

Le présent paragraphe présente les lignes directrices pour la sécurité de l'exploitation d'un système IdM. Le contrôle d'authentification et d'accès est l'un des principaux aspects à traiter.

9.2.1 Signature numérique

La signature numérique est le mécanisme de sécurité qui peut garantir l'authenticité et l'intégrité d'un message qui est signé. Dans un système IdM, l'utilisateur doit, à de nombreuses occasions, prouver sa volonté ou son consentement pour pouvoir effectuer des transactions numériques. Dans ce cas, la signature numérique employée peut servir de preuve pour vérifier son intégrité.

9.2.2 Cryptage

Le système IdM a besoin d'un cryptage à différents niveaux de fonctionnement. Tout d'abord, les messages échangés entre des entités doivent être cryptés, dans la mesure où la confidentialité est requise. En fonction de la politique d'exploitation du système IdM, certaines des données stockées dans une base de données doivent être cryptées afin d'en protéger la confidentialité et d'empêcher un accès non autorisé. Le cryptage assurera un niveau de confidentialité maximal pour le système IdM et garantira au final la confidentialité des données d'un utilisateur et de ses informations d'identité.

9.2.3 Authentification

L'authentification est une fonction de rempart destinée à empêcher des utilisateurs illégitimes d'accéder à un système sans autorisation. Sur l'Internet, l'authentification simple par identifiant/mot de passe est très courante mais présente de nombreux points faibles du point de vue de la sécurité. Par conséquent, il est recommandé d'utiliser une authentification forte dès lors qu'il est nécessaire d'assurer un niveau de confiance élevé dans un utilisateur qui accède au système. L'authentification mutuelle peut permettre de réduire le risque d'attaque par hameçonnage ou par détournement d'adresse.

9.2.4 Communication sécurisée

La plupart des informations échangées entre un utilisateur et un système IdM concernent la vie privée et sont confidentielles par nature. En outre, les messages de protocole échangés par les entités peuvent comporter des informations sensibles et confidentielles qui doivent être cryptées sur les lignes de communication. Il est possible de sécuriser les communications en utilisant des technologies existantes, par exemple une couche SSL ou un réseau privé virtuel.

9.2.5 Contrôle d'accès

Différentes entités, par exemple des administrateurs et des utilisateurs, peuvent accéder à un système IdM pour profiter d'un service ou effectuer une opération de maintenance courante. Il faut un mécanisme de contrôle d'accès adapté pour empêcher des tiers malintentionnés de s'introduire dans le système. Dans la plupart des cas, un contrôle d'accès de type discrétionnaire (c'est-à-dire, des listes de contrôle d'accès) devrait suffire. Toutefois, lorsqu'un modèle de contrôle d'accès plus sécurisé et plus souple est nécessaire, il est possible d'appliquer un modèle de contrôle d'accès fondé sur les rôles qui permet un contrôle à granularité fine plus sophistiqué.

9.3 Lignes directrices pour la sécurité des serveurs IdM

Le présent paragraphe contient des lignes directrices de sécurité particulières pour les serveurs IdM installés et exploités sur des postes de travail ou des serveurs de grande taille.

9.3.1 Sécuriser le système d'exploitation

Les serveurs IdM les plus courants ont un système d'exploitation à vocation générale. Il est possible d'éviter bon nombre des problèmes de sécurité en configurant correctement le système d'exploitation utilisé par le serveur IdM. Etant donné que le serveur IdM est installé sur le système d'exploitation existant, sa sécurité dépend pour beaucoup de celle du système d'exploitation. Les techniques permettant de sécuriser les différents systèmes d'exploitation sont très diverses; par conséquent, le présent paragraphe porte sur les procédures génériques communes à la sécurisation de la plupart des systèmes d'exploitation. [UIT-T X.1205] et [b-NIST SP 800-123] décrivent les fonctions de base de la gestion de la sécurité dans les systèmes d'exploitation.

Pour sécuriser les serveurs IdM, il faut sécuriser le système d'exploitation en appliquant les mesures de base suivantes:

– Appliquer les correctifs et les mises à jour du système d'exploitation.
– Renforcer et configurer le système d'exploitation pour qu'il assure une sécurité adéquate.
– Installer et configurer d'autres mécanismes de contrôle de la sécurité, si besoin est.
– Tester la sécurité du système d'exploitation afin de s'assurer que les mesures prises précédemment permettent de résoudre tous les problèmes de sécurité.

9.3.2 Configurer l'authentification des utilisateurs

Dans le cas de serveurs IdM, seuls quelques administrateurs de serveur désignés devraient être autorisés à configurer le serveur. Pour appliquer les restrictions de politique, le cas échéant, l'administrateur devrait configurer le serveur de sorte qu'il authentifie un utilisateur en demandant la preuve que celui-ci a une autorisation pour ce type d'accès. Dans le cas de serveurs IdM devant assurer des niveaux élevés de confiance, les organisations pourront également utiliser du matériel d'authentification infalsifiable, par exemple des jetons ou des dispositifs à mot de passe à usage unique. Dans ce cas, il est vivement déconseillé d'utiliser des mécanismes d'authentification dans le cadre desquels les informations d'authentification peuvent être réutilisées (par exemple, les mots de passe) et transmises sous forme de texte en clair sur un réseau non fiable car les informations peuvent être interceptées et utilisées par un attaquant pour usurper l'identité d'un utilisateur autorisé.

Par défaut, la configuration du système d'exploitation comprend souvent des comptes d'invités avec ou sans mot de passe. L'administrateur devrait supprimer ou désactiver les comptes d'invités non utilisés afin que les attaquants ne puissent pas s'en servir.

9.3.3 Configurer le contrôle d'accès

La plupart des serveurs IdM permettent de définir des privilèges d'accès pour chaque justificatif ou chaque information d'identité. Un utilisateur qui accède à un serveur IdM ne devrait pas être autorisé à accéder aux informations d'identité d'autres utilisateurs. La configuration adéquate des contrôles d'accès peut contribuer à empêcher la divulgation d'informations d'identité sensibles ou à diffusion limitée qui ne sont pas destinées à être communiquées au public. En outre, il est possible d'utiliser les contrôles d'accès pour limiter l'utilisation des ressources en cas d'attaque par déni de service contre le serveur.

9.3.4 Enregistrement

L'enregistrement est une partie essentielle des contre-mesures efficaces en matière de sécurité. Il est très important que les journaux contiennent des données correctes et soient par la suite contrôlés attentivement. Les journaux des réseaux et des systèmes sont importants, en particulier les journaux systèmes dans le cas de communications cryptées, la surveillance du réseau étant quant à elle moins efficace.

L'examen des journaux est obligatoire et constitue une façon efficace de découvrir une activité suspecte. Dans de nombreux cas, les fichiers de consignation sont souvent la seule trace d'un comportement suspect. Si l'on permet aux mécanismes d'enregistrer des informations, il est alors possible d'utiliser les journaux correspondants pour détecter les tentatives d'intrusion, réussies ou ratées, et de déclencher les mécanismes d'alerte lorsqu'un complément d'enquête est nécessaire. Des procédures et des outils doivent être en place pour traiter et analyser les fichiers de consignation et examiner les notifications d'alerte.

Il faudrait veiller à ce que les contrôles d'accès puissent appliquer une séparation des tâches en s'assurant que les journaux du serveur ne peuvent pas être modifiés par les administrateurs et, éventuellement, que le serveur est uniquement autorisé à annexer les fichiers de consignation.

9.4 Lignes directrices pour la sécurité des clients IdM

Le présent paragraphe décrit des lignes directrices pour assurer la sécurité lorsqu'un programme client IdM est exploité. Lorsqu'un navigateur Internet est utilisé comme client IdM, la vulnérabilité sur le plan de la sécurité dépend du navigateur lui-même. Néanmoins, il est toujours possible d'appliquer une partie des lignes directrices pour assurer la sécurité de l'environnement client.

9.4.1 Distribution sécurisée d'un programme client

A l'heure actuelle, la plupart des plug-ins liés au navigateur sont téléchargés depuis un site web. Si un utilisateur télécharge par accident un programme client IdM pouvant nuire à son système, aucun mécanisme de sécurité, aussi fort soit-il, ne pourra protéger l'utilisateur contre un acte de malveillance. Par conséquent, les fournisseurs de programme client IdM doivent faire en sorte que l'intégrité d'un programme client distribué soit protégée et que ce programme offre un moyen sécurisé de valider son intégrité.

9.4.2 Intégrité d'un programme client

La signature numérique est l'une des meilleures solutions pour assurer l'intégrité d'un programme client. Si le programme client est signé par un fournisseur et qu'un certificat de signature est fourni en vue d'une validation, l'utilisateur peut alors télécharger le programme en toute sécurité et vérifier l'intégrité du code du programme. Une autre méthode consiste à utiliser un algorithme de hachage pour garantir l'intégrité du code. Le code du client est la donnée d'entrée que l'algorithme de hachage utilise pour produire une valeur de hachage, qui est le résumé du code du client. Si la

valeur de hachage est publiée sur le web de façon sécurisée, l'utilisateur peut valider son programme client en calculant la valeur de hachage du programme client téléchargé. Toutefois, la première méthode décrite est plus sûre que la seconde.

9.4.3 Fichier de base de données cliente

Les fichiers d'une base de données cliente devraient être stockés de façon sécurisée. L'accès à la base de données devrait être strictement limité aux utilisateurs authentifiés. Dans la plupart des cas, un client IdM gère les informations de justificatif des utilisateurs, y compris les mots de passe et les jetons de sécurité, qui devraient être conservées sous forme cryptée pour assurer la confidentialité. En outre, le fichier de base de données lui-même devrait être protégé contre toute altération ou modification illicite pour garantir son intégrité. Lorsque le fichier de base de données est supprimé d'un système, il ne devrait rester sur le disque dur aucune trace permettant de récupérer les données ultérieurement.

9.4.4 Mot de passe sécurisé

Le mécanisme de sécurité dépend finalement en grande partie du mot de passe permettant de s'identifier et d'accéder au système. Si l'utilisateur choisit un mot de passe faible qui peut être percé par une attaque de force, alors aucun autre mécanisme de sécurité ne peut protéger le système contre les utilisateurs malintentionnés. Par conséquent, la plus importante des tâches pour un fournisseur de service IdM consiste à faire en sorte que l'utilisateur choisisse un mot de passe fort pour sécuriser sa connexion.

9.4.5 Désinstallation d'un programme client

Lors de la désinstallation d'un programme client, tous les mots de passe, justificatifs et informations d'identité, ainsi que la configuration personnelle du programme client, devraient être définitivement supprimés.

9.5 Lignes directrices pour la sécurité des clients IdM mobiles

Le présent paragraphe décrit des lignes directrices pour la sécurité des clients IdM mobiles qui sont installés et exploités sur un dispositif mobile. Le dispositif mobile a des caractéristiques particulières, comme la portabilité et la mobilité, qui peuvent être des points faibles sur le plan de la sécurité si un attaquant décide de les exploiter.

9.5.1 Dispositif perdu ou volé

Un dispositif mobile étant portable, les risques de perte ou de vol sont très élevés. Il existe de nombreuses manières de s'introduire dans un dispositif mobile pour en extraire des informations personnelles pouvant servir à une fraude d'identité. Par conséquent, le client mobile à l'intérieur d'un dispositif devrait être préparé à l'éventualité d'une attaque visant la sécurité susceptible de donner lieu à une utilisation non autorisée ou à une fraude d'identité. En cas de perte ou de vol du dispositif, l'incident est signalé au fournisseur de communication mobile qui, selon la situation, peut verrouiller le dispositif à distance et empêcher quiconque d'y accéder. Cette mesure est appropriée lorsque le dispositif a été perdu dans un environnement "sans risque", par exemple au domicile ou sur le lieu de travail du propriétaire. Dans tous les autres cas, l'opérateur devrait pouvoir effacer les informations personnelles ou le dossier d'identité stockés dans le dispositif si le propriétaire pense que le dispositif est perdu définitivement ou volé et qu'il n'existe aucun moyen de le récupérer.

9.5.2 Authentification du dispositif

Si le dispositif mobile est équipé d'un écran de petite taille, il est alors très difficile pour l'utilisateur de se connecter au dispositif avec un mot de passe alphanumérique à chaque utilisation. Dans ce cas, le numéro d'identification personnel (code PIN) sert de mot de passe, mais dans de nombreux cas, ce mode d'authentification n'est pas utilisé pour des questions de commodité. Pour remédier à cette situation, le client mobile du système IdM devrait proposer des mécanismes d'authentification

conviviaux mais suffisamment sécurisés et adaptés au dispositif mobile. Le client mobile doit appliquer l'authentification par mot de passe si le dispositif ne prévoit aucun mécanisme d'authentification lorsque l'utilisateur ouvre une session.

9.5.3 Sauvegarde des bases de données

La plupart des informations d'identité sont rassemblées et traitées à l'intérieur d'un dispositif mobile pour différents services. Toutefois, ces identités sont souvent des informations personnelles sensibles et privées dont l'intégrité et la confidentialité doivent être protégées. Comme indiqué précédemment, les risques de perte ou de vol d'un dispositif sont élevés. Par conséquent, le client mobile d'un système IdM doit permettre d'effectuer une sauvegarde de la base de données contenant les informations d'identité. Deux méthodes sont possibles pour ce faire. La première consiste à effectuer une sauvegarde de la base de données dans une mémoire secondaire, par exemple sur une carte mémoire SD (numérique sécurisée) si le dispositif le permet. La seconde méthode consiste à utiliser un serveur de sauvegarde externe afin d'offrir au client un service de sauvegarde des bases de données. Dans ce cas, il est toujours possible de rétablir la base de données, même en cas de perte ou de vol du dispositif.

9.5.4 Sécurité des communications mobiles

La plupart du temps, les dispositifs mobiles communiquent entre eux via des communications mobiles. Toutefois, on sait que les communications mobiles sont très vulnérables aux attaques actives ou passives. Le client mobile d'un système IdM transmet en règle générale des informations personnelles sensibles sur des liaisons mobiles. Par conséquent, l'intégrité et la confidentialité de toute communication avec un client mobile passant par des liaisons mobiles doivent être protégées grâce à un mécanisme de sécurité dans la couche de transport.

9.6 Considérations relatives à la confidentialité dans les systèmes IdM

La confidentialité est une question très importante dans le contexte de la sécurité IdM. Toutefois, chaque pays doit tenir compte de nombreuses règles et réglementations lorsqu'il souhaite mettre en œuvre des lignes directrices en matière de confidentialité. Par conséquent, le présent paragraphe traite d'éléments liés à la confidentialité dans le contexte des systèmes IdM, éléments qui sont donnés pour information.

9.6.1 Consentement de l'utilisateur

Lorsqu'une identité est collectée auprès d'un utilisateur et utilisée par un fournisseur d'identité ou un fournisseur de services, le consentement de l'utilisateur devrait être obtenu de manière explicite. L'idéal est d'obtenir le consentement de l'utilisateur sous la forme d'une signature numérique, qui peut être vérifiée ultérieurement au besoin.

9.6.2 Choix de l'identité

Les systèmes IdM donnent explicitement à un utilisateur la possibilité de choisir s'il autorise ou non la collecte, le transfert, l'utilisation, le stockage, l'archivage ou la suppression de son identité. La confidentialité est accrue pour l'utilisateur puisque c'est lui qui gère la politique d'identité et de confidentialité. Il conviendrait de tenir compte de cette approche centrée sur l'utilisateur lors de la conception du système IdM.

9.6.3 Finalité de l'identité

Les systèmes IdM devraient indiquer à l'utilisateur, de manière aisément compréhensible et avant de la collecte de l'identité, toutes les finalités pour lesquelles les informations personnelles sont recueillies et utilisées. En outre, le système devrait, dans la mesure du raisonnable, s'efforcer d'utiliser l'identité pour la finalité indiquée.

9.6.4 Limitation et réduction au strict minimum des données d'identité

Les systèmes IdM qui collectent l'identité ne devraient demander que les données nécessaires pour atteindre les finalités identifiées, sauf en cas de consentement de l'individu ou selon ce qui est autorisé ou nécessaire aux termes de la loi.

Le système IdM qui collecte les identités devrait appliquer de façon minutieuse des procédures indiquant clairement quelles sont les données d'identité nécessaires avec quelle finalité et comment s'assurer que toutes les opérations de traitement de l'identité ne collectent que le plus petit nombre de données nécessaires pour leur finalité.

9.6.5 Suppression d'identité

Les systèmes IdM devraient supprimer l'identité une fois que la finalité indiquée a été atteinte et si aucune autre obligation juridique ou réglementaire n'impose une période de conservation. Lorsqu'une identité est supprimée, il faudrait veiller à supprimer également toutes les données d'identité stockées dans des systèmes connexes, par exemple dans les systèmes de sauvegarde ou d'archives.

9.6.6 Configuration de la politique de confidentialité

Avant d'exploiter un système IdM, on pourra configurer des politiques de confidentialité, par exemple des politiques de préférence de confidentialité ou d'autorisation de confidentialité. Cette politique régit l'utilisation de l'identité qui est soumise au système par un utilisateur.

9.6.7 Anonymat

L'anonymat peut être l'objectif ultime à atteindre dans un système IdM à confidentialité renforcée. Toutefois, il s'agit d'une fonction très complexe et difficile à proposer à un coût raisonnable. Par conséquent, dans la plupart des cas, l'utilisation d'un pseudonyme peut permettre de répondre aux besoins de confidentialité d'un système IdM.

Bibliographie

[b-NIST SP 800-123] Scarfone, K.A., Jansen, W., and Miles, T. (2008), *Guide to General Server Security*, NIST Special Publication SP-800-123.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2012