UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.810

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(11/95)

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

SÉCURITÉ

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: APERÇU GÉNÉRAL

Recommandation UIT-T X.810

(Antérieurement «Recommandation du CCITT»)

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution nº 1 de la Conférence mondiale de normalisation des télécommunications (CMNT) (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie 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. Le texte de la Recommandation X.810 de l'UIT-T a été approuvé le 21 novembre 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10181-1.

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.

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

(Février 1994)

ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X

Domaine	Recommandations
RÉSEAUX PUBLICS POUR DONNÉES	
Services et services complémentaires	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalisation et commutation	X.50-X.89
Aspects réseau	X.90-X.149
Maintenance	X.150-X.179
Dispositions administratives	X.180-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200-X.209
Définition des services	X.210-X.219
Spécifications des protocoles en mode connexion	X.220-X.229
Spécifications des protocoles en mode sans connexion	X.230-X.239
Formulaires PICS	X.240-X.259
Identification des protocoles	X.260-X.269
Protocoles de sécurité	X.270-X.279
Objets gérés de couche	X.280-X.289
Test de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Considérations générales	X.300-X.349
Systèmes mobiles de transmission de données	X.350-X.369
Gestion	X.370-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	
Réseautage	X.600-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850-X.859
Traitement des transactions	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

TABLE DES MATIÈRES

Résumé

La présente Recommandation | Norme internationale définit le cadre dans lequel les services de sécurité pour les systèmes ouverts sont spécifiés. Cette partie des cadres de sécurité définit l'organisation du cadre de sécurité, définit les concepts de sécurité requis dans plusieurs parties des cadres de sécurité, et décrit les interrelations des services et mécanismes identifiés dans les autres parties du cadre.

Introduction

Plusieurs applications ont des besoins de sécurité pour protéger les communications d'information contre les menaces. Quelques menaces connues ainsi que les services et mécanismes de sécurité qui peuvent être utilisés pour s'en protéger sont décrites dans la Rec. X.800 du CCITT | ISO 7498-2.

La présente Recommandation | Norme internationale définit le cadre dans lequel les services de sécurité pour les systèmes ouverts sont spécifiés.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: APERÇU GÉNÉRAL

1 Domaine d'application

Les cadres de sécurité concernent l'application des services de sécurité dans l'environnement des systèmes ouverts, où le terme *systèmes ouverts* est utilisé pour inclure des domaines comme les bases de données, les applications distribuées, le traitement ODP et l'interconnexion OSI. Les cadres de sécurité sont impliqués dans la définition des moyens d'offrir la protection pour les systèmes et les objets au sein des systèmes, ainsi que les interactions entre systèmes. Ils ne couvrent pas la méthodologie de construction des systèmes ou des mécanismes.

Les cadres de sécurité traitent à la fois des éléments de données et des séquences d'opérations (mais pas des éléments de protocole) utilisés pour obtenir des services spécifiques de sécurité. Ces services de sécurité peuvent s'appliquer aux entités communicantes des systèmes aussi bien qu'aux données échangées entre systèmes, et aux données gérées par les systèmes.

Les cadres de sécurité fournissent la base pour une normalisation ultérieure, fournissant une terminologie cohérente et des définitions d'interfaces de service générique abstrait pour des besoins de sécurité spécifiques. Ils classifient également les mécanismes qui peuvent être utilisés pour répondre à ces besoins.

Un service de sécurité dépend fréquemment d'autres services de sécurité, rendant difficile l'isolation d'une partie de la sécurité des autres parties. Les cadres de sécurité font intervenir des services de sécurité particuliers, décrivent la gamme des mécanismes qui peuvent être utilisés pour fournir les services de sécurité et identifient les interdépendances entre les services et les mécanismes. La description de ces mécanismes peut mettre en jeu la confiance envers un service de sécurité différent, et c'est de cette façon que les cadres de sécurité décrivent la confiance d'un service de sécurité envers un autre.

Cette partie des cadres de sécurité:

- décrit l'organisation des cadres de sécurité;
- décrit les concepts de sécurité qui sont requis dans plus d'une partie des cadres de sécurité;
- décrit la corrélation entre les services et mécanismes identifiés dans les autres parties des cadres.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision, et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: Le modèle de référence de base.*

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

– Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

3 Définitions

Les définitions suivantes sont utilisées dans l'aperçu général ou sont communes à deux parties consécutives ou plus des cadres de sécurité.

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.1 Définitions du modèle de référence de base

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

– couche (N);
– entité (N);
– unité de données de protocole (N);
– processus d'application;
– système réel ouvert;
– système réel.

3.2 Définitions de l'architecture de sécurité

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.800 du CCITT | ISO 7498-2:

– contrôle d'accès;
– disponibilité;
– cryptogramme;
– valeur de contrôle cryptographique;
– déchiffrement;
– déni de service;
– signature numérique;
– chiffrement;
– menace de l'intérieur;
– clé;
– gestion de clé;
– texte en clair;
– menace de l'extérieur;
– audit de sécurité;
– étiquette de sécurité;
– politique de sécurité;
– sensibilité;
– menace.

3.3 Définitions additionnelles

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.3.1 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.

NOTE – Avec certains algorithmes asymétriques de cryptographie, il faut utiliser plus d'une clé privée pour déchiffrer un cryptogramme ou pour générer une signature numérique.

3.3.2 autorité de certification: entité habilitée à laquelle il est fait confiance (dans le contexte d'une politique de sécurité) pour créer des certificats de sécurité contenant une ou plusieurs classes de données relatives à la sécurité.

3.3.3 entité de confiance conditionnelle: entité à laquelle il est fait confiance dans le contexte d'une politique de sécurité, mais qui ne peut pas violer la politique de sécurité sans être détectée.

3.3.4 chaînage cryptographique: mode d'utilisation d'un algorithme cryptographique dans lequel la transformation effectuée par l'algorithme dépend des valeurs des entrées ou sorties précédentes.

3.3.5 empreinte numérique: caractéristique d'un élément de données, telle qu'une valeur de contrôle cryptographique ou le résultat de la réalisation d'une fonction de hachage unidirectionnelle sur les données, qui est suffisamment spécifique à l'élément de données pour qu'il ne soit pas possible de trouver, de façon informatique, un autre élément de données ayant les mêmes caractéristiques.

3.3.6 identificateur caractéristique: données qui identifient de façon univoque une entité.

3.3.7 fonction de hachage: fonction (mathématique) qui fait correspondre les valeurs d'un grand ensemble (potentiellement très grand) de valeurs à une gamme plus réduite de valeurs.

3.3.8 fonction unidirectionnelle: fonction (mathématique) qu'il est facile de calculer mais pour laquelle, lorsque le résultat est connu, il n'est pas possible de trouver, de façon informatique, n'importe laquelle des valeurs qui auraient pu être fournies pour obtenir celui-ci.

3.3.9 fonction de hachage unidirectionnelle: fonction (mathématique) qui est à la fois une fonction unidirectionnelle et une fonction de hachage.

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

3.3.11 clé publique: clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique.

3.3.12 certificat de révocation: certificat de sécurité émis par une autorité de sécurité pour indiquer qu'un certificat de sécurité particulier a été révoqué.

3.3.13 certificat de révocation de liste: certificat de sécurité qui identifie une liste de certificats de sécurité qui ont été révoqués.

3.3.14 scellé: valeur de contrôle cryptographique qui met en œuvre l'intégrité mais qui ne protège pas d'une falsification du récepteur (c'est-à-dire qu'il n'offre pas la non-répudiation). Lorsqu'un scellé est associé à un élément de données, cet élément de données est dit *scellé*.

NOTE – Bien qu'un scellé n'offre pas lui-même la non-répudiation, certains mécanismes de non-répudiation font usage du service d'intégrité offert par les scellés, par exemple, pour protéger les communications avec des tierces parties de confiance.

3.3.15 clé secrète: clé qui est utilisée avec un algorithme symétrique de cryptographie. La possession de cette clé est limitée (habituellement à deux entités).

3.3.16 administrateur de sécurité: personne qui est responsable de la définition ou de l'application d'une ou de plusieurs parties de la politique de sécurité.

3.3.17 autorité de sécurité: entité qui est responsable de la définition, de la mise en œuvre ou de l'application de la politique de sécurité.

3.3.18 certificat de sécurité: ensemble de données relatives à la sécurité émis par une autorité de sécurité ou une tierce partie de confiance ainsi que les informations de sécurité qui sont utilisées pour fournir des services d'intégrité et d'authentification de l'origine des données.

NOTE – Tous les certificats sont réputés être des certificats de sécurité (voir les définitions applicables dans l'ISO 7498-2). Le terme *certificat de sécurité* est adopté afin d'éviter des conflits de terminologie avec la Rec. UIT-T X.509 | ISO/CEI 9594-8 (c'est-à-dire la norme d'authentification de l'annuaire).

3.3.19 chaîne de certificat de sécurité: séquence ordonnée de certificats de sécurité, dans laquelle le premier certificat de sécurité contient des informations relatives à la sécurité et les certificats de sécurité suivants contiennent des informations de sécurité qui peuvent être utilisées pour la vérification des certificats de sécurité précédents.

3.3.20 domaine de sécurité: ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dans lesquels l'ensemble des éléments est sujet à la politique de sécurité, pour les activités spécifiées et la politique de sécurité est administrée par l'autorité de sécurité, pour le domaine de sécurité.

3.3.21 autorité du domaine de sécurité: autorité de sécurité qui est responsable de la mise en œuvre d'une politique de sécurité pour un domaine de sécurité.

3.3.22 information de sécurité: information nécessaire pour mettre en œuvre des services de sécurité.

3.3.23 rétablissement de la sécurité: actions qui sont menées et procédures qui sont utilisées lorsqu'une violation de sécurité est soit détectée soit soupçonnée d'avoir eu lieu.

3.3.24 règles d'interaction sécurisée: règles de politique de sécurité qui régissent des interactions entre domaines de sécurité.

3.3.25 règles de politique de sécurité: représentation d'une politique de sécurité pour un domaine de sécurité au sein d'un système réel.

3.3.26 jeton de sécurité: ensemble de données protégé par un ou plusieurs services de sécurité, ainsi que les informations de sécurité utilisées pour la fourniture de ces services de sécurité, qui est transféré entre les entités communicantes.

3.3.27 algorithme symétrique de cryptographie: algorithme pour réaliser le chiffrement ou algorithme pour réaliser le déchiffrement correspondant dans lequel la même clé est requise à la fois pour le chiffrement et le déchiffrement.

3.3.28 confiance: on dit que l'entité X *fait confiance* à l'entité Y pour un ensemble d'activités si et seulement si l'entité X suppose que l'entité Y se comportera d'une certaine façon par rapport aux activités.

3.3.29 entité de confiance: entité qui peut violer une politique de sécurité, soit en réalisant des actions qu'elle n'est pas censée accomplir, soit en ne réussissant pas à réaliser des actions qu'elle est censée accomplir.

3.3.30 tierce partie de confiance: autorité de sécurité ou son agent auquel il est fait confiance au regard de certaines activités liées à la sécurité (dans le contexte d'une politique de sécurité).

3.3.31 entité de confiance inconditionnelle: entité de confiance qui peut violer une politique de sécurité sans être détectée.

4 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes sont utilisées.

ACI	Information de contrôle d'accès (*access control information*)
OSI	Interconnexion des systèmes ouverts (*open systems interconnection*)
ODP	Traitement réparti ouvert (*open distributed processing*)
SI	Information de sécurité (*security information*)
TTP	Tierce partie de confiance (*trusted third party*)

5 Notation

La notation de couche utilisée est la même que celle qui est définie dans la Rec. UIT-T X.200 | ISO/CEI 7498-1.

Sauf indication contraire, le terme *service* sert à désigner un service de sécurité.

Sauf indication contraire, le terme *certificat* sert à désigner un certificat de sécurité.

6 Organisation

Le cadre de sécurité fait partie d'une Norme internationale multipartie (ISO/CEI 10181) et d'une série de Recommandations de l'UIT. Les cadres de sécurité sont décrits ci-après. Des cadres de sécurité additionnels pourront être identifiés à l'avenir. Le cadre de gestion des clés ne fait pas partie de l'ISO/CEI 10181, mais il a un domaine d'application similaire et sa description est incluse dans un souci d'exhaustivité.

6.1 Partie 1 – Aperçu général

Voir l'article 1.

6.2 Partie 2 – Authentification

Ce cadre décrit tous les aspects d'authentification tels qu'ils s'appliquent aux systèmes ouverts, la relation de l'authentification avec d'autres fonctions de sécurité comme le contrôle d'accès et les besoins de gestion pour l'authentification.

Ce cadre:

a) définit les concepts élémentaires de l'authentification;

b) identifie les classes possibles pour les mécanismes d'authentification;

c) définit les services pour ces classes de mécanismes d'authentification;

d) identifie les besoins fonctionnels pour les protocoles afin de mettre en œuvre ces classes de mécanismes d'authentification;

e) identifie des besoins généraux de gestion pour l'authentification.

Le cadre d'authentification est situé au sommet de la hiérarchie des normes d'authentification qui fournissent les services, la nomenclature et la classification des méthodes d'authentification. Immédiatement en dessous de celui-ci, des normes comme l'ISO/CEI 9798 (mécanismes d'authentification d'entité) fournissent plus en détail un ensemble particulier de ces méthodes. Finalement, au bas de la hiérarchie, des normes comme la Rec. UIT-T X.509 | ISO/CEI 9594-8 (le cadre d'authentification de l'annuaire) utilisent ces concepts et ces méthodes dans le contexte d'une application ou d'un besoin spécifique.

Le cadre d'authentification décrit un modèle d'authentification, un ensemble d'étapes dans lesquelles les activités d'authentification peuvent être rangées par catégories, l'utilisation d'une tierce partie de confiance, l'utilisation de certificats d'authentification pour échanger des informations d'authentification, un service d'authentification générique basé sur ces étapes, et au moins cinq classes de mécanismes d'authentification qui fournissent le service générique d'authentification. Cela comprend des mécanismes protégeant contre la divulgation d'informations d'authentification, et contre la divulgation et la répétition sur les mêmes (et/ou différents) vérificateurs.

6.3 Partie 3 – Contrôle d'accès

Ce cadre définit tous les aspects du contrôle d'accès (c'est-à-dire utilisateur à processus, utilisateur à données, processus à processus, processus à données) dans les systèmes ouverts, les relations avec d'autres fonctions de sécurité, telles que l'authentification et l'audit, et les besoins de gestion pour le contrôle d'accès.

Ce cadre:

a) définit les concepts de base pour le contrôle d'accès;

b) démontre la façon dont les concepts de base du contrôle d'accès peuvent être spécialisés pour mettre en œuvre quelques services et mécanismes de contrôle d'accès communément reconnus;

c) définit ces services et les mécanismes de contrôle d'accès correspondants;

d) identifie les besoins fonctionnels des protocoles pour mettre en œuvre ces services et mécanismes de contrôle d'accès;

e) identifie les besoins de gestion pour mettre en œuvre ces services et mécanismes de contrôle d'accès;

f) traite de l'interaction des services et mécanismes de contrôle d'accès avec d'autres services et mécanismes de sécurité.

Ce cadre de sécurité décrit un modèle de contrôle d'accès, un certain nombre d'étapes dans lesquelles les activités de contrôle d'accès peuvent être rangées par catégories, un service générique de contrôle d'accès basé sur ces étapes, et au moins trois classes de mécanismes de contrôle d'accès qui fournissent le service générique de contrôle d'accès. Cela comprend des listes de contrôle d'accès, des capacités et des étiquettes.

6.4 Partie 4 – Non-répudiation

Ce cadre détaille et étend les concepts des services de non-répudiation décrits dans la Rec. X.800 du CCITT | ISO 7498-2 et fournit un cadre pour le développement et la fourniture de ces services.

Ce cadre:

a) définit les concepts élémentaires de non-répudiation;

b) définit les services généraux de non-répudiation;

c) identifie les mécanismes possibles pour fournir des services de non-répudiation;

d) identifie des besoins généraux de gestion pour des services et mécanismes de non-répudiation.

6.5 Partie 5 – Confidentialité

Le service de confidentialité vise à protéger l'information contre une divulgation non autorisée. Ce cadre traite de la confidentialité des informations pour la recherche, le transfert et la gestion.

Ce cadre:

a) définit les concepts élémentaires de confidentialité;

b) identifie les classes possibles de mécanismes de confidentialité;

c) définit les fonctionnalités de chaque classe de mécanismes de confidentialité;

d) identifie la gestion nécessaire pour mettre en œuvre les classes de mécanismes de confidentialité;

e) traite de l'interaction du mécanisme de confidentialité et des services le mettant en œuvre avec les autres services et mécanismes de sécurité.

Quelques-unes des procédures décrites dans ce cadre de sécurité assurent la confidentialité par l'application de techniques cryptographiques. L'utilisation de ce cadre ne dépend pas de l'utilisation d'une technique cryptographique particulière ou d'autres algorithmes, bien que certaines classes de mécanismes de confidentialité puissent dépendre de propriétés algorithmiques particulières.

6.6 Partie 6 – Intégrité

On appelle intégrité la propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée. Ce cadre couvre l'intégrité des données pour la recherche, le transfert et la gestion des données.

Ce cadre:

a) définit le concept élémentaire d'intégrité;

b) identifie des classes possibles de mécanismes d'intégrité;

c) définit des fonctionnalités pour chaque classe des mécanismes d'intégrité;

d) identifie la gestion nécessaire pour mettre en œuvre les classes des mécanismes d'intégrité;

e) traite de l'interaction des services supports et des mécanismes d'intégrité avec d'autres services et mécanismes de sécurité.

Quelques-unes des procédures décrites dans ce cadre de sécurité permettent l'intégrité par l'application de techniques cryptographiques. L'utilisation de ce cadre ne dépend pas de l'utilisation d'une technique cryptographique particulière ou d'autres algorithmes, bien que certaines classes de mécanismes d'intégrité puissent dépendre de propriétés algorithmiques particulières.

L'intégrité dont il est question dans ce cadre est celle qui est définie par l'invariabilité d'une valeur de données et non pas celle de l'invariabilité de l'information que les données sont supposées représenter. Les autres formes d'invariabilité sont exclues.

6.7 Partie 7 – Audit et alarmes de sécurité

Ce cadre:

a) définit les concepts élémentaires d'audit et d'alarmes de sécurité;

b) fournit un modèle général pour l'audit et les alarmes de sécurité;

c) identifie la relation du service d'audit et d'alarmes de sécurité avec les autres services de sécurité.

Comme pour les autres services de sécurité, un audit de sécurité peut être offert uniquement dans le contexte d'une politique de sécurité. La politique de sécurité sera définie par les autorités de sécurité au sein de leur domaine de sécurité. Toute(s) norme(s) spécifiant des mécanismes basés sur ce cadre devrait (devraient) être capable(s) de mettre en œuvre différentes politiques de sécurité.

6.8 Gestion de clé

Le cadre de gestion de clé, Partie 1 de l'ISO/CEI 11770, a une relation spéciale avec les autres cadres de sécurité car il couvre les fonctions qui ne sont pas directement liées aux autres services de sécurité identifiés dans la Rec. X.800 du CCITT | ISO 7498-2. Ces fonctions sont applicables dans tout environnement de technologie de l'information où le chiffrement ou la signature numérique est approprié(e).

Ce cadre:

a) identifie les objectifs de la gestion de clé;

b) décrit les modèles généraux sur lesquels les mécanismes de gestion de clé sont basés;

c) définit les concepts élémentaires de la gestion de clé communs à toutes les parties de cette norme multipartie;

d) définit les services de gestion de clé;

e) identifie les caractéristiques des mécanismes de gestion de clé;

f) spécifie les besoins pour la gestion des éléments relatifs aux clés durant leur cycle de vie;

g) décrit le cadre pour la gestion des éléments relatifs aux clés durant leur cycle de vie.

7 Concepts communs

De nombreux concepts sont nécessaires dans plus d'une partie des cadres de sécurité. Cette norme définit ces concepts à utiliser dans les autres parties de cette Recommandation | Norme internationale.

7.1 Information de sécurité

L'information de sécurité (SI) est l'information requise pour mettre en œuvre les services de sécurité. A titre d'exemples d'information de sécurité, on peut citer:

– les règles de politique de sécurité;

– les informations pour réaliser des services spécifiques de sécurité, telles que l'information d'authentification (AI) et l'information de contrôle d'accès (ACI);

– les informations relatives aux mécanismes de sécurité, telles que les étiquettes de sécurité, les valeurs de contrôle cryptographique, les certificats de sécurité et les jetons de sécurité.

Les types de SI communs à plus d'un des cadres de sécurité sont traités dans l'article 8.

7.2 Domaines de sécurité

Un domaine de sécurité est un ensemble d'éléments subordonnés à une politique de sécurité donnée administrée, pour certaines activités spécifiques liées à la sécurité, par une seule autorité de sécurité. Les activités d'un domaine de sécurité mettent en jeu un ou plusieurs éléments de ce domaine de sécurité et, éventuellement, des éléments d'autres domaines de sécurité.

Exemples d'activités:

– accès aux éléments;

– établissement ou utilisation des connexions de couche (N);

– opérations relatives à une fonction spécifique de gestion;

– opérations de non-répudiation impliquant un notaire.

Une activité peut être relative à la sécurité même si elle n'est pas sujette à des mécanismes qui pourraient imposer une politique arbitraire pour son utilisation. En particulier, des activités dont on ne peut empêcher le déroulement entre n'importe quel groupe d'éléments peuvent être relatives à la sécurité et devenir, à l'avenir, le sujet de mécanismes de contrôle.

Des exemples d'éléments d'un domaine de sécurité dans un environnement de systèmes ouverts comprennent des éléments logiques ou physiques comme des systèmes ouverts réels, des processus d'application, des entités (N), des unités de données de protocole (N), des relais et des utilisateurs humains de systèmes ouverts réels. Il y a des cas où les utilisateurs humains doivent être distingués des autres éléments dans le domaine de sécurité. En pareils cas, le terme *objets de données* sera utilisé pour distinguer les éléments non humains.

7.2.1 Politique de sécurité et règles de politique de sécurité

Une politique de sécurité exprime, en des termes généraux, des besoins de sécurité pour un domaine de sécurité. Par exemple, une politique de sécurité peut identifier des besoins qui s'appliquent à tous les membres du domaine de sécurité fonctionnant sous des conditions spécifiques, ou qui s'appliquent à toutes les informations dans un domaine de sécurité. La mise en œuvre d'une politique de sécurité se concrétisera par l'identification de services de sécurité qui satisferont la politique de sécurité, et des mécanismes de sécurité seront choisis pour mettre en œuvre les services de sécurité. La décision du choix des mécanismes de sécurité est influencée par les menaces prévues et par la valeur des ressources à protéger.

Les politiques de sécurité sont communément formulées sous forme de principes généraux exprimés en langage naturel. Ces principes reflètent les besoins de sécurité d'une organisation particulière ou les membres d'un domaine de sécurité. Avant que ces besoins puissent être reflétés dans des systèmes ouverts réels, la politique de sécurité doit être détaillée de telle façon qu'un ensemble de règles de politique de sécurité puisse en être dérivé. L'interprétation de ces besoins en tant que règles de sécurité est une activité d'ingénierie. Une politique de sécurité limite les activités des éléments sujets à cette politique de sécurité, soit en demandant certaines actions soit en interdisant certaines activités. Une politique de sécurité peut également donner à des éléments la permission de prendre part à certaines activités. Il s'agit d'une interprétation plus large de la politique de sécurité que celle qui est contenue dans la Rec. X.800 du CCITT | ISO 7498-2, uniquement concernée par l'interconnexion OSI. Les aspects de politique de sécurité spécifiques à un service de sécurité sont présentés dans le cadre de sécurité de ce service.

Les règles de la politique de sécurité pour un domaine de sécurité sont de deux types, celles concernant les activités au sein d'un domaine de sécurité et celles concernant les activités entre domaines de sécurité. Les règles de politique de sécurité du dernier type sont traitées comme des règles d'interaction sécurisée. Une politique de sécurité peut également définir les règles qui s'appliquent aux relations avec tous les domaines de sécurité et les règles qui s'appliquent aux relations avec des domaines de sécurité particuliers.

Les règles de politique de sécurité pour un domaine de sécurité doivent être maintenues en vigueur lorsque le système change ou lorsque les activités et la politique de sécurité du domaine de sécurité sont modifiées.

NOTE – Ce cadre ne concerne pas les aspects suivants de la politique de sécurité:

- la partie qui établit ou maintient elle-même la politique de sécurité;
- les procédures pour établir ou maintenir la politique de sécurité;
- le contenu de la politique de sécurité;
- les procédures pour attacher une politique de sécurité à un domaine de sécurité.

7.2.2 Autorité du domaine de sécurité

Une autorité de domaine de sécurité est une autorité de sécurité qui est responsable de la mise en œuvre d'une politique de sécurité pour un domaine de sécurité.

Une autorité de domaine de sécurité:

- peut être une entité composite; une telle entité doit être identifiable;
- peut, en fonction de la politique de sécurité à laquelle l'autorité du domaine de sécurité peut être sujette, déléguer la responsabilité de mise en œuvre de la politique de sécurité à une ou plusieurs entités;
- a autorité sur les éléments du domaine de sécurité.

NOTE – Une politique de sécurité peut être sans effet si l'autorité du domaine de sécurité a décidé de n'imposer aucune contrainte.

Deux autorités de domaine de sécurité sont dites liées si elles sont contraintes de coordonner leurs politiques de sécurité.

7.2.3 Corrélations entre domaines de sécurité

La notion de domaine de sécurité est jugée importante pour deux raisons, à savoir:

- elle peut être utilisée pour décrire la façon dont la sécurité est gérée et administrée;
- elle peut être utilisée comme module pour modéliser les activités relatives à la sécurité qui mettent en jeu des éléments dépendants d'autorités de sécurité séparées.

Les domaines de sécurité peuvent être liés de plusieurs façons. Quelques relations possibles entre domaines de sécurité sont présentées ici. Les relations entre domaines de sécurité doivent être reflétées dans les politiques de sécurité des domaines de sécurité définis par les autorités de sécurité. Ces relations sont définies en termes d'éléments et d'activités des domaines de sécurité et sont reflétées dans les règles d'interaction sécurisée pour chaque domaine de sécurité associé. Quelques relations particulières entre domaines de sécurité sont décrites dans la suite de ce paragraphe. De nombreuses autres relations entre domaines de sécurité sont possibles.

a) Deux domaines de sécurité sont dits *isolés* entre eux s'ils n'ont pas d'objets de données ni d'activités en commun et, ainsi, ne peuvent pas interagir.

b) Deux domaines de sécurité sont dits *indépendants* entre eux:

   – s'ils n'ont pas d'objets de données en commun;

   – si les activités au sein de chaque domaine de sécurité sont seulement limitées par leurs propres politiques de sécurité (et les ensembles correspondants des règles de politique de sécurité);

   – si les autorités de sécurité des domaines de sécurité ne sont pas contraintes de coordonner leurs politiques de sécurité.

   Deux domaines de sécurité indépendants ou plus peuvent s'accorder pour coordonner le partage d'informations entre eux (voir 7.2.4).

c) Un domaine de sécurité A est dit être un *sous-domaine de sécurité* d'un autre domaine de sécurité B si, et seulement si:

   – l'ensemble des éléments de A est un sous-ensemble de, ou est le même que, l'ensemble des éléments de B;

   – l'ensemble des activités de A est un sous-ensemble de, ou est le même que, l'ensemble des activités de B;

   – la juridiction de A est déléguée de l'autorité de sécurité de B à l'autorité de sécurité de A;

   – la politique de sécurité de A n'est pas en conflit avec la politique de sécurité de B. A peut, si cela est nécessaire et si cela est permis par la politique de sécurité de B, introduire une politique de sécurité supplémentaire.

   NOTE 1 – Un sous-ensemble peut être égal à l'ensemble complet. Un sous-domaine de sécurité peut être formé dans un cas extrême par l'ensemble complet des éléments du superdomaine de sécurité pour certaines classes d'activités et dans un autre cas extrême par toutes les classes d'activités pour quelques sous-ensembles des éléments du superdomaine de sécurité. Entre ces deux cas extrêmes, de nombreuses variantes peuvent exister.

d) Un domaine de sécurité A est dit être un *superdomaine de sécurité* d'un autre domaine de sécurité B si, et seulement si, B est un sous-domaine de sécurité de A.

   NOTE 2 – Les cadres de sécurité n'exigent pas que les concepts isolé, indépendant, sous-domaine, ou superdomaine soient mis en œuvre par tout protocole, toute spécification ou toute mise en œuvre particulière.

7.2.4 Etablissement des règles d'interaction sécurisée

Pour être capable d'échanger de l'information entre domaines de sécurité, un ensemble approuvé de règles de sécurité doit être défini pour cet échange. Ces règles de politique de sécurité sont appelées règles d'interaction sécurisée. Elles font partie des règles de politique de sécurité de chaque domaine de sécurité. Des règles d'interaction sécurisée permettent de sélectionner des services et mécanismes communs de sécurité, potentiellement par le biais de négociation, et de lier les uns aux autres les éléments d'information de sécurité dans chaque domaine de sécurité, potentiellement par le biais de correspondances. L'information de gestion de sécurité nécessaire pour mettre en œuvre des règles d'interaction sécurisée peut être échangée entre domaines de sécurité. En fonction des relations entre domaines de sécurité, les règles d'interaction sécurisée peuvent être déterminées de différentes façons.

Pour des interactions sécurisées entre domaines de sécurité indépendants, les règles d'interaction de sécurité doivent être acceptées par les autorités de sécurité pour les domaines de sécurité impliqués.

Pour des interactions sécurisées entre sous-domaines de sécurité, les règles d'interaction sécurisée peuvent être établies par l'autorité de sécurité du superdomaine de sécurité. Si cela est permis par la politique de sécurité du superdomaine de sécurité, les sous-domaines de sécurité peuvent établir leurs propres règles d'interaction sécurisée.

7.2.5 Transfert d'information de sécurité entre domaines

Des règles d'interaction sécurisée peuvent elles-mêmes constituer une information de sécurité, et cette information de sécurité peut devoir être transférée entre domaines de sécurité. Les cas suivants sont considérés:

– la sémantique et la représentation de l'information de sécurité sont identiques dans chacun des domaines de sécurité. Cela signifie qu'une traduction n'est pas nécessaire;

- la sémantique de l'information de sécurité est identique dans chacun des domaines de sécurité, mais les représentations sont différentes. Cela signifie que la méthode de description de l'information de sécurité est différente, et ainsi la traduction de syntaxe est nécessaire;
- la sémantique mais aussi la représentation de l'information de sécurité sont différentes dans chacun des domaines de sécurité. Cela signifie que des règles d'interaction sécurisée doivent spécifier la façon dont l'information de sécurité d'un domaine est traduite dans l'information de sécurité de l'autre domaine. La traduction de syntaxe peut aussi être nécessaire.

7.3 Considérations de politique de sécurité pour des services spécifiques de sécurité

Des mécanismes de contrôle d'accès peuvent être utilisés dans certaines mises en œuvre d'un service d'intégrité ou d'un service de confidentialité. En pareils cas, les règles de politique de sécurité relatives à la mise en œuvre d'un service d'intégrité ou d'un service de confidentialité doivent décrire la façon dont les mécanismes de contrôle de sécurité seront utilisés. Les mécanismes de contrôle d'accès sont décrits en termes d'initiateurs et de cibles (dans la Rec. UIT-T X.812 | ISO/CEI 10181-3). Les règles de politique de sécurité indiquent comment les entités et les éléments d'information et de données présents dans les politiques d'intégrité et de confidentialité sont liés aux initiateurs et aux cibles dans les mécanismes de contrôle d'accès.

Les politiques de confidentialité sont définies en termes d'entités pouvant examiner des éléments d'information. Il y a deux façons par lesquelles une action réalisée par un initiateur sur une cible peut révéler de l'information à une entité. Premièrement, le résultat de l'action peut fournir à l'initiateur des informations sur la cible. Deuxièmement, la demande d'action peut fournir à la cible quelques informations sur l'initiateur. Lorsque des mécanismes de contrôle d'accès sont utilisés pour fournir un service de confidentialité, les entités qui tentent d'obtenir des informations sont considérées comme étant des initiateurs et les éléments d'information comme étant des cibles.

Les politiques d'intégrité sont définies en termes d'entités pouvant modifier des éléments de données. Il y a deux façons dont une action réalisée par un initiateur sur une cible peut modifier des données. Premièrement, l'action peut modifier directement l'information contenue dans la cible. Deuxièmement, le résultat de l'action peut entraîner la modification des données que possède l'initiateur. Lorsque des mécanismes de contrôle d'accès sont utilisés pour fournir un service d'intégrité, les entités qui tentent de modifier des données sont considérées comme étant des initiateurs, et les éléments de données comme étant des cibles.

7.4 Entités de confiance

Une entité est qualifiée d'*entité de confiance* pour certaines classes d'activités, dans le contexte d'une politique de sécurité, si ladite entité peut violer la politique de sécurité, soit en accomplissant des actions qu'elle n'est pas censée accomplir, soit en n'accomplissant pas les actions qu'elle est censée accomplir. La politique de sécurité définit les entités de confiance et définit pour chaque entité de confiance l'ensemble des activités pour lesquelles il lui est fait confiance. Une entité de confiance pour un ensemble particulier d'activités ne l'est pas nécessairement pour toutes les activités d'un domaine de sécurité.

Une politique de sécurité prônant qu'une entité devrait se comporter d'une façon particulière ne garantit pas nécessairement que l'entité se comportera de cette façon. Par conséquent, une politique de sécurité peut requérir des moyens pour détecter des violations de la politique de sécurité provoquées par le mauvais comportement de l'entité de confiance. Une entité de confiance qui peut mal se comporter sans aucune détection est appelée *entité de confiance inconditionnelle*. Une entité de confiance pouvant violer la politique de sécurité, mais ne pouvant pas le faire sans être détectée, est appelée *entité de confiance conditionnelle*.

Il peut être fait inconditionnellement confiance à une entité de confiance pour un sous-ensemble de ses activités, alors que dans le même temps il lui est fait conditionnellement confiance pour un sous-ensemble différent de ses activités. Une telle entité peut, d'une certaine façon, violer de façon indécelable la politique de sécurité mais, d'une autre façon, ne peut pas violer de façon indécelable la politique de sécurité.

Une politique de sécurité d'un domaine de sécurité peut déclarer que, pour certains ensembles d'activités dans le domaine de sécurité, il est fait confiance à un élément qui n'est pas dans le domaine de sécurité. Des règles d'interaction sécurisée (voir 7.2.4) peuvent définir la façon dont certaines entités du domaine de sécurité devraient interagir avec une entité de confiance hors du domaine de sécurité.

7.5 Confiance

On dit que l'entité X *fait confiance* à l'entité Y (pour un ensemble d'activités) si et seulement si X se fie à Y pour se comporter d'une façon déterminée par rapport aux activités.

La confiance n'est pas nécessairement mutuelle. Une entité qui n'est pas une entité de confiance peut faire usage de services fournis par une entité de confiance. L'exemple d'une telle situation de confiance mutuelle se présente lorsque deux entités de confiance coopèrent à la réalisation d'une activité, et chacune des deux entités s'appuie sur l'autre pour l'aider à imposer la politique de sécurité.

La confiance n'est pas nécessairement transitive. Une politique de sécurité peut définir la transitivité de la relation de confiance dans des situations spécifiques. Si l'entité A se fie aux services fournis par l'entité B, et l'entité de confiance B se fie aux services fournis par l'entité de confiance C, A peut alors indirectement compter que C se comportera d'une façon déterminée. Lorsque tel est le cas, la confiance est transitive. Cependant, dans d'autres circonstances, B pourrait prendre des dispositions pour assurer que le mauvais comportement de C ne puisse pas affecter les activités de A. Dans ce cas, la confiance n'est pas transitive.

7.6 Tierces parties de confiance

Une tierce partie de confiance est une autorité de sécurité ou son agent à qui il est fait confiance (dans le contexte d'une politique de sécurité) pour certaines activités relatives à la sécurité.

Exemples de tierces parties de confiance:

- une tierce partie de confiance pour l'authentification;
- un notaire ou un service d'estampillage temporel pour la non-répudiation;
- un centre de distribution de clé pour la gestion de clé.

8 Information générique de sécurité

Certains types d'information de sécurité sont nécessaires dans plusieurs cadres de sécurité. Le présent article a pour objet de décrire ces types d'information de sécurité.

Les mécanismes de sécurité décrits dans les cadres de sécurité impliquent normalement l'échange d'informations de sécurité entre les entités qui ont besoin de services de sécurité pour une interaction ou entre une autorité de sécurité et les entités en interaction. Quatre formes communes d'information de sécurité sont utilisées par les mécanismes décrits dans ces cadres:

- les étiquettes de sécurité utilisées pour indiquer la politique de sécurité applicable à un élément, une voie de communication ou un élément de données;
- les valeurs de contrôle cryptographique utilisées pour détecter les modifications d'un élément de données;
- les certificats de sécurité utilisés pour protéger des informations de sécurité obtenues auprès d'une autorité de sécurité ou d'une autorité TTP utilisée par une ou plusieurs parties en interaction;
- les jetons de sécurité utilisés pour protéger les informations de sécurité qui sont transférées entre les parties en interaction.

NOTE – L'information de sécurité peut être protégée par plusieurs mécanismes de sécurité différents. Certains mécanismes de sécurité sont basés sur l'utilisation de la cryptographie, alors que d'autres utilisent des moyens physiques.

8.1 Etiquettes de sécurité

Une étiquette de sécurité est un ensemble d'attributs de sécurité lié à un élément, une voie de communication ou un élément de données. Une étiquette de sécurité indique également, soit explicitement soit implicitement, l'autorité de sécurité responsable pour créer la liaison et la politique de sécurité applicable à l'utilisation de l'étiquette. Une étiquette de sécurité peut être utilisée en vue de mettre en œuvre une combinaison de services de sécurité.

Exemples d'utilisation d'étiquettes de sécurité:

- mettre en œuvre un système de contrôle d'accès basé sur une étiquette de sécurité comprenant l'application du contrôle d'accès pour assurer l'intégrité et/ou la confidentialité;
- indiquer le degré de confiance dans les données et ses besoins de manipulation;
- indiquer la sensibilité des données et ses besoins de manipulation;
- indiquer la protection, le rejet et les autres besoins de manipulation.

8.2 Valeurs de contrôle cryptographique

Une valeur de contrôle cryptographique est une information qui est obtenue en réalisant une transformation cryptographique sur une unité de données. Les scellés, les signatures et empreintes numériques constituent trois exemples de valeurs de contrôle cryptographique.

Un scellé est une forme de valeur de contrôle cryptographique calculée en utilisant un algorithme symétrique de cryptographie et une clé secrète partagée par les entités communicantes. On utilise les scellés pour détecter une modification des données durant le transfert.

Une signature numérique est une valeur de contrôle cryptographique qui protège d'une falsification de la part du récepteur; on la calcule en utilisant une clé privée et un algorithme asymétrique de cryptographie. La validation de la signature numérique requiert le même algorithme cryptographique et la clé publique correspondante.

NOTE 1 – Bien qu'il y ait d'autres moyens d'éviter que le récepteur ne falsifie une valeur de contrôle cryptographique (par exemple, en utilisant des modules cryptographiques résistant à l'altération), les cadres de sécurité utilisent le terme de signature numérique pour faire référence à une valeur de contrôle cryptographique produite en utilisant un algorithme asymétrique de cryptographie.

NOTE 2 – Avec certains algorithmes asymétriques de cryptographie, il faut utiliser plusieurs clés privées pour calculer une signature numérique. Lorsque de tels algorithmes sont utilisés, la possession de chacune des clés privées peut être limitée à différentes entités, de sorte que les entités doivent coopérer pour produire une signature numérique.

Une empreinte numérique est une caractéristique d'un élément de données suffisamment spécifique à l'élément de donnée pour qu'il ne soit pas possible de trouver, de façon informatique, un autre élément de données ayant la même empreinte. On peut utiliser certaines formes de valeurs de contrôle cryptographique (par exemple, le résultat de l'application d'une fonction unidirectionnelle aux données) pour fournir une empreinte numérique. Les empreintes numériques peuvent être fournies par d'autres moyens que les algorithmes cryptographiques. Par exemple, une copie d'un élément de données est une empreinte numérique.

NOTE 3 – Les fonctions unidirectionnelles ne sont pas l'équivalent des empreintes numériques. Certaines fonctions unidirectionnelles ne se prêtent pas à la création d'empreintes numériques et certaines empreintes numériques ne sont pas créées à l'aide des fonctions unidirectionnelles.

NOTE 4 – Le calcul d'une signature numérique au moyen d'un algorithme asymétrique peut prendre beaucoup de temps car les algorithmes asymétriques sont, en général, consommateurs en calcul. Une signature numérique peut être calculée à partir d'une empreinte numérique des données plutôt qu'à partir des données elles-mêmes. Cela peut donner de meilleures performances, puisqu'il peut être plus rapide de calculer une signature numérique d'une courte empreinte numérique que de calculer une signature numérique d'un long message.

Une valeur de contrôle cryptographique ne protège pas nécessairement contre la réplication d'une unité de données unique. Pour obtenir la protection contre la réplication, on peut inclure dans les données certaines informations susceptibles d'être utilisées en vue de détecter les réplications, comme une séquence de nombre ou une date, ou encore recourir au chaînage cryptographique. Pour assurer la protection contre la réplication, cette information doit être vérifiée par le récepteur de l'unité de données protégée.

8.3 Certificats de sécurité

8.3.1 Introduction aux certificats de sécurité

Un certificat de sécurité est un ensemble de données relatives à la sécurité, publié par une autorité de sécurité ou par une tierce partie de confiance, auquel s'ajoutent les informations de sécurité qui servent à fournir les services d'intégrité et d'authentification de l'origine des données pour les données. Un certificat de sécurité peut contenir une indication des périodes pendant lesquelles les données sont valides.

Les certificats de sécurité sont utilisés pour transporter l'information de sécurité entre une autorité de sécurité (ou une tierce partie de confiance) et les entités ayant besoin de cette information pour réaliser les fonctions de sécurité. Un certificat de sécurité peut contenir l'information de sécurité nécessaire pour plusieurs services de sécurité.

Comme cela est décrit dans les autres cadres de sécurité, un certificat de sécurité peut contenir des informations SI utilisées à:

- des fins de contrôle d'accès;
- des fins d'authentification;
- des fins d'intégrité;
- des fins de confidentialité;
- des fins de non-répudiation;
- des fins d'audit;
- des fins de gestion de clé.

8.3.2 Vérification et chaînage des certificats de sécurité

La vérification d'un certificat de sécurité consiste à valider son intégrité, vérifier l'identité déclarée de l'émetteur du certificat de sécurité, et vérifier que l'émetteur est autorisé à créer le certificat de sécurité. Ces opérations peuvent nécessiter la présence d'autres informations SI.

Si le vérificateur du certificat de sécurité n'a pas l'information SI nécessaire pour vérifier un certificat de sécurité, on peut utiliser un certificat de sécurité d'une autre autorité de sécurité pour fournir l'information SI nécessaire. Ce processus peut être répété de façon à fournir une chaîne de certificats de sécurité. Ceux-ci transportent l'information SI qui assure un chemin sécurisé entre une autorité de sécurité connue (c'est-à-dire une autorité pour laquelle une information SI a déjà été établie) et une entité nécessitant une information SI certifiée.

Une chaîne de certificats de sécurité ne devrait être utilisée que lorsqu'elle est compatible avec les limitations imposées par toutes les politiques de sécurité concernées. L'existence d'une chaîne n'est pas suffisante. Une chaîne devrait être utilisée uniquement lorsqu'une telle utilisation est permise par les relations de confiance entre le vérificateur de la chaîne et les autorités de sécurité qui ont créé les certificats dans la chaîne, et lorsqu'elle est également permise par les relations de confiance entre ces autorités de sécurité. Ces relations sont définies par la politique de sécurité du vérificateur de la chaîne de certificats et les politiques de sécurité des autorités de sécurité. En particulier, il est fait confiance à certaines autorités de sécurité qui émettront des certificats de sécurité pour d'autres autorités de sécurité alors que l'on se fie uniquement à d'autres autorités qui émettront des certificats de sécurité pour les entités administrées par elles.

8.3.3 Révocation des certificats de sécurité

L'information SI contenue dans un certificat de sécurité peut cesser d'être valide. Par exemple, si une clé privée est mise en péril, la clé publique correspondante ne devrait plus être utilisée, et les certificats de sécurité qui contiennent cette clé publique devraient donc être révoqués.

Les mécanismes qui peuvent être utilisés pour révoquer des certificats de sécurité comprennent des certificats de révocation et des certificats de liste de révocation. Un *certificat de révocation* est un certificat de sécurité qui indique qu'un certificat de sécurité particulier a été révoqué. Un *certificat de liste de révocation* est un certificat de sécurité qui identifie une liste de certificats de sécurité qui ont été révoqués.

8.3.4 Réutilisation des certificats de sécurité

On utilise certains certificats de sécurité pour prendre en charge plusieurs instances de communication, alors que d'autres sont censés n'être utilisés qu'une seule fois. Le certificat d'authentification défini dans la Rec. UIT-T X.509 | ISO/CEI 9594-8 est un exemple de certificat de sécurité conçu pour être utilisé plusieurs fois. Le certificat de contrôle d'accès qui autorise un seul accès est un exemple de certificat de sécurité destiné à être utilisé une seule fois. Ce dernier type de certificat peut contenir des informations visant à empêcher sa réutilisation (numéro unique, par exemple).

8.3.5 Structure des certificats de sécurité

La forme générale d'un certificat de sécurité présente trois composants:

- l'information requise dans tous les certificats de sécurité;
- l'information de sécurité spécifique à un ou plusieurs services de sécurité;
- l'information pour contrôler ou limiter l'utilisation de l'information de sécurité.

L'information requise dans tous les certificats de sécurité comprend deux catégories:

a) l'information qui fournit à la fois l'intégrité et l'authentification de l'origine des données (par exemple, une valeur de contrôle cryptographique et des indications sur l'information à utiliser pour la vérifier). Puisque le service d'authentification de l'origine des données est fourni, une indication de l'identité de la source déclarée du certificat de sécurité (c'est-à-dire l'autorité émettrice) doit également être fournie;

b) l'information à partir de laquelle une période de validité peut être identifiée (par exemple, une période de validité explicite) ou extraite (par exemple, une date de création et une période de validité implicite). Cela évite une réutilisation indéfinie du certificat de sécurité, bien que le certificat de sécurité puisse être réutilisé plusieurs fois pendant la période de validité.

L'information utilisée pour contrôler ou limiter l'utilisation de l'information de sécurité comprend trois catégories:

a) *l'information utilisée pour protéger le certificat de sécurité d'une utilisation non autorisée*

Exemples:

- l'information (par exemple, un identificateur caractéristique) qui identifie l'entité ou les entités dont l'information SI figure dans le certificat de sécurité;

- l'information qui identifie les entités qui sont autorisées à utiliser l'information SI contenue dans le certificat de sécurité;
- l'information qui contrôle le nombre de fois où le certificat peut être utilisé;
- l'information qui identifie la politique de sécurité dans le cadre de laquelle le certificat de sécurité peut être utilisé;
- les méthodes de protection et les paramètres associés pour protéger le certificat de sécurité contre le vol (voir l'Annexe A pour les exemples);
- l'information utilisée pour la protection contre la réplication (par exemple, un numéro unique ou un défi);

b) *l'information qui peut être utilisée pour aider un audit de sécurité*

Exemples:

- un identificateur de référence de certificat de sécurité (par exemple, un numéro de série) unique pour le certificat de sécurité par rapport à tous les certificats de sécurité émis par la même autorité de sécurité ou le même agent;
- l'identité (à des fins d'audit) de l'entité pour laquelle le certificat de sécurité a été initialement émis;

c) *l'information qui peut être utilisée pour contribuer au rétablissement de la sécurité*

Exemples:

- un identificateur de référence de certificat de sécurité qui peut être utilisé pour révoquer un certificat de sécurité spécifique;
- un identificateur de groupe de certificats de sécurité qui peut être utilisé pour révoquer un groupe de certificats de sécurité.

8.4 Jetons de sécurité

Un jeton de sécurité est un ensemble de données protégées par un ou plusieurs services de sécurité, et d'informations de sécurité utilisées dans la fourniture de ces services de sécurité, qui est transféré entre des entités communicantes. Les jetons de sécurité peuvent être classifiés en fonction de ceux qui les créent et des services de sécurité utilisés pour protéger leurs contenus.

Un jeton de sécurité émis par une autorité de sécurité et protégé par les services d'intégrité et d'authentification de l'origine des données est appelé certificat de sécurité (voir 8.3).

De nombreux services de sécurité nécessitent un échange d'informations de sécurité, protégé pour l'intégrité entre deux entités communicantes qui ne sont pas des autorités de sécurité. Les jetons de sécurité utilisés pour permettre ces échanges protégés pour l'intégrité ne sont pas des certificats de sécurité, car les entités qui les génèrent ne sont pas des autorités de sécurité. De tels jetons de sécurité sont appelés *jetons de sécurité protégés pour l'intégrité*.

Tous les jetons de sécurité protégés pour l'intégrité contiennent l'information suivante:

- l'information qui fournit à la fois l'intégrité et l'authentification de l'origine des données (par exemple, une valeur de contrôle cryptographique et une indication de l'information à utiliser pour la vérifier).

Un jeton de sécurité protégé pour l'intégrité peut contenir un ou plusieurs des éléments d'information additionnels suivants:

- l'information à partir de laquelle une période de validité peut être identifiée;
- l'information utilisée pour la protection contre la réplication (par exemple, un numéro unique).

9 Fonctionnalités génériques de sécurité

De nombreuses fonctionnalités sont requises dans plusieurs cadres de sécurité. Le présent article définit ces fonctionnalités à utiliser dans les autres cadres de sécurité.

9.1 Fonctionnalités liées à la gestion

Ce paragraphe identifie des types génériques de fonctionnalités de gestion. Il peut exister des sous-classes de ces fonctionnalités de gestion qui peuvent être spécifiques à un mécanisme particulier de sécurité.

9.1.1 Installer l'information SI

Cette fonctionnalité établit un ensemble initial d'informations SI liées à un élément.

9.1.2 Démonter l'information SI

Cette fonctionnalité provoque le retrait d'une entité d'un domaine de sécurité, en révoquant l'information SI qui déclare l'entité comme étant membre du domaine de sécurité.

9.1.3 Changer l'information SI

Cette fonctionnalité est appelée pour modifier l'information SI associée à un élément.

9.1.4 Valider l'information SI

Cette fonctionnalité attache un ensemble d'informations SI à un élément. La fonctionnalité *valider l'information SI* est déclenchée par une autorité de sécurité ou par son agent.

9.1.5 Invalider l'information SI

Cette fonctionnalité interdit toute utilisation de l'information SI associée à un élément. La fonctionnalité *invalider l'information SI* est déclenchée par une autorité de sécurité ou son agent. L'information SI qui a été mise hors d'usage par la fonctionnalité *invalider l'information SI* peut demeurer stockée au sein du système à des fins d'audit et pour assurer que l'information SI reste hors d'usage.

9.1.6 Mise hors d'usage/remise en service du service de sécurité

Ces fonctionnalités mettent hors d'usage ou remettent en service des aspects identifiés d'un service de sécurité.

9.1.7 Insérer

Cette fonctionnalité oblige une autorité de sécurité à enregistrer certaines informations de sécurité associées à une entité. La fonctionnalité d'inscription peut être déclenchée par une entité autre qu'une autorité de sécurité. Par exemple, une entité désirant se joindre à un domaine de sécurité peut utiliser le dispositif d'inscription pour notifier à une autorité de sécurité qu'elle souhaite se joindre au domaine de sécurité.

9.1.8 Enlever

Cette fonctionnalité provoque l'enlèvement d'un élément d'un domaine de sécurité et la révocation de son information SI associée. Cette fonctionnalité est déclenchée par une autorité de sécurité ou par son agent. Une politique de sécurité peut exiger que certains types d'information SI ne soient jamais détruits.

9.1.9 Distribuer l'information SI

Cette fonctionnalité est déclenchée par une autorité de sécurité ou par son agent pour mettre les éléments d'une information SI à la disposition d'autres entités.

9.1.10 Lister l'information SI

Cette fonctionnalité liste l'information SI qui est liée à un élément donné.

9.2 Fonctionnalités liées aux aspects opérationnels

9.2.1 Identifier les autorités de sécurité de confiance

Cette fonctionnalité identifie les autorités de sécurité auxquelles il est fait confiance dans le contexte d'une politique de sécurité pour des éléments spécifiques et pour des activités données (par exemple, pour fournir des clés de chiffrement, des certificats de sécurité pour le contrôle d'accès ou encore des certificats d'authentification de sécurité).

9.2.2 Identifier des règles d'interaction sécurisée

Cette fonctionnalité identifie les règles d'interaction sécurisée à utiliser. Cela peut être effectué par le biais d'information préétablie ou par le biais de négociations entre des éléments de domaines liés entre eux comme cela est décrit en 7.2.4.

NOTE – Les règles d'interaction sécurisée sont établies en vertu d'un accord entre domaines de sécurité et non pas grâce à l'utilisation de cette fonctionnalité. Celle-ci identifie, parmi les règles d'interaction sécurisée déjà établies, celles qui s'appliquent à une activité donnée.

9.2.3 Acquérir l'information SI

Cette fonctionnalité acquiert l'information SI avant toute activité.

Exemples de sous-classes de cette fonctionnalité:

- contrôle d'accès: obtenir l'information ACI de l'initiateur, obtenir l'information ACI de la cible;
- authentification: acquérir.

9.2.4 Générer l'information SI

Cette fonctionnalité génère l'information SI pour une activité spécifique liée à la sécurité. L'information SI peut être liée à des données.

Exemples de sous-classes de cette fonctionnalité:

- contrôle d'accès: action de liaison de l'ACI;
- authentification: générer;
- non-répudiation: générer la preuve.

9.2.5 Vérifier l'information SI

Cette fonctionnalité vérifie la validité de l'information SI produite par le déclenchement de la fonctionnalité *générer l'information SI*. La fonctionnalité de *vérification SI* peut elle-même produire l'information SI à fournir à une autre activation de la fonctionnalité *vérifier l'information SI*.

Exemples de sous-classes de cette fonctionnalité:

- contrôle d'accès: action de vérification d'ACI;
- authentification: vérification;
- non-répudiation: validation de la preuve.

Un exemple de situation dans laquelle la sortie de la fonctionnalité de *vérification SI* est restituée pour une vérification plus poussée concerne un protocole bidirectionnel pour une authentification mutuelle. Supposons que les entités A et B souhaitent s'authentifier réciproquement et que A initie l'échange du protocole. L'entité A déclenche la fonctionnalité *générer* pour créer l'information d'authentification qui contient à la fois une preuve de l'identité de A et un défi auquel l'entité B est censée répondre. L'entité B déclenche la fonctionnalité *vérifier* pour vérifier que le défi venait de l'entité A, et crée également un nouvel élément d'information d'authentification contenant une preuve de l'identité de B et répond au défi de l'entité A. L'entité A déclenche alors la fonctionnalité *vérifier* pour traiter la réponse de l'entité B. La fonctionnalité *vérifier* vérifie que la réponse venait de l'entité B et qu'elle satisfait au défi initial.

10 Interactions entre mécanismes de sécurité

Il arrive souvent qu'il faille plusieurs services de sécurité différents pour une seule instance de communication. Ce besoin peut être satisfait à condition d'utiliser un seul mécanisme de sécurité qui fournit plusieurs services de sécurité ou d'utiliser simultanément plusieurs mécanismes de sécurité différents.

Lorsque des mécanismes de sécurité différents sont utilisés simultanément, il arrive parfois qu'ils interagissent d'une manière défavorable qui peut être exploitée par un attaquant. Autrement dit, des mécanismes qui offrent un niveau acceptable de sécurité lorsqu'ils sont utilisés isolément peuvent devenir plus vulnérables lorsqu'ils sont utilisés conjointement avec d'autres mécanismes. On peut souvent combiner deux mécanismes de sécurité de plusieurs façons différentes; les vulnérabilités des mécanismes ainsi combinés peuvent différer selon la façon dont ils ont été combinés.

Une interaction particulièrement importante se produit entre des mécanismes lorsqu'on combine deux mécanismes de cryptographie (par exemple, combinaison d'un mécanisme d'intégrité avec un mécanisme de confidentialité ou d'un mécanisme de non-répudiation avec un mécanisme de confidentialité). Les propriétés de sécurité des mécanismes ainsi combinés dépendent de l'ordre dans lequel les deux transformations cryptographiques sont appliquées.

En général, lorsqu'on utilise des algorithmes asymétriques de cryptographie, il convient d'appliquer une transformation d'intégrité ou de non-répudiation au texte en clair et les données signées ou scellées qui en résultent doivent alors être chiffrées.

Il se peut qu'il faille appliquer les deux services dans l'ordre inverse (c'est-à-dire le service de confidentialité en premier), lorsque les services concernent des entités différentes; de plus, il faut qu'une entité puisse vérifier l'intégrité du cryptogramme sans être autorisée à connaître le texte en clair. Cette situation peut se produire dans les systèmes de messagerie lorsqu'un agent de transfert de message peut avoir besoin de vérifier l'intégrité et l'origine du message sans avoir reçu l'autorisation de connaître le texte clair du message.

L'utilisation des services de confidentialité et d'intégrité dans cet ordre inverse comporte le risque que le service d'intégrité ne puisse pas assurer la non-répudiation. Si ces trois services sont souhaités et que l'ordre inverse d'intégrité et de confidentialité est nécessaire, il est alors possible d'appliquer deux mécanismes d'intégrité, l'un avant le mécanisme de confidentialité et l'autre après celui-ci. On trouvera un exemple de cette situation dans les systèmes de messagerie; si la confidentialité est assurée, deux signatures numériques différentes peuvent alors être placées sur le message (l'une étant calculée sur le cryptogramme pour la consommation de l'agent de transfert du message et l'autre sur le texte en clair de façon à fournir une non-répudiation d'origine au récepteur).

11 Déni de service et disponibilité

Le déni de service survient lorsque le service se situe en dessous du niveau requis, y compris lorsque le service est indisponible. De tels dénis de service peuvent être provoqués par des attaques intentionnelles ou par des conditions accidentelles telles qu'une tempête ou un tremblement de terre. La disponibilité est une condition pour laquelle il n'y a aucun déni de service ou qualité dégradée des communications.

Il n'est pas toujours possible d'empêcher une condition de déni de service. On peut utiliser des services de sécurité pour détecter le déni d'un service afin que des mesures correctives puissent être prises. Une telle détection peut ne pas permettre de déterminer si la condition était le résultat d'une attaque ou d'une condition accidentelle. Une politique de sécurité particulière peut exiger que lorsqu'une condition de déni de service est identifiée, elle doit être archivée (à des fins d'audit) et une alarme être envoyée au processeur d'alarme.

Lorsqu'une condition de déni de service a été identifiée, on peut également utiliser des services de sécurité pour la corriger et revenir à un niveau de service acceptable. Cette identification et ces actions correctives peuvent impliquer l'utilisation de services de sécurité et de services d'autres types (par exemple, réacheminement du trafic sur d'autres liaisons, basculement vers des dispositifs de secours pour le stockage ou mise en service de processeurs de secours).

De nombreux types différents de service sont sujets à des attaques de déni de service, et les mécanismes utilisés pour les empêcher peuvent varier en fonction de chaque type d'application protégé. Cela signifie qu'il n'est pas possible de classifier, de façon générale, les mécanismes de protection contre les dénis de service qui ne sont pas traités plus en détail dans les cadres individuels de sécurité.

12 Autres besoins

D'autres mesures de sécurité que celles qui sont décrites dans ces cadres peuvent être nécessaires (par exemple, des mesures de sécurité physique et personnelle). La définition des services de sécurité pour mettre en œuvre ces mesures ne fait pas partie du champ d'application de la présente Recommandation | Norme internationale. L'utilisation de telles mesures de sécurité supplémentaires peut même éviter le recours à certains services de sécurité décrits dans ces cadres.

Annexe A

Exemples de mécanismes de protection pour les certificats de sécurité

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

Une menace potentielle mettant en jeu les certificats de sécurité est la menace qu'utiliserait un attaquant pour déclarer faussement être l'entité à laquelle le certificat fait référence. Une telle utilisation non autorisée d'un certificat de sécurité est qualifiée de vol du certificat de sécurité.

Cette menace peut aussi bien être une menace interne qu'une menace externe. La menace externe est celle d'un attaquant qui pourrait obtenir un certificat de sécurité en écoutant une communication dans laquelle il n'est pas impliqué par ailleurs. La menace interne est celle d'une entité qui a légitimement besoin d'obtenir un certificat (par exemple, afin d'établir l'information SI d'une entité avec laquelle elle communique) et qui pourrait faussement déclarer être l'entité référencée dans le certificat.

Un certificat de sécurité peut être protégé contre le vol en utilisant les services de sécurité des communications OSI ou en utilisant une autre méthode de protection nécessitant des paramètres supplémentaires, internes et externes au certificat de sécurité.

Un mécanisme de protection pour les certificats de sécurité permet la délégation si une entité qui a le droit d'utiliser le certificat de sécurité peut transférer ce droit à une autre entité. Certains mécanismes décrits dans la présente annexe permettent la délégation.

A.1 Protection utilisant un service de sécurité des communications OSI

La menace de vol par un élément externe peut être contrée en utilisant un service de confidentialité lorsque le certificat de sécurité est transféré entre les entités communicantes.

A.2 Protection utilisant un paramètre dans le certificat de sécurité

Il y a plusieurs autres méthodes pour protéger contre le vol les certificats de sécurité. Chacune de ces méthodes est basée sur des paramètres internes au certificat et sur des paramètres externes associés. Les méthodes particulières utilisées peuvent être indiquées dans le certificat de sécurité.

Ces méthodes comprennent:

- la méthode d'authentification;
- la méthode de clé secrète;
- la méthode de clé publique;
- la méthode de fonction unidirectionnelle.

Un certificat de sécurité peut utiliser une combinaison de plusieurs de ces méthodes.

A.2.1 La méthode d'authentification

Dans cette méthode, le paramètre interne est composé des identificateurs caractéristiques des entités autorisées à utiliser le certificat. Le paramètre externe est le paramètre caractéristique de l'entité qui tente d'utiliser le certificat. Ce paramètre externe est fourni par un service d'authentification. De façon optionnelle, le certificat peut inclure des paramètres internes additionnels tels que le numéro de série du certificat d'authentification utilisé dans le processus d'authentification.

La méthode d'authentification offre la protection suivante pour le certificat de sécurité:

- elle limite l'utilisation du certificat de sécurité aux entités dont les identificateurs sont inclus dans le certificat de sécurité.

Cette méthode ne permet pas à un utilisateur autorisé pour le certificat de donner ses droits à une autre entité, puisque les entités qui peuvent utiliser le certificat sont définies au moment où le certificat est créé. Ainsi, cette méthode ne permet pas la délégation.

A.2.2 La méthode de la clé secrète

Dans cette méthode, le certificat complet est chiffré en utilisant un algorithme cryptographique symétrique. Le paramètre externe dans cette méthode est la clé secrète qui a été utilisée pour chiffrer le certificat.

La méthode de la clé secrète offre la protection suivante pour le certificat de sécurité:

– elle limite l'utilisation du certificat de sécurité aux entités qui connaissent la valeur de la clé secrète (et sont ainsi capables de déchiffrer le certificat chiffré).

Cette méthode permet la délégation, puisqu'un utilisateur autorisé pour le certificat peut donner ce droit à une autre entité soit en lui donnant la clé secrète soit en lui donnant le certificat déchiffré.

A.2.3 La méthode de la clé publique

Dans cette méthode, le paramètre interne est la clé publique. Le paramètre externe est la clé privée correspondante.

La méthode de la clé publique offre, pour le certificat de sécurité, la protection suivante:

– elle limite l'utilisation du certificat de sécurité aux entités qui connaissent la valeur de la clé privée (et sont ainsi capables de calculer des signatures numériques en utilisant la clé privée).

Cette méthode permet la délégation, puisqu'un utilisateur autorisé pour le certificat peut donner ce droit à une autre entité en lui donnant la clé privée.

A.2.4 La méthode de la fonction à sens unique

Dans cette méthode, le paramètre interne est le résultat de l'application d'une fonction unidirectionnelle au paramètre externe. Le paramètre interne est appelé *clé de protection* alors que le paramètre externe est appelé *clé de contrôle*.

La méthode de la fonction unidirectionnelle offre, pour le certificat de sécurité, la protection suivante:

– elle limite l'utilisation du certificat de sécurité aux entités qui connaissent la valeur de la clé de contrôle (et sont ainsi capables de prouver qu'elles connaissent la clé de contrôle en révélant sa valeur).

Cette méthode permet la délégation, puisqu'un utilisateur autorisé pour le certificat peut donner ce droit à une autre entité en lui donnant la clé de contrôle.

A.3 Protection des paramètres internes et externes lors de leur transfert

Quatre cas doivent être considérés:

– transfert du paramètre interne vers l'autorité émettrice avant que le certificat ne soit créé. Ce cas se présente seulement si les paramètres interne et externe ne sont pas générés par l'autorité émettrice;

– transfert du paramètre externe depuis l'autorité émettrice après que le certificat est créé. Ce cas est nécessaire seulement si les paramètres interne et externe sont générés par l'autorité émettrice;

– transfert du paramètre externe entre entités lorsque le droit d'utiliser le certificat est revendiqué;

– transfert du paramètre externe entre entités lorsque le droit d'utiliser le certificat est délégué.

A.3.1 Transfert des paramètres internes vers l'autorité de sécurité émettrice

Dans la méthode d'authentification, la méthode de la clé publique et la méthode de la fonction unidirectionnelle, le paramètre interne peut être communiqué à l'autorité de sécurité avant d'être placé dans le certificat de sécurité. Le paramètre interne doit être protégé pour l'intégrité lorsqu'il est transféré vers l'autorité de sécurité.

Dans la méthode de la clé sécrète, le paramètre externe (par exemple la clé secrète) peut être communiqué à l'autorité de sécurité avant la création du certificat. Ce transfert nécessite à la fois la protection de l'intégrité et de la confidentialité.

A.3.2 Transfert de paramètres externes entre entités

Dans la méthode d'authentification, le paramètre externe (l'identité de l'utilisateur du certificat de sécurité) est fourni par un mécanisme d'authentification.

Dans la méthode de la clé secrète et la méthode de la fonction unidirectionnelle, le paramètre externe doit être transféré entre entités lorsque le certificat est utilisé. Cela limite l'utilisation du certificat de sécurité à ceux qui connaissent la valeur correcte de la clé secrète ou de la clé de contrôle. Le paramètre externe doit être protégé en ce qui concerne la confidentialité lorsqu'il est échangé entre entités.

Une différence entre ces deux méthodes tient au fait que lorsque la méthode de la clé secrète est utilisée, il est nécessaire de révéler la valeur du paramètre externe avant que la valeur de contrôle cryptographique puisse être vérifiée, alors que dans la méthode unidirectionnelle, la valeur de contrôle du certificat de sécurité peut être vérifiée avant que le paramètre externe ne soit révélé.

Dans la méthode de la clé privée, le paramètre externe n'a pas besoin d'être transmis entre les entités lorsque le certificat est utilisé, puisque l'entité peut prouver qu'elle connaît la clé privée sans la révéler (en créant une signature numérique). Avec cette méthode, le paramètre externe (la clé privée) doit seulement être transmis lorsque le droit d'utiliser le certificat est délégué. La clé privée doit être gardée confidentielle lorsqu'elle est communiquée entre les entités.

A.4 Utilisation de certificats de sécurité par une seule entité ou par des groupes d'entités

Les méthodes de protection décrites ci-dessus peuvent être utilisées pour limiter l'utilisation d'un certificat de sécurité soit à une seule entité désignée soit à un groupe désigné d'entités:

- un certificat de sécurité peut être attaché à une seule entité; la clé secrète, la clé privée ou la clé de contrôle est communiquée à une seule entité sous une forme chiffrée, et l'identificateur caractéristique ou les attributs de sécurité de l'entité apparaissent dans le certificat de sécurité;
- un certificat de sécurité peut être lié à un groupe désigné d'entités; la clé secrète, la clé privée ou la clé de contrôle est communiquée aux membres du groupe sous une forme chiffrée, et l'identificateur caractéristique ou les attributs de sécurité du groupe apparaissent dans le certificat de sécurité. De cette façon, n'importe quel membre du groupe peut utiliser le certificat de sécurité.

A.5 Liaison d'un certificat de sécurité avec les accès

Les certificats de sécurité peuvent être utilisés pour le contrôle d'accès. Dans ce cas, il est important d'établir un lien sécurisé entre un certificat de sécurité et les demandes d'accès qu'il assure. En l'absence d'un tel lien, le certificat de sécurité est alors vulnérable à une attaque de réplication dans laquelle un attaquant transmet une copie du certificat de sécurité original suivie d'une demande d'accès falsifiée.

On peut éviter cette attaque en utilisant un service d'intégrité pour lier ensemble le certificat de sécurité, le paramètre externe et la demande d'accès.

Lorsque la méthode d'authentification est utilisée, cette liaison peut être effectuée en liant l'échange d'authentification à un mécanisme d'intégrité. Cela est décrit dans le cadre d'authentification (Rec. UIT-T X.811 | ISO/CEI 10181-2).

Lorsque la méthode de la clé secrète est utilisée, cette liaison peut être effectuée en incorporant une clé pour un mécanisme d'intégrité dans la partie principale du certificat de sécurité et en utilisant cette clé pour sceller la demande d'accès. On peut aussi utiliser la clé secrète (ou une variante de celle-ci) comme clé d'un mécanisme d'intégrité.

NOTE – L'utilisation de la même clé cryptographique à la fois pour un mécanisme d'intégrité et pour un mécanisme de confidentialité peut rendre certaines attaques possibles. Pour se prémunir contre ces attaques, des *variantes de clé* peuvent être utilisées. Une variante d'une clé cryptographique est constituée d'une autre clé cryptographique qui en est dérivée, mais n'est pas la même que la clé d'origine.

Lorsque la méthode de la fonction unidirectionnelle est utilisée, la liaison peut être effectuée en utilisant la clé de contrôle comme clé d'un mécanisme d'intégrité basé sur des fonctions unidirectionnelles.

Lorsque la méthode de la clé publique est utilisée, la liaison peut être effectuée en utilisant la clé privée pour signer les demandes d'accès.

Avec toutes ces méthodes, la liaison entre le certificat de sécurité, le paramètre externe et la demande d'accès peut également être effectuée en utilisant un service d'intégrité fourni par un service de communications OSI.

Annexe B

Bibliographie

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

– Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour systèmes ouverts: Cadre d'authentification.*

– Recommandation UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité dans les systèmes ouverts: Contrôle d'accès.*

– Recommandation UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Cadre d'authentification.*

– ISO/CEI 11770-1[1)], *Technologies de l'information – Techniques de sécurité – Gestion de clé – Partie 1: Cadre de gestion de clé.*

– ISO/CEI 9798-1:1991, *Technologies de l'information – Techniques de sécurité – Mécanismes d'authentification d'entité – Partie 1: Modèle général.*

1) A paraître.