NORME INTERNATIONALE

ISO/CEI 10181-1

Première édition
1996-08-01

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Aperçu

Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview

Numéro de référence
ISO/CEI 10181-1:1996(F)

Sommaire

Version française tirée en 1997

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement des Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10181-1 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.810.

ISO/CEI 10181 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts* :

— *Partie 1: Aperçu*

— *Partie 2: Cadre d'authentification*

— *Partie 3: Cadre de contrôle d'accès*

— *Partie 4: Cadre de non-répudiation*

— *Partie 5: Cadre de confidentialité*

— *Partie 6: Cadre d'intégrité*

— *Partie 7: Cadre pour l'audit de sécurité et les alarmes*

Les annexes A et B de la présente partie de l'ISO/CEI 10181 sont données uniquement à titre d'information.

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.

Page blanche

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: APERÇU

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 I 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 I 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 I Normes internationales identiques

- Recommandation UIT-T X.200 (1994) I 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.