NORME INTERNATIONALE

ISO/CEI 10181-6

Première édition
1996-09-15

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

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

Numéro de référence
ISO/CEI 10181-6:1996(F)

Sommaire

ISO/CEI Copyright Office • Case postale 56 • CH-1211 Genève 20 • Suisse

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 de 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 ou 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 10181-6 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.815.

L'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: Vue d'ensemble*

— *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 d'audit de sécurité*

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

Introduction

De nombreuses applications de systèmes ouverts ont des exigences de sécurité qui dépendent de l'intégrité des données. Ces exigences peuvent inclure la protection de données utilisées pour assurer d'autres services de sécurité tels que l'authentification, le contrôle d'accès, la confidentialité, l'audit et la non-répudiation qui, si un «attaquant» pouvait les modifier, risqueraient de réduire ou d'annihiler l'efficacité de ces services.

La propriété caractérisant des données qui n'ont pas été altérées ou détruites d'une manière non autorisée est appelée «intégrité». La présente Recommandation | Norme internationale définit un cadre général pour la fourniture de services d'intégrité.

Page blanche

NORME INTERNATIONALE

RECOMMANDATION UIT-T

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

1 Domaine d'application

La Recommandation I Norme internationale sur les Cadres de sécurité pour les systèmes ouverts couvre l'application des services de sécurité dans un environnement de systèmes ouverts où le terme «systèmes ouverts» est utilisé pour des domaines tels que les bases de données, les applications distribuées, le traitement réparti ouvert (ODP) et l'interconnexion OSI. Les Cadres de sécurité ont pour but de définir les moyens d'assurer la protection pour les systèmes et les objets à l'intérieur des systèmes, ainsi que les interactions entre les systèmes. Ils ne couvrent pas la méthodologie de construction des systèmes ou mécanismes.

Les Cadres de sécurité couvrent à la fois les éléments de données et les séquences d'opérations (mais non les éléments de protocole) qui peuvent servir à obtenir des services de sécurité spécifiques. Ces services de sécurité peuvent s'appliquer aux entités communicantes des systèmes ainsi qu'aux données échangées entre les systèmes et aux données gérées par les systèmes.

La présente Recommandation I Norme internationale qui traite de l'intégrité des données lors de l'extraction, du transfert et de la gestion des informations:

1) définit les concepts élémentaires de l'intégrité des données;
2) identifie les classes possibles de mécanismes d'intégrité;
3) identifie les fonctionnalités pour chaque classe de mécanisme d'intégrité;
4) identifie les ressources de gestion requises pour prendre en charge les diverses classes de mécanismes d'intégrité;
5) examine l'interaction des mécanismes d'intégrité et des services supports avec d'autres services et mécanismes de sécurité.

Plusieurs types de normes peuvent utiliser ce cadre d'intégrité, notamment:

1) les normes qui incorporent le concept d'intégrité;
2) les normes qui spécifient des services abstraits incluant l'intégrité;
3) les normes qui spécifient les utilisations d'un service d'intégrité;
4) les normes qui spécifient les moyens d'assurer l'intégrité dans une architecture de systèmes ouverts;
5) les normes qui spécifient les mécanismes d'intégrité.

De telles normes peuvent utiliser ce cadre d'intégrité comme indiqué ci-dessous:

- les normes des types 1), 2), 3), 4) et 5) peuvent utiliser la terminologie de ce cadre d'intégrité;
- les normes des types 2), 3), 4) et 5) peuvent utiliser les fonctionnalités définies à l'article 7 de ce cadre d'intégrité;
- les normes du type 5) peuvent être fondées sur les classes de mécanismes définies à l'article 8 de ce cadre d'intégrité.

Certaines des procédures décrites dans ce Cadre de sécurité assurent l'intégrité par l'application de techniques cryptographiques. Ce cadre ne dépend pas de l'utilisation d'algorithmes cryptographiques ou autres particuliers mais certaines classes de mécanismes d'intégrité peuvent dépendre de propriétés d'algorithme particulières.

NOTE – Bien que l'ISO ne normalise pas les algorithmes cryptographiques, il normalise néanmoins les procédures utilisées pour les enregistrer dans l'ISO/CEI 9979.

L'intégrité traitée par la présente Recommandation | Norme internationale est celle qui est définie par la constance d'une valeur de données. Cette notion (constance d'une valeur de données) englobe toutes les instances dans lesquelles différentes représentations d'une valeur de données sont jugées équivalentes (telles que différents codages ASN.1 de la même valeur). Les autres formes d'invariance sont exclues.

L'utilisation du terme «données» dans la présente Recommandation | Norme internationale inclut tous les types de structure de données (tels que séries ou ensembles de données, séquences de données, systèmes de fichiers et bases de données).

Ce Cadre de sécurité s'applique à la mise en œuvre de l'intégrité pour les données dont on pense que l'écriture est accessible à d'éventuels «attaquants». Par conséquent, il met l'accent sur la mise en œuvre de l'intégrité par des mécanismes – cryptographiques et non cryptographiques – qui ne dépendent pas exclusivement de la régulation de l'accès.

2 Références normatives

Les Recommandations et les 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. Toute Recommandation et Norme 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-T 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.*
- Recommandation UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Technologies de l'information – Protocole de sécurité de la couche réseau.*
- Recommandation UIT-T X.274 (1994) | ISO/CEI 10736:1995, *Technologies de l'information – Télécommunications et échange d'informations entres systèmes – Protocole de sécurité de la couche transport.*
- Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*
- Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre de sécurité pour les 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 pour les systèmes ouverts: contrôle d'accès.*

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

- Recommandation UIT-T X.224 (1993), *Protocole pour assurer le service de couche transport en mode connexion pour l'interconnexion des systèmes ouverts.*

  ISO/CEI 8073:1992 – *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Interconnexion de systèmes ouverts OSI – Protocole pour fourniture du service de transport en mode connexion.*

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

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

2.3 Références additionnelles

- ISO/CEI 9979:1991, *Techniques cryptographiques – Procédures pour l'enregistrement des algorithmes cryptographiques.*

3 Définitions

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

3.1 La présente Recommandation I Norme internationale se fonde sur les concepts énoncés dans la Rec. UIT-T X.200 I ISO/CEI 7498-1 et utilise les termes suivants qui y sont définis:

a) connexion (N);

b) entité (N);

c) fonctionnalité (N);

d) couche (N);

e) SDU (N);

f) service (N):

g) données d'utilisateur (N).

3.2 La présente Recommandation I Norme internationale se fonde sur les concepts énoncés dans la Rec. X.800 du CCITT I ISO 7498-2 et utilise les termes suivants qui y sont définis:

a) contrôle d'accès;

b) intégrité de la connexion;

c) intégrité des données;

d), e) déchiffrement;

f) signature numérique;

g), h) chiffrement;

i) politique de sécurité fondée sur l'identité;

j) intégrité;

k) clé;

l) contrôle de routage;

m) politique de sécurité fondée sur des règles.

NOTE – Sauf indication contraire, le terme «intégrité» utilisé dans la présente Norme désigne l'intégrité des données.

3.3 La présente Recommandation I Norme internationale utilise les termes généraux relatifs à la sécurité indiqués ci-dessous et définis dans la Rec. UIT-T X.810 I ISO/CEI 10181-1:

a) empreinte numérique;

b) fonction de hachage;

c) fonction unidirectionnelle;

d) clé privée;

e) clé publique;

f) scellé;

g) clé secrète;

h) tierce partie de confiance.

3.4 La présente Recommandation I Norme internationale se fonde sur les concepts énoncés dans la Rec. UIT-T X.811 I ISO/CEI 10181-2 et utilise le terme suivant qui y est défini:

– paramètre variant dans le temps.

3.5 Pour les besoins de la présente Recommandation I Norme internationale, les définitions suivantes s'appliquent:

3.5.1 **voie protégée par l'intégrité**: voie de communication à laquelle un service d'intégrité a été appliqué.

NOTE – Deux formes de service d'intégrité pour les voies de communication (intégrité en mode connexion et intégrité en mode sans connexion) sont mentionnées dans la Rec. UIT-T X.800 du CCITT I ISO 7498-2. Elles sont décrites dans l'Annexe A.

3.5.2 **environnement protégé par l'intégrité**: environnement dans lequel toute modification (y compris la création et la suppression) non autorisée de données est empêchée ou est détectable.

3.5.3 **données protégées par l'intégrité**: données et tous attributs pertinents se trouvant dans un environnement protégé par l'intégrité.

3.5.4 **protection**: conversion de données en données protégées par l'intégrité.

3.5.5 **retrait de l'intégrité**: conversion de données protégées par l'intégrité en données initialement protégées.

3.5.6 **validation**: vérification de données protégées par l'intégrité pour détecter une perte d'intégrité.

4 Abréviations

PDU Unité de données de protocole (*protocol data unit*)

SDU Unité de données de service (*service data unit*)

SII Informations de protection de l'intégrité (*shield integrity information*)

MDII Informations de détection de modification de l'intégrité (*modification detection integrity information*)

UII Informations de retrait de l'intégrité (*unshield integrity information*)

5 Présentation générale de l'intégrité

Le but du service d'intégrité est de protéger l'intégrité des données et de leurs attributs associés qui peut être compromise de diverses manières, comme indiqué ci-dessous:

1) modification non autorisée des données;
2) suppression non autorisée des données;
3) création non autorisée des données;
4) insertion non autorisée des données;
5) répétition non autorisée des données.

Le service d'intégrité assure la protection contre ces menaces par des moyens de prévention ou par la détection avec ou sans récupération des données. La protection efficace de l'intégrité peut ne pas être possible si les informations de contrôle nécessaires (clés et informations SII) ne sont pas protégées par l'intégrité et/ou la confidentialité; il arrive souvent que cette protection repose implicitement ou explicitement sur des principes différents de ceux qui figurent dans le mécanisme de protection des données.

La notion d'environnements protégés est utilisée explicitement dans ce cadre afin d'introduire l'idée que la protection de l'intégrité inclut la protection contre la création et/ou la suppression non autorisées de données. Ainsi, la création/la suppression non autorisée de données peut être considérée comme étant la modification non autorisée d'un certain environnement protégé. De même, l'insertion et la répétition de données peuvent être considérées comme étant des modifications d'un ensemble structuré de données (tel qu'une séquence, ou une structure de données).

Il convient de noter que certaines altérations de données peuvent être considérées comme n'ayant aucune incidence sur leur intégrité. Par exemple, si une description ASN.1 contient un type de données **SET OF** (ensemble de), il n'y a pas de violation de l'intégrité si les membres du type de données sont réordonnés. Les mécanismes d'intégrité perfectionnés peuvent reconnaître que certaines transformations de données structurées ne compromettent pas l'intégrité des données. Ces mécanismes permettent des transformations de données signées ou scellées sans qu'il soit nécessaire de recalculer respectivement la signature numérique ou le scellé.

Le but d'un service d'intégrité est d'assurer la protection contre toute modification non autorisée des données, y compris la création et la suppression non autorisées des données ou d'en effectuer la détection. La mise en œuvre d'un service d'intégrité est réalisée au moyen des activités suivantes:

1) **protection** génération de données protégées par l'intégrité à partir de données initiales;
2) **validation** vérification de données protégées par l'intégrité pour détecter une perte d'intégrité;
3) **retrait de la protection** régénération des données initiales à partir de données protégées par l'intégrité.

Ces activités n'utilisent pas nécessairement les techniques de cryptographie et lorsqu'elles le font, elles ne transforment pas nécessairement les données. Par exemple, on peut exécuter l'opération de **protection** en ajoutant un scellé ou une signature numérique aux données. Dans ce cas, après **validation** effective, on **retire la protection** en enlevant le scellé/la signature numérique.

L'intégrité s'applique, comme indiqué ci-après, à l'extraction, au transfert et à la gestion des données:

1) pour l'information transférée dans un environnement OSI, le service d'intégrité est assuré en combinant **l'opération de protection**, le transfert utilisant une fonctionnalité (N-1) et **le retrait de la protection** pour former la partie transmission d'un service (N);

2) pour la mise en mémoire et l'extraction des données, le service d'intégrité est assuré en combinant **l'opération de protection**, la mise en mémoire et l'extraction ainsi que **l'opération de retrait de la protection**.

Les deux **opérations de protection** et de **retrait de la protection** peuvent être exécutées de telle sorte que les mêmes données [par exemple, toutes les données d'une connexion (N)] incluent simultanément des parties qui n'ont pas encore été **protégées**, des parties qui sont protégées par l'intégrité des données et des parties qui **ne sont plus protégées**.

Les mécanismes d'intégrité établissent des environnements protégés et les phases de **protection** et de **retrait de la protection** peuvent impliquer le transfert de données entre des environnements protégés. Lorsque des données protégées par l'intégrité sont transférées d'un environnement protégé par un mécanisme d'intégrité à un autre, l'opération de **protection** du second mécanisme doit précéder l'opération de **retrait de la protection** du premier mécanisme afin que les données soient protégées d'une manière continue.

5.1 Concepts de base

On peut distinguer plusieurs types de service d'intégrité selon l'activité de traitement de données considérée (création, suppression, modification, insertion et/ou répétition), selon que la prévention ou seulement la détection des violations est nécessaire et selon qu'ils assurent ou non la récupération des données en cas de violation de l'intégrité. Les différents types de service d'intégrité sont décrits au 5.2.

Les mécanismes que l'on peut utiliser pour assurer ces services peuvent être divisés en grandes catégories qui dépendent du niveau d'activité systématique supposée dans une tentative de violation de l'intégrité. Ces différents types de mécanisme sont décrits au 5.3.

5.2 Types de services d'intégrité

Les services d'intégrité sont classés en fonction des critères suivants:

1) selon le type de violation contre laquelle ils assurent la protection. Les types de violation sont les suivants:

   a) modification non autorisée de données;

   b) création non autorisée de données;

   c) suppression non autorisée de données;

   d) insertion non autorisée de données;

   e) répétition non autorisée de données.

2) selon le type de protection qu'ils assurent. Les types de protection sont les suivants:

   a) prévention de la perte d'intégrité;

   b) détection de la perte d'intégrité.

3) selon qu'ils incluent ou non des mécanismes de récupération des données.

   Dans le premier cas (avec récupération des données), l'opération de **retrait de la protection** permet de récupérer les données initiales (et, éventuellement, de signaler une action de récupération ou une erreur à des fins telles que l'audit) lorsque l'opération de **validation** indique une altération.

   Dans le dernier cas (sans récupération des données), l'opération de **retrait de la protection** ne permet pas de récupérer les données initiales lorsque l'opération de **validation** indique une altération de ces données.

5.3 Types de mécanismes d'intégrité

En général, la capacité de protection des données dépend du support utilisé. Certains supports sont, par leur nature même, difficiles à protéger (comme les supports de stockage amovibles ou les supports de communication), de telle sorte que des parties non autorisées peuvent, à volonté, accéder aux données et les modifier techniquement. Dans ces supports,