



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

# UIT-T

SECTEUR DE LA NORMALISATION  
DES TÉLÉCOMMUNICATIONS  
DE L'UIT

# X.815

(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: CADRE D'INTÉGRITÉ**

#### **Recommandation UIT-T X.815**

(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 n° 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.815 de l'UIT-T a été approuvé le 21 novembre 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10181-6.

---

## 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.

© UIT 1996

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'UIT.

# 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 |
|------------------------------------------------------|-----------------|
| <b>RÉSEAUX PUBLICS POUR DONNÉES</b>                  |                 |
| 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     |
| <b>INTERCONNEXION DES SYSTÈMES OUVERTS</b>           |                 |
| 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     |
| <b>INTERFONCTIONNEMENT DES RÉSEAUX</b>               |                 |
| Considérations générales                             | X.300-X.349     |
| Systèmes mobiles de transmission de données          | X.350-X.369     |
| Gestion                                              | X.370-X.399     |
| <b>SYSTÈMES DE MESSAGERIE</b>                        | X.400-X.499     |
| <b>ANNUAIRE</b>                                      | X.500-X.599     |
| <b>RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES</b>        |                 |
| 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     |
| <b>GESTION OSI</b>                                   | X.700-X.799     |
| <b>SÉCURITÉ</b>                                      | X.800-X.849     |
| <b>APPLICATIONS OSI</b>                              |                 |
| Engagement, concomitance et rétablissement           | X.850-X.859     |
| Traitement des transactions                          | X.860-X.879     |
| Opérations distantes                                 | X.880-X.899     |
| <b>TRAITEMENT OUVERT RÉPARTI</b>                     | X.900-X.999     |



## TABLE DES MATIÈRES

|          | <i>Page</i>                                                                                        |
|----------|----------------------------------------------------------------------------------------------------|
| 1        | Domaine d'application..... 1                                                                       |
| 2        | Références normatives ..... 2                                                                      |
| 2.1      | Recommandations   Normes internationales identiques..... 2                                         |
| 2.2      | Paires de Recommandations   Normes internationales équivalentes par leur contenu technique ..... 2 |
| 2.3      | Références additionnelles ..... 2                                                                  |
| 3        | Définitions..... 3                                                                                 |
| 4        | Abréviations ..... 4                                                                               |
| 5        | Présentation générale de l'intégrité..... 4                                                        |
| 5.1      | Concepts de base..... 5                                                                            |
| 5.2      | Types de services d'intégrité ..... 5                                                              |
| 5.3      | Types de mécanismes d'intégrité..... 5                                                             |
| 5.4      | Menaces contre l'intégrité ..... 6                                                                 |
| 5.5      | Types d'attaque contre l'intégrité..... 7                                                          |
| 6        | Politiques d'intégrité ..... 7                                                                     |
| 6.1      | Expression des politiques..... 7                                                                   |
| 6.1.1    | Caractérisation des données ..... 8                                                                |
| 6.1.2    | Caractérisation des entités..... 8                                                                 |
| 6.1.2.1  | Politiques fondées sur l'identité..... 8                                                           |
| 6.1.2.2  | Politiques fondées sur des règles ..... 8                                                          |
| 7        | Informations et fonctions d'intégrité ..... 8                                                      |
| 7.1      | Informations d'intégrité ..... 8                                                                   |
| 7.1.1    | Informations de protection de l'intégrité ..... 8                                                  |
| 7.1.2    | Informations de détection de modification de l'intégrité..... 8                                    |
| 7.1.3    | Informations de retrait de l'intégrité..... 8                                                      |
| 7.2      | Fonctions d'intégrité..... 9                                                                       |
| 7.2.1    | Fonctions relatives à l'exploitation..... 9                                                        |
| 7.2.2    | Fonctions relatives à la gestion ..... 9                                                           |
| 8        | Classification des mécanismes d'intégrité ..... 10                                                 |
| 8.1      | Mise en œuvre de l'intégrité par la cryptographie..... 10                                          |
| 8.1.1    | Mise en œuvre de l'intégrité par les scellés..... 10                                               |
| 8.1.2    | Mise en œuvre de l'intégrité par les signatures numériques..... 10                                 |
| 8.1.3    | Mise en œuvre de l'intégrité par le chiffrement de données redondantes ..... 11                    |
| 8.2      | Mise en œuvre de l'intégrité par le contexte..... 11                                               |
| 8.2.1    | Reproduction des données ..... 11                                                                  |
| 8.2.2    | Contexte convenu au préalable ..... 12                                                             |
| 8.3      | Mise en œuvre de l'intégrité par détection et accusé de réception ..... 12                         |
| 8.4      | Mise en œuvre de l'intégrité par prévention ..... 12                                               |
| 9        | Interactions avec d'autres services et mécanismes de sécurité ..... 12                             |
| 9.1      | Contrôle d'accès ..... 12                                                                          |
| 9.2      | Authentification de l'origine des données ..... 12                                                 |
| 9.3      | Confidentialité..... 13                                                                            |
| Annexe A | – Intégrité dans le modèle de référence de base OSI ..... 14                                       |
| Annexe B | – Cohérence externe des données..... 16                                                            |
| Annexe C | – Description générale des fonctions d'intégrité..... 18                                           |

## Résumé

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

## 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.

## NORME INTERNATIONALE

## RECOMMANDATION UIT-T

# TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: CADRE D'INTÉGRITÉ

## 1 Domaine d'application

La Recommandation | 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 | 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 entre 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 | Norme internationale, les définitions suivantes s'appliquent.

**3.1** La présente Recommandation | Norme internationale se fonde sur les concepts énoncés dans la Rec. UIT-T X.200 | 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 | Norme internationale se fonde sur les concepts énoncés dans la Rec. X.800 du CCITT | 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 | Norme internationale utilise les termes généraux relatifs à la sécurité indiqués ci-dessous et définis dans la Rec. UIT-T X.810 | 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 | Norme internationale se fonde sur les concepts énoncés dans la Rec. UIT-T X.811 | 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 | 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 | 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 ( <i>protocol data unit</i> )                                                      |
| SDU  | Unité de données de service ( <i>service data unit</i> )                                                         |
| SII  | Informations de protection de l'intégrité ( <i>shield integrity information</i> )                                |
| MDII | Informations de détection de modification de l'intégrité ( <i>modification detection integrity information</i> ) |
| UII  | Informations de retrait de l'intégrité ( <i>unshield integrity information</i> )                                 |

## 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,

le but du mécanisme d'intégrité est d'assurer la détection de la modification et, éventuellement, le rétablissement des données affectées. On distingue donc différents cas de mécanismes d'intégrité qui sont indiqués ci-dessous:

- 1) ceux qui empêchent l'accès au support, notamment les mécanismes suivants:
  - a) voies physiquement isolées, exemptes de bruit;
  - b) contrôle de l'acheminement;
  - c) contrôle d'accès.
- 2) ceux qui détectent les modifications non autorisées de données ou de séquences d'éléments de données, y compris les cas de création, de suppression ou de reproduction de données. Ces mécanismes sont les suivants:
  - a) scellés;
  - b) signatures numériques;
  - c) reproduction des données (utilisée pour combattre d'autres types de violation);
  - d) empreintes numériques associées à des transformations cryptographiques;
  - e) séquençement des messages.

En termes de force de protection, ces mécanismes peuvent être classés comme suit:

- 1) aucune protection;
- 2) détection de modification et de création de données;
- 3) détection de modification, de création, de suppression et de reproduction de données;
- 4) détection de modification et de création de données avec récupération;
- 5) détection de modification, de création, de suppression et de reproduction de données avec récupération.

#### **5.4 Menaces contre l'intégrité**

En termes de services assurés, les menaces peuvent être classées comme suit:

- 1) création/modification/suppression/insertion/reproduction non autorisées de données dans des environnements qui assurent l'intégrité des données par la prévention.

Exemple: raccordement clandestin à une voie sûre.

- 2) création/modification/suppression/insertion/reproduction non autorisées et non détectées dans des environnements qui assurent l'intégrité des données par la détection.

Exemple: l'intégrité des données peut être assurée par le chiffrement des données protégées et des totaux de contrôle associés comme cela est décrit dans la Rec. UIT-T X.274 | ISO/CEI 10736. Si les entités communicantes A et B utilisent la même clé pour assurer le chiffrement et que l'origine des données n'est pas protégée par l'intégrité, les données protégées par l'intégrité qui ont été envoyées de A à B peuvent être soumises ultérieurement à A comme si elles émanaient de B (attaque par réflexion).

En ce qui concerne le support sur lequel les données résident, les menaces peuvent être classées comme suit:

- 1) menaces particulières contre le support sur lequel les données sont mises en mémoire;
- 2) menaces particulières contre le support sur lequel les données sont transmises;
- 3) menaces indépendantes du support.

Dans la mesure où la présente Recommandation | Norme internationale considère les violations d'intégrité comme étant des actions non autorisées, elle ne traite pas la question des modifications autorisées qui peuvent violer la cohérence externe des données, comme indiqué dans l'Annexe B (par exemple, fausse comptabilité). En conséquence, la présente Recommandation | Norme internationale ne traite pas la question des attaques de l'intérieur, contrairement au cadre de confidentialité (ce dernier traite des questions relatives à la protection continue des informations telles que la possibilité, pour un accès autorisé, d'être suivi de la divulgation non autorisée, intentionnelle ou non, d'informations protégées par la confidentialité).

## 5.5 Types d'attaque contre l'intégrité

A chacune des menaces énumérées ci-dessus correspond une ou plusieurs attaques, c'est-à-dire des instanciations de la menace en question. Les attaques visant à déjouer le ou les mécanismes utilisés pour assurer l'intégrité peuvent être classées comme suit:

- 1) attaques visant à déjouer les mécanismes cryptographiques ou à exploiter les faiblesses de ces mécanismes; il s'agit notamment des attaques suivantes:
  - a) pénétration du mécanisme cryptographique;
  - b) suppression et reproduction (sélectives).
- 2) attaques visant à déjouer le mécanisme contextuel utilisé (les mécanismes contextuels échangent des données à des moments et/ou dans des emplacements précis). Il s'agit notamment des attaques suivantes:
  - a) modifications massives et coordonnées de répliques d'éléments de données;
  - b) pénétration du mécanisme d'établissement de contextes.
- 3) attaques visant à déjouer les mécanismes de détection et d'accusé de réception. Il s'agit notamment des attaques suivantes:
  - a) faux accusés de réception;
  - b) exploitation d'un séquençement défectueux entre le mécanisme d'accusé de réception et le traitement des données reçues.
- 4) attaques visant à déjouer ou à suborner les mécanismes de prévention de l'accès; il s'agit notamment des attaques suivantes:
  - a) attaques contre le mécanisme proprement dit;
  - b) pénétration des services dont le mécanisme dépend;
  - c) exploitation des programmes utilitaires avec effets secondaires imprévus.

## 6 Politiques d'intégrité

Une politique d'intégrité est l'élément de la politique de sécurité qui concerne la mise en œuvre et l'utilisation du service d'intégrité.

Les données dont l'intégrité est protégée font l'objet d'un contrôle concernant les entités qui peuvent les créer, les modifier et les supprimer. Une politique d'intégrité doit donc identifier les données qui font l'objet de contrôles et indiquer quelles entités doivent normalement être autorisées à les créer, les modifier ou les supprimer.

Selon l'importance relative de l'intégrité des différents types de données, une politique d'intégrité peut également indiquer le type et la force des mécanismes qu'il convient d'utiliser afin d'assurer les services d'intégrité pour chacun des différents types de données.

La gestion d'une politique de sécurité en termes d'intégrité n'est pas traitée dans la présente Recommandation | Norme internationale.

### 6.1 Expression des politiques

Dans l'expression d'une politique d'intégrité, des moyens sont nécessaires pour identifier les informations et les entités en cause.

Une politique de sécurité peut être considérée comme étant un ensemble de règles. Chaque règle d'une politique d'intégrité peut associer une caractérisation des données et une caractérisation des entités ainsi qu'un ensemble d'activités de traitement des données autorisées (généralement, la création, la modification et la suppression de données). Dans certaines politiques, ces règles ne sont pas exprimées explicitement mais peuvent être déduites de l'expression de la politique.

Un certain nombre de modes d'expression possibles des politiques d'intégrité sont décrits ci-après. Il convient de noter que, même si certains mécanismes d'intégrité peuvent comporter des aspects parallèles dans des types particuliers d'expression des politiques, le mode d'expression d'une politique n'implique pas directement l'utilisation d'un mécanisme spécifique pour la mise en œuvre de cette politique.

### 6.1.1 Caractérisation des données

Une politique peut caractériser les données de diverses manières, par exemple:

- 1) en identifiant les entités autorisées à créer/modifier/supprimer ces données;
- 2) par leur emplacement; ou
- 3) en identifiant le contexte dans lequel les données sont présentées (par exemple, leur fonction envisagée).

### 6.1.2 Caractérisation des entités

Il existe plusieurs manières de caractériser les entités auxquelles s'applique une politique d'intégrité. Deux principaux exemples sont donnés ci-après.

#### 6.1.2.1 Politiques fondées sur l'identité

Dans cette forme d'expression de politique, les entités sont identifiées individuellement ou comme faisant partie d'un groupe d'entités équivalentes (pour les besoins de la politique d'intégrité) ou encore elles sont identifiées par le rôle qu'elles assument. Ainsi, chaque entité admise avec succès à exercer une activité de traitement de données possédera une identité individuelle, une identité de groupe ou une identité de rôle utilisée pour la caractériser.

Dans le cas de rôles, une politique d'intégrité peut spécifier des groupes exclusifs de rôles disponibles pour chaque entité, les rôles de différents groupes ne pouvant alors être revendiqués simultanément.

#### 6.1.2.2 Politiques fondées sur des règles

Dans cette forme d'expression de politique d'intégrité, les attributs sont associés à chaque entité et à chaque élément de données protégé par l'intégrité. Les règles générales qui régissent les attributs des entités et des données déterminent les actions autorisées. Les politiques fondées sur les règles sont examinées plus en détail dans l'aperçu général des Cadres de sécurité (voir la Rec. UIT-T X.810 | ISO/CEI 10181-1).

## 7 Informations et fonctions d'intégrité

Le présent article classe les informations nécessaires pour le bon fonctionnement d'un service d'intégrité ainsi que les fonctionnalités qui utilisent ou génèrent les informations en question.

### 7.1 Informations d'intégrité

Afin de **protéger**, de **valider** les données ou de **retirer leur protection**, on peut utiliser des informations auxiliaires. Ces informations auxiliaires sont appelées «informations d'intégrité». Ces informations d'intégrité peuvent être classées comme suit.

#### 7.1.1 Informations de protection de l'intégrité

Les informations de protection de l'intégrité (SII), sont des informations utilisées pour **protéger** les données; on peut citer les exemples suivants:

- 1) clés privées;
- 2) clés secrètes;
- 3) identificateur d'algorithme et paramètres cryptographiques associés;
- 4) paramètres variant dans le temps (par exemple, timbres horodateurs).

#### 7.1.2 Informations de détection de modification de l'intégrité

Les informations de détection de modification de l'intégrité (MDII), sont des informations utilisées pour **valider** les données protégées par l'intégrité. On peut citer les exemples suivants:

- 1) clés publiques;
- 2) clés secrètes.

#### 7.1.3 Informations de retrait de l'intégrité

Les informations d'intégrité nécessaires au retrait de la protection (UII), sont des informations utilisées pour **retirer la protection** des données dont l'intégrité est protégée. Citons, à titre d'exemple, les informations suivantes:

- 1) clés publiques;
- 2) clés secrètes.

## 7.2 Fonctions d'intégrité

On a identifié un certain nombre de fonctions d'intégrité énumérées dans l'Annexe C. Parmi ces fonctions, on peut distinguer celles qui se rapportent aux aspects d'exploitation et celles qui se rapportent aux aspects de gestion.

### 7.2.1 Fonctions relatives à l'exploitation

Ces fonctions sont les suivantes:

#### 1) **protection**

Cette fonction applique la protection par l'intégrité aux données. Paramètres d'entrée possibles:

- données à protéger;
- informations SII;
- identificateurs spécifiques à un mécanisme, mentionnés dans l'Annexe C.

Paramètres de sortie possibles:

- données protégées par l'intégrité;
- codes d'achèvement/retour;

#### 2) **validation**

Cette fonction vérifie les données protégées par l'intégrité pour détecter d'éventuelles modifications. Paramètres d'entrée possibles:

- données protégées par l'intégrité;
- informations MDII;
- identificateurs spécifiques à un mécanisme, mentionnés dans l'Annexe C.

Paramètres de sortie possibles:

- indication sur la violation éventuelle de l'intégrité des données.

#### 3) **retrait de la protection**

Cette fonction convertit les données protégées par l'intégrité en données initialement **protégées**. Paramètres d'entrée possibles:

- données protégées par l'intégrité;
- informations UII;
- identificateurs spécifiques à un mécanisme, mentionnés dans l'Annexe C.

Paramètres de sortie possibles:

- données;
- codes d'achèvement/retour.

### 7.2.2 Fonctions relatives à la gestion

Les fonctions de gestion de l'intégrité permettent à un utilisateur d'obtenir, de modifier et de supprimer des informations (telles que les clés) qui sont nécessaires pour assurer l'intégrité. Il s'agit, d'une manière générale, des fonctions suivantes:

- 1) installation d'informations de gestion;
- 2) modification d'informations de gestion;
- 3) suppression d'informations de gestion;
- 4) listage d'informations de gestion;
- 5) désactivation d'informations de gestion;
- 6) réactivation d'informations de gestion.

## 8 Classification des mécanismes d'intégrité

Le présent article classe les mécanismes d'intégrité selon les moyens qu'ils utilisent pour assurer un service d'intégrité.

### 8.1 Mise en œuvre de l'intégrité par la cryptographie

Il existe deux classes de mécanisme d'intégrité cryptographique à prendre en considération:

- 1) les mécanismes d'intégrité fondés sur les techniques cryptographiques symétriques dans lesquelles la validation des données protégées par l'intégrité est possible si l'on connaît la clé secrète qui a été utilisée pour protéger les données;
- 2) les mécanismes d'intégrité fondés sur les techniques cryptographiques asymétriques dans lesquelles la validation des données protégées par l'intégrité est possible si l'on connaît la clé publique correspondant à la clé privée qui a été utilisée pour protéger les données.

Les mécanismes du premier type correspondent aux scellés alors que les mécanismes du second type correspondent aux signatures numériques.

On peut utiliser les paramètres variant dans le temps avec des mécanismes d'intégrité fondés sur des techniques cryptographiques, de façon à assurer la protection contre la reproduction.

#### 8.1.1 Mise en œuvre de l'intégrité par les scellés

L'utilisation de scellés assure l'intégrité par l'adjonction d'une valeur de contrôle cryptographique aux données à protéger. Dans cette technique, on utilise la même clé secrète pour protéger et valider l'intégrité des données. Lorsqu'on utilise cette classe de mécanisme, tous les validateurs éventuels sont connus à l'avance ou doivent avoir le moyen d'accéder à la clé secrète.

L'ensemble d'entités capables de sceller les données et l'ensemble d'entités capables de valider les données coïncident par définition.

Ce mécanisme permet de détecter les modifications de la façon suivante:

- **protection:** on l'assure en adjoignant une valeur de contrôle cryptographique aux données qui doivent être protégées par l'intégrité (par exemple, on calcule une fonction unidirectionnelle en plus des données à protéger, valeur qui est transformée à l'aide d'un mécanisme de chiffrement);
- **validation:** on l'obtient en utilisant les données, la valeur de contrôle cryptographique ainsi que la clé secrète pour déterminer si les données correspondent au scellé, (par exemple, la fonction pourrait soumettre les données et la clé secrète à la fonction de protection et comparer le scellé qui en résulte avec la valeur qui a été en fait attribuée aux données). Lorsque les données correspondent au scellé, on considère qu'il n'est pas nécessaire de les modifier;
- **retrait de la protection:** on l'obtient en supprimant la valeur de contrôle cryptographique, dès que les données ont été validées.

#### 8.1.2 Mise en œuvre de l'intégrité par les signatures numériques

Les signatures numériques sont calculées à l'aide d'une clé privée et d'un algorithme cryptographique asymétrique. Les données protégées (à savoir, les données plus la signature numérique ajoutée) peuvent être validées par la clé publique correspondante qui peut en général être publiquement disponible.

Les signatures numériques permettent à l'ensemble d'entités qui peuvent **valider** les données d'avoir une taille et une composition arbitraires.

Le mécanisme permet de détecter les modifications de la façon suivante:

- **protection:** on l'obtient en adjoignant des valeurs de contrôle cryptographique aux données qui doivent être protégées par l'intégrité (par exemple, on calcule une empreinte numérique des données à protéger, valeur qui est combinée avec la clé privée et, éventuellement, avec d'autres paramètres pour générer une ou plusieurs valeurs qui forment, collectivement, la signature numérique);
- **validation:** on l'obtient en utilisant une empreinte numérique des données reçues de la signature numérique et de la clé publique avec un algorithme qui vérifie la signature numérique. Si la vérification de la signature numérique échoue, on considère que les données ont été modifiées;
- **retrait de la protection:** on l'effectue en supprimant la valeur de contrôle cryptographique, une fois que les données ont été validées.

Ce mécanisme peut également assurer l'authentification et la non-répudiation de l'origine des données.

### 8.1.3 Mise en œuvre de l'intégrité par le chiffrement de données redondantes

L'intégrité des données redondantes (par exemple, le langage naturel) peut être assurée par le chiffrement. Les données qui comportent des codes de détection d'erreur et des empreintes numériques sont redondantes et leur intégrité peut être protégée par le chiffrement (à condition que l'algorithme de chiffrement utilisé empêche de prédire comment les modifications apportées aux données chiffrées seront reflétées sur les données initiales après déchiffrement).

Les protocoles de sécurité de couche inférieure (voir les Rec. UIT-T X.273 | ISO/CEI 11577 et UIT-T X.274 | ISO/CEI 10736) utilisent ce type de mécanisme pour assurer l'intégrité des données protégées par la confidentialité.

Ce mécanisme permet de détecter la modification des données de la façon indiquée ci-après:

- **protection:** on l'obtient en chiffrant les données redondantes.
- **validation:** on l'obtient en déchiffrant les données protégées et en déterminant si celles-ci satisfont aux invariances éventuelles auxquelles ont satisfait les données initiales.

Exemples:

- 1) si les données initiales constituaient une séquence de caractères ASCII, les données récupérées devraient avoir la même propriété;
  - 2) si les données initiales étaient censées être exprimées par un être humain dans une langue donnée, les données récupérées devraient être exprimées dans le même langage communément accepté par l'homme, ou (être accompagnées de légères modifications);
  - 3) si les données initiales contenaient des totaux de contrôle, on peut calculer les mêmes totaux sur les parties pertinentes des données protégées et voir si les résultats correspondent aux valeurs de total de contrôle incorporées dans les données déchiffrées.
- **retrait de la protection:** on l'effectue en déchiffrant les données chiffrées.

NOTE – On sait que ce mécanisme ne se prête pas à plusieurs formes communes de redondance (par exemple, des données avec codes de détection d'erreur) utilisées avec des formes communes de chiffrement (par exemple, chiffres en bloc, tels que DES, avec ou sans chaînage). Un exemple relativement simple de pièges possibles est indiqué ci-après:

Si un texte ASCII (par exemple, du courrier électronique courant) devait être protégé par un chiffrement DES, le message pourrait être modifié de manière non décelable par troncature (à moins naturellement que l'en-tête du courrier renferme un indicateur de longueur, comme c'est fréquemment le cas).

## 8.2 Mise en œuvre de l'intégrité par le contexte

On peut assurer l'intégrité par des mécanismes qui mettent en mémoire ou transmettent les données dans un ou plusieurs contextes convenus au préalable. Ces mécanismes peuvent protéger les données ainsi que les structures de données (par exemple, séquences d'unités de données). Il s'agit notamment des mécanismes indiqués ci-après.

### 8.2.1 Reproduction des données

Cette classe de mécanismes d'intégrité est fondée sur la reproduction des données dans l'espace (par exemple, plusieurs zones de mise en mémoire) ou dans le temps (par exemple, à différents instants). On admet implicitement que des «attaquants» éventuels ne peuvent simultanément compromettre plus qu'un nombre limité de répliques et que, chaque fois que des attaques sont détectées, on peut reconstruire les données à partir des copies authentiques.

A titre d'exemple, un tel mécanisme peut être utilisé par des bases de données résistant aux attaques de pénétration.

Ces mécanismes assurent la détection de la perte d'intégrité avec récupération des données et peuvent être utilisés conjointement avec d'autres mécanismes de sécurité. Ils assurent l'intégrité de la façon suivante:

- on assure la **protection** en établissant de nombreuses copies des mêmes données successivement dans le temps ou à différents emplacements;
- on assure la **validation** en recueillant une copie des données à chacun des instants ou des emplacements déterminés. On les compare et, si elles ne sont pas toutes identiques, on en déduit qu'il s'est produit une violation d'intégrité;
- on peut effectuer le **retrait de la protection** (avec récupération) lorsqu'un critère préétabli est rempli (par exemple, «90% des valeurs ou plus concordent») en choisissant comme valeur correcte celle qui minimise une mesure affectée au préalable (par exemple, la probabilité d'une récupération erronée).

Il convient de noter que notre critère de récupération doit être satisfait lorsque toutes les valeurs concordent et que, dans ces circonstances, la valeur qui minimise la mesure doit être la valeur commune.

### 8.2.2 Contexte convenu au préalable

Ces mécanismes assurent la détection de la suppression de données protégées par l'intégrité et sont souvent utilisés conjointement avec d'autres mécanismes d'intégrité.

- on effectue la **protection** en fournissant les données à un instant et/ou un emplacement spécifiques dans les limites d'un niveau de variation donné;
- on effectue la **validation** en comptant sur les données à un instant et/ou un emplacement précis. Si elles ne sont pas présentes, on estime qu'une violation de l'intégrité a eu lieu.

Pour empêcher la substitution d'autres données il faut, comme indiqué plus haut, combiner ce mécanisme avec d'autres mécanismes d'intégrité.

### 8.3 Mise en œuvre de l'intégrité par détection et accusé de réception

Ces mécanismes utilisent une détection d'intégrité chaque fois que des opérations «équipotentes» avec rétroinformation positive sont effectuées (une opération est jugée «équipotente» si des exécutions multiples et successives de cette opération donnent le même résultat qu'une seule d'entre elles). Les transmissions avec accusés de réception positifs (telles que celles de la classe de transport 4 décrite dans la Rec. UIT-T X.224 | ISO/CEI 8073) et les opérations distantes avec rétroinformation sont des exemples de ces mécanismes. Ces mécanismes supposent que les opérations de **protection** et de **validation/retrait de protection** portent sur la même durée et ne sont pas, en général, appropriées pour la mise en mémoire des données.

- **protection**: cette opération est exécutée par répétition de la même action jusqu'à ce que d'autres dispositions doivent être prises en vertu de la politique d'intégrité ou jusqu'à l'obtention d'un accusé de réception positif;
- **validation**: cette opération est exécutée sur chaque instance de données protégées (sauf dispositions contraires prévues par la politique d'intégrité); toute validation effectuée avec succès se traduit par l'envoi d'un accusé de réception positif à l'entité qui exécute l'opération de protection.

Si une correction peut être effectuée pour la remise d'informations correctes à partir de l'opération de **retrait de protection** du mécanisme de protection contre la modification de l'intégrité utilisée, ce mécanisme peut envoyer un accusé de réception positif.

On renforce l'efficacité du système si, lorsque l'opération de **validation** indique un résultat négatif (une modification ou une suppression des données a eu lieu), un accusé de réception négatif est envoyé à l'entité qui exécute l'opération de **protection**.

Ces mécanismes sont fondés sur l'hypothèse que les modifications des données peuvent être détectées par d'autres moyens et, par conséquent, ils peuvent être considérés comme étant des mécanismes améliorés de protection contre une modification des données.

### 8.4 Mise en œuvre de l'intégrité par prévention

On peut assurer l'intégrité en empêchant l'accès physique aux supports de transmission ou de mise en mémoire des données et par le contrôle d'accès.

La spécification des moyens d'empêcher l'accès physique n'est pas traitée ici.

Le contrôle d'accès est décrit dans la Recommandation relative au Cadre du contrôle d'accès.

## 9 Interactions avec d'autres services et mécanismes de sécurité

Le présent article indique comment on peut utiliser d'autres services et mécanismes de sécurité pour assurer l'intégrité. L'utilisation de l'intégrité pour assurer d'autres services de sécurité n'est pas décrite ici.

### 9.1 Contrôle d'accès

On peut utiliser le contrôle d'accès pour créer des environnements protégés par l'intégrité.

### 9.2 Authentification de l'origine des données

On peut utiliser l'authentification de l'origine des données pour assurer l'intégrité. Par exemple, si l'origine d'une unité PDU ne peut être authentifiée, cette unité PDU peut être jugée douteuse. De même, si la source présumée d'une unité PDU n'est pas autorisée à créer l'unité PDU, il s'est produit une violation de l'intégrité.

### 9.3 Confidentialité

Dans certains cas on peut combiner la redondance avec le chiffrement pour obtenir des données qui ne peuvent être modifiées sans détection.

En fait, les données redondantes (telles que le langage naturel et les données y compris les totaux et les fonctions de hachage) ont des propriétés invariantes. En règle générale, les modifications apportées aux données chiffrées ne préservent pas, avec une forte probabilité, ces propriétés une fois que les données modifiées sont «déchiffrées».

(On peut dire aussi que lorsque  $k$  bits d'information sont codés en séquences binaires  $k + m$ , les codages valables constituent un sous-ensemble incomplet de toutes les séquences binaires possibles; si, après déchiffrement, les modifications apportées au résultat des données chiffrées donnent lieu à des modifications qui sont considérées comme étant aléatoires du point de vue de l'attaquant, la probabilité que des données altérées soient déchiffrées comme codage valable est de l'ordre de  $2^{-m}$ .)

La redondance (y compris les totaux de contrôle et les fonctions de hachage) utilisée conjointement avec la confidentialité fondée sur la cryptographie peut donc assurer l'intégrité.

## Annexe A

### Intégrité dans le modèle de référence de base OSI

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

La relation des services de sécurité avec le modèle de référence OSI est définie dans la Rec. UIT-T X.800 du CCITT | ISO 7498-2. La présente annexe résume les aspects relatifs à l'intégrité.

Différents services de sécurité, indiqués ci-après, sont pris en considération:

- intégrité en mode connexion avec reprise;
- intégrité en mode connexion sans reprise;
- intégrité sélective du champ en mode connexion;
- intégrité en mode sans connexion;
- intégrité sélective du champ en mode sans connexion.

#### A.1 Intégrité en mode connexion avec reprise

L'intégrité en mode connexion assure l'intégrité de toutes les données d'utilisateur (N) sur une connexion (N) et détecte toute donnée modifiée, insérée, supprimée ou répétée dans une séquence entière d'unités SDU (avec tentative de reprise).

#### A.2 Intégrité en mode connexion sans reprise

L'intégrité en mode connexion assure l'intégrité de toutes les données d'utilisateur (N) sur une connexion (N) et détecte toute donnée modifiée, insérée, supprimée ou répétée dans une séquence entière d'unités SDU (sans tentative de reprise).

#### A.3 Intégrité sélective du champ en mode connexion

L'intégrité sélective du champ assure l'intégrité de champs sélectionnés dans les données d'utilisateur (N) d'une unité SDU (N) transférée sur une connexion et prend la forme d'une indication permettant de savoir si les champs sélectionnés ont été modifiés, insérés, supprimés ou répétés.

#### A.4 Intégrité en mode sans connexion

Lorsque ce service est fourni par la couche (N), il donne l'assurance de l'intégrité à l'entité (N + 1) requérante.

#### A.5 Intégrité sélective du champ en mode sans connexion

Ce service assure l'intégrité de champs sélectionnés dans une unité SDU (N) en mode sans connexion et prend la forme d'une indication permettant de savoir si les champs sélectionnés ont été modifiés.

#### A.6 Utilisation de l'intégrité dans les couches OSI

Les services d'intégrité s'appliquent aux couches OSI suivantes:

- couche liaison de données (couche 2);
- couche réseau (couche 3);
- couche transport (couche 4);
- couche application (couche 7).

##### A.6.1 Utilisation de l'intégrité au niveau de la couche liaison de données

Les services d'intégrité peuvent être assurés au niveau de la couche liaison de données comme cela est décrit dans IEEE 802.10.

**A.6.2 Utilisation de l'intégrité au niveau de la couche réseau**

L'intégrité en mode connexion sans reprise et l'intégrité en mode sans connexion sont les seuls services de sécurité assurés au niveau de la couche réseau. L'intégrité en mode connexion sans reprise et l'intégrité en mode sans connexion peuvent être assurées par un mécanisme d'intégrité des données parfois combiné à un mécanisme de chiffrement. Ces services permettent d'assurer l'intégrité entre les nœuds de réseau, les nœuds de sous-réseau ou les relais.

**A.6.3 Utilisation de l'intégrité au niveau de la couche transport**

L'intégrité en mode connexion avec reprise, l'intégrité en mode connexion sans reprise et l'intégrité en mode sans connexion sont les seuls services de sécurité assurés au niveau de la couche transport. L'intégrité en mode connexion avec ou sans reprise et l'intégrité en mode sans connexion peuvent être assurées par un mécanisme d'intégrité des données parfois combiné à un mécanisme de chiffrement. Ces services permettent d'assurer l'intégrité entre les systèmes terminaux.

**A.6.4 Utilisation de l'intégrité au niveau de la couche application**

Tous les services d'intégrité, à savoir l'intégrité en mode connexion avec reprise, l'intégrité en mode connexion sans reprise, l'intégrité sélective du champ en mode connexion, l'intégrité en mode sans connexion et l'intégrité sélective du champ en mode sans connexion peuvent être assurées au niveau de la couche application. L'intégrité en mode connexion avec ou sans reprise et l'intégrité en mode sans connexion peuvent être prises en charge à l'aide d'un mécanisme d'intégrité des données de couche inférieure (parfois combiné à un mécanisme de chiffrement). L'intégrité sélective du champ peut être assurée par un mécanisme d'intégrité des données de couche inférieure (parfois combiné à un mécanisme de chiffrement) au niveau de la couche présentation.

## Annexe B

## Cohérence externe des données

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

NOTE – Le texte ci-après traite les questions d'intégrité interne/externe (développées dans le document initial de Clark et Wilson ainsi que dans d'autres travaux ultérieurs) et analyse l'incidence que ces notions pourraient avoir sur le cadre d'intégrité. Chaque fois que cela est possible et afin de réduire tout risque de paraphrase, le texte reproduit certains passages des publications citées.

Les références non normatives 1, 2 et 3 mentionnées ci-après contiennent un certain nombre de références à un modèle d'intégrité proposé par D.D. Clark et D.R. Wilson. Le texte qui suit a pour but de résumer ce modèle et de mettre en lumière les points susceptibles d'influencer le cadre de sécurité dont il est question ici.

Ce cadre interprète l'intégrité en termes de maintien d'un invariant spécifique concernant les données (la valeur constante de ces données). Le modèle de Clark et Wilson prend en considération des invariants complémentaires. Il suppose notamment qu'un système informatique reflète et émule des données et des processus qui sont externes à l'ordinateur. Le test final d'intégrité consiste donc à s'assurer que les données contenues dans l'ordinateur sont en conformité avec le monde qu'elles sont censées représenter. Il en résulte que les contrôles d'intégrité ne peuvent jamais être une question strictement interne à l'ordinateur.

En conséquence, l'intégrité des données dans un modèle de Clark-Wilson peut être considérée comme étant une approche en deux étapes:

- 1) des mécanismes adéquats doivent exister pour déclencher des modifications, lorsque celles-ci sont nécessaires, de sorte que la cohérence externe des données soit maintenue;
- 2) des mécanismes adéquats doivent exister pour que, lorsque des modifications sont déclenchées, elles soient exécutées comme une opération atomique d'une transaction bien formée.

Dans l'hypothèse où les points ci-dessus reflètent exactement notre interprétation intuitive de l'intégrité, nous sommes amenés à établir la distinction sémantique suivante:

- **cohérence interne:** une donnée est intérieurement cohérente si, et seulement si, toutes les modifications de cette donnée répondent aux exigences d'intégrité pertinentes des politiques de sécurité;
- **cohérence externe:** une donnée est extérieurement cohérente chaque fois que sa valeur est conforme à la situation du monde réel qu'elle décrit.

Si on accepte cette distinction, elle peut être combinée avec la classification ci-après de la force de la protection de l'intégrité:

- une protection forte maintient la cohérence interne et externe des données. Une protection faible détecte la violation de la cohérence interne et/ou externe des données.

En outre, et dans la mesure où les modifications des données sont exécutées comme des opérations atomiques par des processus fiables, on peut souhaiter examiner les propriétés de ces opérations pour répondre aux questions suivantes:

- 1) l'atomicité de l'opération peut-elle être violée?;
- 2) a-t-on des assurances que l'opération sera effectivement exécutée?

Enfin, on peut souhaiter classer les mécanismes d'intégrité en fonction du maintien des propriétés suivantes:

- cohérence interne/externe;
- protection faible/forte;
- atomicité/assurance des opérations sur les données protégées.

Lorsqu'on spécifie un mécanisme d'intégrité, il faut donc prendre en considération les aspects suivants:

- 1) quelle forme de cohérence (interne, externe ou les deux) le mécanisme assure-t-il?
- 2) assure-t-il une protection faible ou forte de l'intégrité des données? Résiste-t-il aux attaques techniques, aux modifications aléatoires ou aux deux? Assure-t-il la récupération des données?
- 3) protège-t-il l'atomicité des opérations et donne-t-il (aussi) l'assurance que l'opération sera bien exécutée?

## Références

- 1) CLARK, David et WILSON, David: A Comparison of Commercial and Military Computer Security Policies, *Proceedings of 1987 IEEE Symposium on Security and Privacy*.
- 2) NIST Special Publication 500-160: Report on the Invitational Workshop on Integrity Policy in Computer Information Systems (WIPCIS); édité par Stuart W. Katzke et Zella G. Ruthberg.
- 3) NIST Special Publication 500-168: Report on the Invitational Workshop on Data Integrity; édité par Zella G. Ruthberg et William T. Polk.

## Annexe C

## Description générale des fonctions d'intégrité

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

|                                                         |                                                  |                                                                                                                             |                                                                                                                                                                        |                                                                                                                                                                                                                                                       |                                                                                                                                    |               |
|---------------------------------------------------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Description générale des fonctions d'intégrité          |                                                  |                                                                                                                             | Elément                                                                                                                                                                | Entité: Initiateur, vérificateur, intégrité-TTP                                                                                                                                                                                                       |                                                                                                                                    |               |
|                                                         |                                                  |                                                                                                                             |                                                                                                                                                                        | Fonction:                                                                                                                                                                                                                                             |                                                                                                                                    |               |
|                                                         |                                                  |                                                                                                                             |                                                                                                                                                                        | Objet d'information: Données protégées par l'intégrité                                                                                                                                                                                                |                                                                                                                                    |               |
|                                                         |                                                  |                                                                                                                             | But du service                                                                                                                                                         | Protéger les données contre toute modification/suppression/création/insertion/reproduction non autorisée                                                                                                                                              |                                                                                                                                    |               |
| A<br><br>C<br>T<br><br>I<br>V<br><br>I<br>T<br><br>É    |                                                  | Entité                                                                                                                      | Autorité de domaine de sécurité (SDA)                                                                                                                                  |                                                                                                                                                                                                                                                       |                                                                                                                                    |               |
|                                                         |                                                  | Fonction                                                                                                                    |                                                                                                                                                                        |                                                                                                                                                                                                                                                       |                                                                                                                                    |               |
|                                                         | Activité relative à la gestion                   |                                                                                                                             | – Installation des informations de gestion<br>– Modification des informations de gestion<br>– Suppression des informations de gestion                                  |                                                                                                                                                                                                                                                       | – Listage des informations de gestion<br>– Désactivation des informations de gestion<br>– Réactivation des informations de gestion |               |
|                                                         |                                                  | Entité                                                                                                                      | Initiateur                                                                                                                                                             |                                                                                                                                                                                                                                                       | Vérificateur                                                                                                                       | Intégrité-TTP |
|                                                         |                                                  | Fonction                                                                                                                    |                                                                                                                                                                        |                                                                                                                                                                                                                                                       |                                                                                                                                    |               |
|                                                         | Activité relative à l'exploitation               | – Protection des données<br>Etiquette ACL<br>Total de contrôle<br>Valeur de contrôle cryptographique<br>Signature numérique |                                                                                                                                                                        | – Validation d'intégrité<br>Etiquette ACL<br>Total de contrôle<br>Valeur de contrôle cryptographique<br>Signature numérique<br><br>– Retrait de la protection (récupération des données)<br>Valeur de contrôle cryptographique<br>Signature numérique | – Emission:<br>ACL<br>Valeur de contrôle cryptographique<br>Total de contrôle<br>Certificat                                        |               |
|                                                         |                                                  |                                                                                                                             |                                                                                                                                                                        |                                                                                                                                                                                                                                                       |                                                                                                                                    |               |
| I<br>N<br>F<br>O<br>R<br>M<br>A<br>T<br><br>I<br>O<br>N | Elément de données entrée/sortie géré par la SDA |                                                                                                                             | – Identités (initiateur, vérificateur, intégrité-TTP)<br>– Clés cryptographiques<br>– Valeur de variante temporelle                                                    |                                                                                                                                                                                                                                                       |                                                                                                                                    |               |
|                                                         | Type d'information utilisé dans l'opération      |                                                                                                                             | – Information d'intégrité «protection» (SII)<br>– Information d'intégrité «détection de modification (MDII)<br>– Information d'intégrité «retrait de protection» (UII) |                                                                                                                                                                                                                                                       |                                                                                                                                    |               |
|                                                         | Informations de contrôle                         |                                                                                                                             | – Période de temps<br>– Voies d'acheminement                                                                                                                           |                                                                                                                                                                                                                                                       | – Emplacement<br>– Etat du système                                                                                                 |               |

La présente annexe utilise les concepts suivants:

## C.1 Entités d'intégrité

L'intégrité dans les systèmes ouverts implique certaines entités de base:

- initiateur;
- vérificateur;
- tierce partie de confiance pour les fonctions d'intégrité.

**C.1.1 Initiateur**

Entité qui génère des données protégées par l'intégrité en protégeant les données et en les envoyant ou en les mettant en mémoire.

**C.1.2 Vérificateur**

Entité qui reçoit ou extrait des données provenant de l'initiateur, vérifie leur valeur après les avoir validées pour détecter une perte d'intégrité et, le cas échéant, régénère la valeur des données.

**C.1.3 Tierce partie de confiance (TTP) pour les fonctions d'intégrité**

Entité qui distribue des informations SII ou MDI et/ou effectue des opérations relatives à l'intégrité au nom de l'initiateur ou du vérificateur.