



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.814

(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
DE CONFIDENTIALITÉ

Recommandation UIT-T X.814

(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.814 de l'UIT-T a été approuvé le 21 novembre 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10181-5.

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

TABLE DES MATIÈRES

	<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
3	Définitions..... 2
3.1	Définitions du modèle de référence de base 2
3.2	Définitions de l'architecture de sécurité 3
3.3	Définitions de l'aperçu général des cadres de sécurité 3
3.4	Définitions additionnelles 3
4	Abréviations 4
5	Présentation générale de la confidentialité 4
5.1	Principes de base..... 4
5.1.1	Protection des informations 4
5.1.2	Opérations de dissimulation et de révélation 5
5.2	Types de services de confidentialité 5
5.3	Types de mécanismes de confidentialité..... 6
5.4	Menaces contre la confidentialité..... 7
5.4.1	Menaces lorsque la confidentialité est assurée par des mesures visant à empêcher l'accès 7
5.4.2	Menaces lorsque la confidentialité est assurée par la dissimulation des informations..... 7
5.5	Types d'attaques contre la confidentialité 7
6	Politiques de confidentialité 8
6.1	Expression des politiques..... 8
6.1.1	Caractérisation des informations..... 8
6.1.2	Caractérisation des entités..... 8
7	Informations et fonctions de confidentialité..... 8
7.1	Informations de confidentialité 8
7.1.1	Informations de confidentialité «dissimulation»..... 9
7.1.2	Informations de confidentialité «révélation» 9
7.2	Fonctions de confidentialité 9
7.2.1	Fonctions relatives à l'exploitation..... 9
7.2.1.1	Dissimulation 9
7.2.1.2	Révélation 9
7.2.2	Fonctions relatives à la gestion 10
8	Mécanismes de confidentialité 10
8.1	Mise en œuvre de la confidentialité par des mesures visant à empêcher l'accès..... 10
8.1.1	Mise en œuvre de la confidentialité par la protection des supports physiques 10
8.1.2	Mise en œuvre de la confidentialité par le contrôle de l'acheminement 10
8.2	Mise en œuvre de la confidentialité par le chiffrement..... 10
8.2.1	Mise en œuvre de la confidentialité par le remplissage de données 11
8.2.2	Mise en œuvre de la confidentialité par des événements fictifs..... 11
8.2.3	Mise en œuvre de la confidentialité par la protection des en-têtes d'unité PDU..... 11
8.2.4	Mise en œuvre de la confidentialité par des champs variant dans le temps..... 11
8.3	Mise en œuvre de la confidentialité par l'emplacement contextuel 12
9	Interactions avec d'autres services et mécanismes de sécurité 12
9.1	Contrôle d'accès 12

	<i>Page</i>
Annexe A – Confidentialité dans le modèle de référence OSI	13
A.1 Confidentialité en mode connexion	13
A.2 Confidentialité en mode sans connexion.....	13
A.3 Confidentialité sélective des champs	13
A.4 Confidentialité du flux de trafic	13
A.5 Utilisation de la confidentialité dans les couches OSI	13
A.5.1 Utilisation de la confidentialité au niveau de la couche physique	13
A.5.2 Utilisation de la confidentialité au niveau de la couche liaison de données	13
A.5.3 Utilisation de la confidentialité au niveau de la couche réseau.....	14
A.5.4 Utilisation de la confidentialité au niveau de la couche transport.....	14
A.5.5 Utilisation de la confidentialité au niveau de la couche présentation	14
A.5.6 Utilisation de la confidentialité au niveau de la couche application	14
Annexe B – Exemple de séquence de passages par différents contextes de protection de la confidentialité	15
Annexe C – Représentation des informations	16
Annexe D – Voies occultes	17
Annexe E – Description générale des fonctions de confidentialité	18
E.1 Entités de confidentialité.....	18
E.1.1 Initiateur.....	18
E.1.2 Vérificateur	18
E.1.3 Tierce partie de confiance (TTP) pour les fonctions de confidentialité	18

Résumé

La présente Recommandation définit un cadre général pour la fourniture de services de confidentialité. La confidentialité est une propriété selon laquelle aucune information n'est communiquée ou divulguée à des individus, entités ou processus non autorisés.

Introduction

De nombreuses applications de systèmes ouverts ont des exigences en matière de sécurité qui dépendent des mesures prises pour empêcher la divulgation des informations. Ces exigences peuvent inclure la protection des informations utilisées pour assurer d'autres services de sécurité tels que l'authentification, le contrôle d'accès ou l'intégrité qui, si elles sont connues d'un «attaquant», risquent de réduire ou d'annihiler l'efficacité de ces services.

La confidentialité est une propriété selon laquelle aucune information n'est communiquée ou divulguée à des individus, entités ou processus non autorisés.

La présente Recommandation | Norme internationale définit un cadre général pour la fourniture de services de confidentialité.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

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

1 Domaine d'application

La présente 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» s'applique notamment à 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 la confidentialité des informations lors de l'extraction, du transfert et de la gestion des données

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

Plusieurs types de normes peuvent utiliser ce cadre de sécurité, notamment

- 1) les normes qui incorporent le concept de confidentialité;
- 2) les normes qui spécifient des services abstraits incluant la confidentialité;
- 3) les normes qui spécifient les utilisations d'un service de confidentialité;
- 4) les normes qui spécifient les moyens d'assurer la confidentialité dans une architecture de système ouvert;
- 5) les normes qui spécifient les mécanismes de confidentialité.

De telles normes peuvent utiliser ce cadre de sécurité comme indiqué ci-dessous:

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

Comme avec d'autres services de sécurité, la confidentialité ne peut être assurée que dans le contexte d'une politique de sécurité déterminée pour une application particulière. Les définitions de politiques de sécurité spécifiques sortent du cadre de la présente Recommandation | Norme internationale.

La présente Recommandation | Norme internationale n'a pas pour but de spécifier les détails des échanges de protocole qu'il convient d'effectuer pour assurer la confidentialité.

La présente Recommandation | Norme internationale ne spécifie pas les mécanismes particuliers nécessaires pour assurer ces services de confidentialité ni les détails complets des services et protocoles de gestion de sécurité. Les mécanismes génériques nécessaires pour assurer la confidentialité sont décrits à l'article 8.

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

NOTE – Bien que l'ISO ne normalise pas les algorithmes cryptographiques, elle normalise néanmoins les procédures utilisées pour les enregistrer dans l'ISO/CEI 9979:1991 – Procédures pour l'enregistrement des algorithmes cryptographiques.

Ce cadre de sécurité s'applique à la mise en œuvre de la confidentialité lorsque les informations sont représentées par des données dont la lecture est accessible à d'éventuels «attaquants». Son domaine d'application englobe la confidentialité du flux de trafic.

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. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-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.233 (1993) | ISO/CEI 8473-1:1994, *Technologies de l'information – Protocole assurant le service réseau en mode sans connexion de l'interconnexion de systèmes ouverts: spécification du protocole.*
- Recommandation UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – 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.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 X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*
ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: architecture de sécurité.*

3 Définitions

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

3.1 Définitions du modèle de référence de base

La présente Recommandation | Norme internationale utilise les termes généraux relatifs à la sécurité définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1 et énumérés ci-dessous:

- a) connexion (N);
- b) entité (N);
- c) fonctionnalité (N);
- d) couche (N);

- e) PDU (N);
- f) SDU (N);
- g) service (N);
- h) données sans connexion (N);
- i) données d'utilisateur (N);
- j) segmentation.

3.2 Définitions de l'architecture de sécurité

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

- a) menace active;
- b) confidentialité;
- c) déchiffrement (decipherment);
- d) déchiffrement (decryption);
- e) chiffrement (encipherment);
- f) chiffrement (encryption);
- g) politique de sécurité fondée sur l'identité;
- h) clé;
- i) menace passive;
- j) contrôle de routage;
- k) politique de sécurité fondée sur des règles;
- l) sensibilité;
- m) analyse du trafic;
- n) bourrage.

3.3 Définitions de l'aperçu général des cadres de sécurité

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

- a) clé secrète;
- b) clé privée;
- c) clé publique.

3.4 Définitions additionnelles

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

3.4.1 environnement protégé par la confidentialité: Environnement qui empêche la divulgation non autorisée d'informations en prévenant toute inspection non autorisée des données ou toute obtention non autorisée d'informations sensibles par l'inspection des données. Les informations sensibles peuvent inclure une partie ou la totalité des attributs de données (valeur, taille, existence, etc.).

3.4.2 données protégées par la confidentialité: Données et tous attributs associés contenus dans un environnement protégé par la confidentialité.

NOTE – Un environnement protégé par la confidentialité peut également protéger une partie (ou la totalité) des attributs des données protégées par la confidentialité.

3.4.3 informations protégées par la confidentialité: Informations dont tous les codages concrets (c'est-à-dire les données) sont protégés par la confidentialité.

3.4.4 dissimulation: Opération qui applique une protection par confidentialité à des données non protégées ou une protection par confidentialité supplémentaire à des données déjà protégées.

3.4.5 révélation: Opération qui supprime une partie ou la totalité de la protection par confidentialité appliquée précédemment.

3.4.6 informations de confidentialité «dissimulation»: Informations utilisées pour exécuter l'opération de dissimulation.

3.4.7 informations de confidentialité «révélation»: Informations utilisées pour exécuter l'opération de révélation.

3.4.8 attaque directe: Attaque d'un système fondé sur les déficiences des algorithmes, des principes ou des propriétés sur lesquels s'appuie un mécanisme de sécurité.

3.4.9 attaque indirecte: Attaque d'un système qui n'est pas fondé sur les déficiences d'un mécanisme de sécurité particulier (par exemple, attaques qui contournent le mécanisme ou qui dépendent de l'utilisation incorrecte du mécanisme par le système).

4 Abréviations

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

HCI	Informations de confidentialité dissimulation (<i>hiding confidentiality information</i>)
PDU	Unité de données de protocole (<i>protocol data unit</i>)
RCI	Informations de confidentialité révélation (<i>revealing confidentiality information</i>)
SDU	Unité de données de service (<i>service data unit</i>)

5 Présentation générale de la confidentialité

5.1 Principes de base

Le but du service de confidentialité est de faire en sorte que les informations ne soient communiquées qu'à des parties autorisées. Dans la mesure où les informations sont représentées par des données et où ces données peuvent entraîner des modifications contextuelles (par exemple, des manipulations de fichiers peuvent entraîner des modifications de répertoire ou des modifications du nombre d'emplacements de mise en mémoire disponibles), les informations peuvent être obtenues de diverses manières à partir d'une donnée, comme indiqué ci-après:

- 1) par la compréhension de la sémantique des données (par exemple, la valeur des données);
- 2) par l'utilisation des attributs associés des données (par exemple, existence, date de création, taille, date de la dernière mise à jour, etc.) pour en tirer des déductions;
- 3) par l'examen du contexte des données, c'est-à-dire des autres objets de données qui lui sont associés;
- 4) par l'observation des variations dynamiques de la représentation.

On peut protéger les informations en veillant à ce que la communication des données soit limitée aux parties autorisées ou en représentant les données de telle sorte que leur sémantique ne reste accessible qu'à ceux qui possèdent certaines informations critiques. Pour qu'une protection par la confidentialité soit efficace, il faut que les informations de contrôle nécessaires (telles que les clés et autres informations RCI) soient protégées. Cette protection peut être assurée par des mécanismes qui sont différents de ceux que l'on utilise pour protéger les données (par exemple, les clés cryptographiques peuvent être protégées par des moyens physiques).

Les notions d'environnements protégés et d'environnements de chevauchement protégés sont utilisées dans ce cadre de sécurité. Les données contenues dans les environnements protégés sont protégées par l'application d'un mécanisme (ou de mécanismes) de sécurité particulier(s). Toutes les données contenues dans un environnement protégé sont donc protégées de la même façon. Lorsque deux environnements ou plus se chevauchent, les données contenues dans la zone de chevauchement bénéficient d'une protection multiple. On peut en déduire que la protection continue de données transférées d'un environnement à l'autre implique nécessairement l'existence d'environnements de chevauchement protégés.

5.1.1 Protection des informations

On réalise la communication ou la mise en mémoire d'informations en représentant les informations sous la forme d'éléments de données. Les mécanismes de confidentialité assurent la protection contre la divulgation d'informations en protégeant les parties ou la totalité des éléments de données énumérées au 5.1 ci-dessus.

Pour assurer la confidentialité, on peut utiliser notamment les moyens suivants:

- 1) empêcher que l'on connaisse l'existence des données ou les caractéristiques des données (telles que la taille ou la date de création des données);
- 2) empêcher l'accès à la lecture des données;
- 3) empêcher que l'on connaisse la sémantique des données.

Les mécanismes de confidentialité assurent la protection contre la divulgation des informations

- 1) en empêchant la divulgation du mode de représentation des éléments d'information; ou
- 2) en empêchant la divulgation des règles de représentation.

Dans le second cas, on peut assurer la protection contre la divulgation de l'existence ou d'autres attributs d'un élément de données en combinant plusieurs éléments de données en un élément de données composite et en empêchant la divulgation des règles de représentation de l'objet composite.

5.1.2 Opérations de dissimulation et de révélation

L'opération de **dissimulation** peut être modélisée sous la forme d'un transfert d'informations d'un environnement A à (B), environnement de chevauchement de A avec un autre environnement C. L'opération de révélation peut être considérée comme étant l'opposé de l'opération de dissimulation. Ces opérations sont illustrées par un graphique dans l'Annexe B.

Lorsque des informations sont transférées d'un environnement protégé par un mécanisme de confidentialité à un environnement protégé par un autre mécanisme de confidentialité:

- 1) si l'opération de **dissimulation** du second mécanisme précède l'opération de **révélation** du premier mécanisme, les informations sont protégées d'une manière continue;
- 2) si l'opération de **révélation** du premier mécanisme précède l'opération de **dissimulation** du second mécanisme, les informations ne sont pas protégées d'une manière continue.

Pour que le point 1) ci-dessus soit possible, une certaine forme de commutativité doit exister entre l'opération de **révélation** de l'ancien mécanisme et l'opération de **dissimulation** du nouveau mécanisme. A titre d'exemple d'opérations de **dissimulation** et de **révélation** avec des propriétés commutatives, on peut citer le cas où un environnement est protégé par le contrôle d'accès ou par des moyens physiques et où l'autre environnement est protégé par des transformations cryptographiques.

La confidentialité a une incidence, comme indiqué ci-après, sur l'extraction, le transfert et la gestion des informations:

- 1) la confidentialité est assurée, dans le transfert d'informations utilisant l'interconnexion OSI, lorsque l'opération de **dissimulation**, l'opération de transfert utilisant une fonctionnalité (N-1), et l'opération de **révélation** sont combinées pour former la partie transmission d'un service (N);
- 2) la confidentialité est assurée, dans l'extraction et la mise en mémoire de données, lorsque l'opération de **dissimulation**, l'opération de mise en mémoire et d'extraction, et l'opération de **révélation** sont combinées pour former un service de mise en mémoire et d'extraction d'un niveau plus élevé;
- 3) d'autres formes de confidentialité peuvent être assurées par la combinaison des opérations de **dissimulation** et de **révélation** avec d'autres opérations (par exemple, celles qui sont utilisées pour les besoins de la gestion des données).

Avec certains mécanismes de confidentialité, la fonction de **dissimulation** divulgue une partie des données protégées par la confidentialité à l'utilisateur du service avant que la fonction ait achevé le traitement de toutes les données. De même, avec certains mécanismes, la fonction de **révélation** peut commencer à travailler sur la partie traitement d'un élément de données protégé par la confidentialité avant même qu'il soit totalement disponible. Ainsi, un élément de données peut comprendre simultanément des parties qui ne sont pas encore **dissimulées**, des parties qui sont **dissimulées** et des parties qui ont été **révélées**.

5.2 Types de services de confidentialité

Les services de confidentialité peuvent être classés selon le type de protection des informations qu'ils assurent.

Les types de protection des informations sont les suivants:

- 1) protection de la sémantique des données;
- 2) protection de la sémantique des données et des attributs associés;
- 3) protection de la sémantique des données, des attributs associés et de toute information susceptible d'être obtenue à partir des données en question.

En outre, on peut classer les services selon le type de menace qui existe dans l'environnement dans lequel ils fonctionnent et contre lequel les informations sont protégées. D'après ce critère, les services sont classés comme suit:

1) *Protection contre les menaces externes*

Ces services supposent que ceux qui ont un accès légitime aux informations ne les divulgueront pas à des parties non autorisées. Ils ne protègent pas les informations divulguées à des parties autorisées et n'imposent aucune contrainte à ces parties lorsqu'elles possèdent des informations précédemment protégées.

Exemple: des fichiers sensibles en A sont protégés par chiffrement. Toutefois, les processus qui possèdent les clés de déchiffrement requises peuvent lire les fichiers protégés et écrire ultérieurement sur des fichiers non protégés.

2) *Protection contre les menaces internes*

Ces services supposent que ceux qui sont autorisés à accéder à des informations et données critiques peuvent, volontairement ou non, exercer des activités qui compromettent éventuellement la confidentialité des informations à protéger.

Exemple: des étiquettes de sécurité et autorisations sont rattachées aux ressources qui sont protégées et aux entités qui peuvent y accéder. Les accès sont restreints selon un modèle de contrôle de flux bien défini et bien compris.

Les services qui protègent la confidentialité contre les menaces internes doivent interdire les voies occultes (voir l'Annexe D) ou limiter leur débit de transfert d'information à des niveaux acceptables. Ils doivent, en outre, empêcher toute déduction non autorisée qui pourrait être faite à partir de l'utilisation imprévue de voies d'information légitimes (telles que les déductions fondées sur des consultations soigneusement construites de bases de données – dont chacune est individuellement légitime – ou les déductions fondées sur l'aptitude/l'inaptitude d'un programme utilitaire de système à exécuter une commande).

5.3 Types de mécanismes de confidentialité

L'objectif des mécanismes de confidentialité est d'empêcher la divulgation non autorisée d'informations. A cet effet, un mécanisme de confidentialité peut:

1) empêcher l'accès aux données (par exemple, protection physique d'une voie).

On peut utiliser des mécanismes de contrôle d'accès (décrits dans la Rec. UIT-T X.812 | ISO/CEI 10181-3) pour permettre aux seules entités autorisées d'accéder aux données.

Les techniques de protection physique sortent du cadre de la présente Recommandation | Norme internationale. Elles sont néanmoins incluses dans d'autres normes telles que ISO 10202 (Architecture de sécurité des systèmes de transaction financière utilisant des cartes à circuit intégré) et ANSI X9.17/ISO 8734 (*Financial Institution Key Management – Wholesale*);

2) utiliser des techniques de mise en correspondance qui rendent les informations à protéger relativement inaccessibles sauf à ceux qui possèdent certaines informations critiques sur la technique de mise en correspondance. Ces techniques incluent:

- a) le chiffrement;
- b) le remplissage de données;
- c) l'étalement du spectre.

Des mécanismes de confidentialité de l'un ou l'autre type peuvent être utilisés conjointement avec d'autres mécanismes du même type ou d'un type différent.

Les mécanismes de confidentialité peuvent assurer différents types de protection:

- protection de la sémantique des données;
- protection des attributs des données (y compris l'existence des données);
- protection contre les déductions.

Des exemples de ces classes de mécanisme sont donnés ci-dessous:

- 1) chiffrement pour dissimuler des données;
- 2) chiffrement des données conjointement avec la segmentation et le remplissage pour dissimuler la longueur des unités PDU (voir 8.2);
- 3) techniques d'étalement du spectre pour dissimuler l'existence d'une voie de communication.

5.4 Menaces contre la confidentialité

Il existe une seule menace générique contre les informations protégées par la confidentialité, à savoir la divulgation des informations protégées. Plusieurs menaces existent à l'encontre des données protégées par la confidentialité, qui correspondent aux diverses façons dont les informations protégées par la confidentialité peuvent être déduites des données. On trouvera ci-après une description des menaces qui concernent les données protégées par la confidentialité dans différents environnements.

5.4.1 Menaces lorsque la confidentialité est assurée par des mesures visant à empêcher l'accès

Il s'agit notamment des menaces suivantes:

- 1) pénétration du mécanisme d'interdiction de l'accès, par exemple:
 - a) exploitation des faiblesses dans les voies physiquement protégées;
 - b) usurpation d'identité ou utilisation inadéquate de certificats;
 - c) exploitation des faiblesses dans la mise en œuvre du mécanisme de prévention (par exemple, un utilisateur peut demander l'accès à un fichier A, se voir accorder l'accès audit fichier et ensuite modifier le nom du fichier pour avoir accès à un autre fichier, B);
 - d) intégration de chevaux de Troie dans le logiciel de confiance;
- 2) pénétration des services dont dépend le mécanisme de prévention (par exemple, usurpation d'identité lorsque l'accès est fondé sur l'authentification de l'identité, utilisation impropre de certificats ou pénétration du mécanisme d'intégrité servant à protéger les certificats);
- 3) exploitation des programmes utilitaires du système qui peuvent divulguer, directement ou indirectement, des informations sur le système;
- 4) voies occultes.

5.4.2 Menaces lorsque la confidentialité est assurée par la dissimulation des informations

Il s'agit notamment des menaces suivantes:

- 1) pénétration du mécanisme cryptographique (que ce soit par une analyse cryptographique, par des clés détournées, par des attaques sous forme de texte en clair choisi ou par d'autres moyens);
- 2) analyse du trafic;
- 3) analyse des en-têtes d'unité PDU;
- 4) voies occultes.

5.5 Types d'attaques contre la confidentialité

A chacune des menaces énumérées ci-dessus correspondent une ou plusieurs attaques, c'est-à-dire des instanciations de la menace en question.

Il est possible de distinguer des attaques actives et des attaques passives, c'est-à-dire des attaques contre la confidentialité qui entraînent une modification du système et des attaques contre la confidentialité qui n'entraînent pas de modification du système.

NOTE – Le fait qu'une attaque soit passive ou active dépend aussi bien des caractéristiques du système que des actions entreprises par l'attaquant.

Exemples d'attaque passive:

- 1) lecture secrète des données et branchement clandestin;
- 2) analyse du trafic;
- 3) analyse des en-têtes d'unité PDU à des fins non légitimes;
- 4) copie de données d'unité PDU destinées à d'autres systèmes que ceux qui sont envisagés;
- 5) analyse cryptographique.

Exemples d'attaque active:

- 1) chevaux de Troie (code dont les caractéristiques non documentées facilitent les violations de la sécurité);
- 2) voies occultes;
- 3) pénétration des mécanismes qui assurent la confidentialité, telle que la pénétration du mécanisme d'authentification (par exemple, usurpation avec succès de l'identité d'une entité autorisée), la pénétration du mécanisme de contrôle d'accès et l'interception de clés;
- 4) invocations parasites de la fonctionnalité cryptographique, telles que les attaques sous forme de texte en clair choisi.

6 Politiques de confidentialité

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

Les données qui représentent des informations dont la confidentialité est protégée font l'objet d'un contrôle concernant les entités qui peuvent les lire. Une politique de confidentialité doit donc identifier les informations qui font l'objet de contrôles et indiquer quelles entités doivent normalement être autorisées à les lire.

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

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

6.1 Expression des politiques

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

Une politique de sécurité peut être considérée comme un ensemble de règles. Chacune de ces règles peut, dans une politique de confidentialité, associer une caractérisation des données et une caractérisation des entités. Dans certaines politiques, ces règles ne sont pas exprimées explicitement mais peuvent être déduites de la politique.

Un certain nombre de modes d'expression possibles des politiques de confidentialité sont décrits ci-après. Il convient de noter que, même si certains mécanismes de confidentialité 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 informations

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

- 1) en identifiant l'entité qui les crée;
- 2) en identifiant un groupe d'entités dont l'une quelconque des entités peut les lire;
- 3) par leur emplacement;
- 4) 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 qui entrent en jeu dans une règle de politique de confidentialité. Deux de ces manières généralement rencontrées consistent à identifier individuellement et sans ambiguïté les entités ou à associer des attributs à chaque entité. Ces deux formes de caractérisation des entités donnent lieu à deux types de politique, à savoir les politiques fondées sur l'identité et les politiques fondées sur des règles. Ces politiques sont examinées en détail dans le cadre du contrôle d'accès (voir la Rec. UIT-T X.812 | ISO/CEI 10181-3).

7 Informations et fonctions de confidentialité

7.1 Informations de confidentialité

Les opérations de **dissimulation** et de **révélation** sont examinées au 5.1.2. L'Annexe B montre, à l'aide de la Figure B.1, comment les données passent d'un environnement protégé par la confidentialité à un autre en utilisant ces opérations.

Avec certains mécanismes de confidentialités, les opérations de **dissimulation** et de **révélation** des données utilisent des informations auxiliaires. Ces informations auxiliaires sont appelées respectivement «informations de confidentialité **dissimulation**» (HCI) et «informations de confidentialité **révélation**» (RCI).

7.1.1 Informations de confidentialité «dissimulation»

Les informations de confidentialité «dissimulation», HCI, sont des informations utilisées par l'opération de **dissimulation**.

Citons, à titre d'exemple:

- 1) les clés publiques;
- 2) les clés symétriques;
- 3) l'emplacement où les données doivent être mises en mémoire;
- 4) les règles de segmentation.

7.1.2 Informations de confidentialité «révélation»

Les informations de confidentialité «révélation», RCI, sont des informations utilisées par l'opération de **révélation**.

Citons, à titre d'exemple:

- 1) les clés privées;
- 2) les clés symétriques;
- 3) l'emplacement où les données ont été mises en mémoire;
- 4) les règles de segmentation.

7.2 Fonctions de confidentialité

Un certain nombre de fonctions de confidentialité ont été identifiées; elles sont énumérées dans l'Annexe E. 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

7.2.1.1 Dissimulation

Cette fonction applique la protection par confidentialité aux données. Paramètres d'entrée possibles pour cette fonction:

- 1) données (éventuellement protégées par la confidentialité);
- 2) informations HCI;
- 3) identificateurs spécifiques à un mécanisme comme ceux qui sont mentionnés dans l'Annexe E.

Paramètres de sortie possibles:

- 1) données protégées par la confidentialité;
- 2) autres résultats de l'opération de **dissimulation** effectuée;
- 3) identificateur caractéristique de l'environnement protégé par la confidentialité dans lequel les données protégées par la confidentialité ont été placées.

7.2.1.2 Révélation

Cette fonction retire la protection qu'une opération de **dissimulation** antérieure avait conférée aux données. Paramètres d'entrée possibles pour cette fonction:

- 1) données protégées par la confidentialité;
- 2) informations RCI;
- 3) identificateurs spécifiques à un mécanisme comme ceux qui sont mentionnés dans l'Annexe E.

Paramètres de sortie possibles:

- 1) données (éventuellement protégées par la confidentialité);
- 2) autres résultats de l'opération de **révélation** effectuée;
- 3) identificateur caractéristique de l'environnement dans lequel les données obtenues ont été placées.

7.2.2 Fonctions relatives à la gestion

Les fonctions de gestion de la confidentialité permettent à un utilisateur d'obtenir, de modifier et de supprimer les informations HCI et RCI (telles que les clés) qui sont nécessaires pour assurer la confidentialité. 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.

8 Mécanismes de confidentialité

La confidentialité des données peut dépendre du support sur lequel les données résident ou transitent. En conséquence:

- 1) on peut assurer la confidentialité des données mises en mémoire en utilisant des mécanismes qui dissimulent la sémantique (tels que le chiffrement) ou qui fragmentent les données;
- 2) on peut assurer la confidentialité des données en transit en utilisant des mécanismes qui interdisent l'accès (tels que les voies protégées physiquement ou le contrôle de l'acheminement), des mécanismes qui dissimulent la sémantique des données (tels que le chiffrement) ou des mécanismes qui dispersent les données (tels que les sauts de fréquence).

On peut utiliser ces types de mécanisme isolément ou conjointement.

La classification ci-dessus montre qu'on peut grouper les mécanismes de confidentialité comme suit:

- 1) mécanismes qui empêchent l'accès non autorisé aux données;
- 2) mécanismes de chiffrement qui dissimulent les données tout en les laissant accessibles;
- 3) mécanismes contextuels qui rendent les données seulement en partie accessibles de telle sorte qu'elles ne puissent être entièrement recréées à partir d'un volume limité de données recueillies.

8.1 Mise en œuvre de la confidentialité par des mesures visant à empêcher l'accès

On peut assurer ce type de confidentialité par le contrôle d'accès, comme indiqué dans la Rec. UIT-T X.812 | ISO/CEI 10181-3, par la protection des supports physiques et par le contrôle de l'acheminement, comme indiqué ci-dessous.

8.1.1 Mise en œuvre de la confidentialité par la protection des supports physiques

On peut prendre des mesures physiques pour faire en sorte que les données sur un support ne puissent être inspectées que par l'utilisation d'un ensemble spécifique et limité de mécanismes. On assure la confidentialité des données en veillant à ce que seules les entités autorisées puissent se servir de ces mécanismes.

8.1.2 Mise en œuvre de la confidentialité par le contrôle de l'acheminement

Le but de ce mécanisme est d'empêcher la divulgation non autorisée des informations représentées par les éléments de données transférés. Le mécanisme assure la confidentialité en n'utilisant que des ressources fiables et sécurisées pour acheminer les données.

8.2 Mise en œuvre de la confidentialité par le chiffrement

Le but de ces mécanismes est d'empêcher la divulgation de la sémantique des données en transit ou mises en mémoire. Ces mécanismes peuvent être considérés comme fonctionnant entre deux ensembles d'entités:

- toute entité du premier ensemble peut détenir initialement les données (avec accès à la sémantique);
- toute entité du second ensemble est un destinataire autorisé des informations représentées par les données.

On distingue différentes classes de mécanisme de confidentialité indiquées ci-dessous:

- 1) mécanismes de confidentialité fondés sur le chiffrement symétrique dans lequel on utilise la même clé pour chiffrer (opération de **dissimulation**) et pour déchiffrer (opération de **révélation**) les données;
- 2) mécanismes de confidentialité fondés sur le chiffrement asymétrique dans lequel on utilise une clé publique pour chiffrer (opération de **dissimulation**) les données et la clé privée correspondante pour les déchiffrer (opération de **révélation**).

La principale distinction entre ces deux classes de mécanisme fondamentales est que, en 1), les mécanismes qui sont capables d'exécuter l'opération de **dissimulation** sont également capables d'exécuter l'opération de **révélation** et vice versa, tandis que, en 2), tous, ou presque tous les mécanismes peuvent exécuter l'opération de **dissimulation** tandis que seuls ceux qui ont accès à la clé privée peuvent effectuer l'opération de **révélation**.

8.2.1 Mise en œuvre de la confidentialité par le remplissage de données

Ce mécanisme a pour but d'empêcher la divulgation des informations représentées par la taille d'un élément de données. Il accroît la taille des éléments de données de telle sorte que la taille d'un élément de données avec remplissage n'ait que peu de rapport avec sa taille initiale. L'un des moyens permettant d'obtenir ce résultat consiste à ajouter des données aléatoires au début ou à la fin de l'élément de données de telle sorte que le remplissage soit reconnaissable comme tel par les entités autorisées mais ne puisse être distingué des données par les entités non autorisées. On peut, à cet effet, utiliser le remplissage de données en combinaison avec des transformations cryptographiques.

On peut utiliser ce mécanisme conjointement avec la segmentation des données au niveau de la couche réseau, comme indiqué dans la Rec. UIT-T X.273 | ISO/CEI 11577.

Le remplissage de données permet d'empêcher l'utilisation de la taille des données comme voie occulte.

8.2.2 Mise en œuvre de la confidentialité par des événements fictifs

Le but de ce mécanisme est d'empêcher toute déduction fondée sur la fréquence d'apparition d'un événement donné. On peut trouver une instance de ce mécanisme dans les protocoles de sécurité de la couche réseau qui visent à dissimuler le volume de trafic échangé sur des liaisons non fiables.

Ce mécanisme produit des pseudo-événements (par exemple, fausses unités PDU) que seules les parties autorisées peuvent identifier. On peut utiliser ce type de mécanisme pour répondre aux attaques par voie occulte qui mettent en œuvre la signalisation fondée sur les variations de la fréquence d'une activité.

NOTE – Le remplissage de données et le bourrage sont des exemples de ce mécanisme. Dans les deux cas, le mécanisme protège les attributs d'un objet en intégrant celui-ci dans un objet plus grand et en protégeant l'ensemble par des moyens cryptographiques.

8.2.3 Mise en œuvre de la confidentialité par la protection des en-têtes d'unité PDU

Le but de ce mécanisme est d'empêcher toute déduction fondée sur les en-têtes d'unité PDU au cours de la communication.

La dissimulation d'adresse, telle qu'elle est décrite dans la Rec. UIT-T X.273 | ISO/CEI 11577, est un exemple de ce mécanisme. Un système intermédiaire X peut recevoir une unité PDU, la chiffrer et l'intégrer dans une nouvelle unité PDU dont l'origine semble être X et dont la destination semble être Y, système homologue où les données sont déchiffrées et où l'unité PDU initiale est récupérée. L'en-tête initial (y compris les adresses) étant chiffré, aucune déduction fondée sur les informations d'en-tête n'est possible autre que celle qui est due au fait que X et Y échangent des unités PDU chiffrées.

Une autre instance de ce mécanisme est celle où, pour chaque unité PDU authentique envoyée par un système A, on crée n copies supplémentaires avec diverses adresses de destination et options d'en-tête (c'est-à-dire que le système crée un trafic de diffusion factice; ce mécanisme est aussi un exemple des mécanismes décrits au 8.2.2 ci-dessus).

La dissimulation d'adresse au niveau de la couche réseau est décrite dans la Rec. UIT-T X.273 | ISO/CEI 11577. Elle peut être effectuée dans d'autres couches (par exemple, la Rec. UIT-T X.411 | ISO/CEI 10021-4, intitulée systèmes de messagerie, décrit l'utilisation de la dissimulation d'adresse au niveau de la couche application).

Ce mécanisme applique des principes analogues à ceux qui sont exposés au 8.3.

8.2.4 Mise en œuvre de la confidentialité par des champs variant dans le temps

Ce mécanisme, utilisé conjointement avec le chiffrement, protège contre les déductions fondées sur les variations dynamiques des éléments de données. A cet effet, il combine les données à protéger avec des champs variant dans le temps de telle sorte que des attaquants ne puissent établir si les modifications de la représentation sont dues à des modifications des données ou à des modifications des champs variant dans le temps. En principe, ce mécanisme génère une représentation de données différente pour chaque observation potentielle significative des données protégées si bien que les déductions fondées sur l'absence d'une variation dynamique sont également rejetées. Exemple:

1) Transmission d'unité PDU

Un champ variant dans le temps est placé devant la partie protégée de chaque unité PDU; les données combinées qui en résultent sont ensuite chiffrées à l'aide d'un mécanisme cryptographique avec chaînage (c'est-à-dire que le champ qui varie affecte le chiffrement des données ultérieures).

2) *Stockage*

Ce cas se produit lorsque des champs variant dans le temps sont placés au début des fichiers stockés de façon à dissimuler les modifications (ou l'absence de celles-ci).

On peut utiliser ce mécanisme conjointement avec le remplissage de données et la segmentation de façon à dissimuler les variations de la taille des données protégées.

8.3 Mise en œuvre de la confidentialité par l'emplacement contextuel

On peut assurer une certaine forme de protection de la confidentialité consistant à empêcher l'accès aux données lorsque celles-ci sont situées dans un contexte quelconque parmi un grand nombre de contextes différents. S'il est impossible (pour des raisons informatiques ou physiques) d'examiner tous les contextes éventuels avant que le contexte utilisé ne soit modifié, on obtient un certain niveau de confidentialité.

Exemples de tels mécanismes:

- 1) la mise en œuvre d'un grand nombre de voies physiques ou virtuelles par lesquelles les informations sont transmises (par exemple, utilisation avec «étalement du spectre» d'une fréquence parmi un grand nombre de fréquences radioélectriques);
- 2) la mise en œuvre d'un grand nombre d'emplacements pour le stockage des données (par exemple, adresses sur un disque magnétique);
- 3) la transmission d'informations par le biais de voies de communications secondaires cachées qui sont dissimulées dans une voie de communication primaire (stéganographie).

Cette forme de confidentialité suppose que les destinataires non autorisés ne peuvent obtenir les informations qui permettent d'identifier le contexte correct à un instant donné. Ces informations doivent donc être elles-mêmes protégées par un service de confidentialité.

9 Interactions avec d'autres services et mécanismes de sécurité

Cet article indique comment on peut utiliser d'autres services et mécanismes de sécurité pour assurer la confidentialité. L'utilisation de la confidentialité pour assurer d'autres services de sécurité n'est pas décrite ici.

9.1 Contrôle d'accès

Le contrôle d'accès, tel qu'il est décrit dans la Rec. UIT-T X.812 | ISO/CEI 10181-3 peut servir à réglementer l'accès aux données.

Annexe A

Confidentialité dans le modèle de référence 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. X.800 du CCITT | ISO 7498-2. La présente annexe résume les aspects relatifs à la confidentialité.

Différents services de sécurité sont pris en considération:

- confidentialité en mode connexion;
- confidentialité en mode sans connexion;
- confidentialité sélective des champs;
- confidentialité du flux de trafic.

A.1 Confidentialité en mode connexion

La confidentialité en mode connexion assure la confidentialité de toutes les données d'utilisateur (N) sur une connexion (N).

A.2 Confidentialité en mode sans connexion

La confidentialité en mode sans connexion assure la confidentialité de champs sélectionnés dans les données d'utilisateur (N) dans une seule unité SDU (N) en mode sans connexion.

A.3 Confidentialité sélective des champs

La confidentialité sélective des champs assure la confidentialité de champs sélectionnés dans les données d'utilisateur (N) sur une connexion (N) ou dans une seule unité SDU en mode sans connexion (N).

A.4 Confidentialité du flux de trafic

La confidentialité du flux de trafic assure la protection des informations qui pourraient être déduites de l'observation des flux de trafic.

A.5 Utilisation de la confidentialité dans les couches OSI

Les services de confidentialité s'appliquent aux couches OSI suivantes:

- couche physique (couche 1);
- couche liaison de données (couche 2);
- couche réseau (couche 3);
- couche transport (couche 4);
- couche présentation (couche 6);
- couche application (couche 7).

A.5.1 Utilisation de la confidentialité au niveau de la couche physique

La confidentialité en mode connexion et la confidentialité du flux de trafic sont les seuls services de confidentialité assurés, isolément ou conjointement, au niveau de la couche physique. La confidentialité du flux de trafic revêt deux formes: la confidentialité totale du flux de trafic qui ne peut être assurée que sur certains types de transmission et la confidentialité limitée du flux de trafic qui peut toujours être assurée.

A.5.2 Utilisation de la confidentialité au niveau de la couche liaison de données

La confidentialité en mode connexion et la confidentialité en mode sans connexion sont les seuls services de sécurité assurés au niveau de la couche liaison de données. Ces services utilisent des mécanismes de chiffrement.

A.5.3 Utilisation de la confidentialité au niveau de la couche réseau

La confidentialité en mode connexion, la confidentialité en mode sans connexion et la confidentialité du flux de trafic sont les seuls services de sécurité assurés au niveau de la couche réseau. La confidentialité en mode connexion et la confidentialité en mode sans connexion peuvent être assurées par un mécanisme de chiffrement et/ou par le contrôle de l'acheminement. La confidentialité du flux de trafic peut être assurée par un mécanisme de remplissage de trafic conjointement avec un service de confidentialité au niveau ou au-dessous de la couche réseau et/ou avec le contrôle de l'acheminement. Ces services permettent d'assurer la confidentialité entre les nœuds de réseau, les nœuds de sous-réseau ou les relais.

A.5.4 Utilisation de la confidentialité au niveau de la couche transport

La confidentialité en mode connexion et la confidentialité en mode sans connexion sont les seuls services de confidentialité assurés au niveau de la couche transport. La confidentialité en mode connexion et la confidentialité en mode sans connexion peuvent être assurées par un mécanisme de chiffrement. Ces services permettent d'assurer la confidentialité entre les systèmes terminaux.

A.5.5 Utilisation de la confidentialité au niveau de la couche présentation

La confidentialité en mode connexion, la confidentialité en mode sans connexion et la confidentialité sélective des champs peuvent être assurées au niveau de la couche présentation. Dans le cas de la confidentialité sélective des champs, l'indication des champs qui doivent être protégés par la confidentialité est fournie par la couche application.

A.5.6 Utilisation de la confidentialité au niveau de la couche application

Tous les services de confidentialité, à savoir la confidentialité en mode connexion, la confidentialité en mode sans connexion, la confidentialité sélective des champs et la confidentialité du flux de trafic, peuvent être assurés au niveau de la couche application. La confidentialité en mode connexion et la confidentialité en mode sans connexion peuvent être prises en charge à l'aide d'un mécanisme de chiffrement de couche inférieure. La confidentialité sélective des champs peut être assurée par un mécanisme de chiffrement au niveau de la couche présentation. Un service de confidentialité limitée du trafic peut être assuré à l'aide d'un mécanisme de remplissage de trafic au niveau de la couche application conjointement avec un service de confidentialité au niveau d'une couche inférieure.

Annexe B

Exemple de séquence de passages par différents contextes
de protection de la confidentialité

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

La Figure B.1 est un exemple de séquence d'opérations de **dissimulation/révélation** qui préservent la confidentialité des données lorsque celles-ci passent d'un environnement initial A à un environnement E. Dans cet exemple, on suppose que les environnements A et E assurent la confidentialité par le contrôle d'accès tandis que l'environnement C protège la confidentialité par le chiffrement. Les environnements de chevauchement B (A et C) et D (C et E) protègent les données par le chiffrement ainsi que par le contrôle d'accès.

Le diagramme illustre les opérations suivantes:

- 1) opération de **dissimulation**, t, qui chiffre les données, les plaçant ainsi dans l'environnement de chevauchement B;
- 2) opération de **révélation**, u, qui transfère les données de B à C. Cette opération de **révélation** retire les données de l'environnement protégé par le contrôle d'accès mais n'affecte pas la protection de la confidentialité qui a été appliquée avec l'opération de **dissimulation** «t»;
- 3) opération de **dissimulation**, v, qui applique à nouveau la protection par le contrôle d'accès en transférant les données dans l'environnement de chevauchement D où les données sont protégées par le chiffrement et par le contrôle d'accès de E;
- 4) opération de **révélation**, w, qui déchiffre les données, les transférant ainsi de D à E.

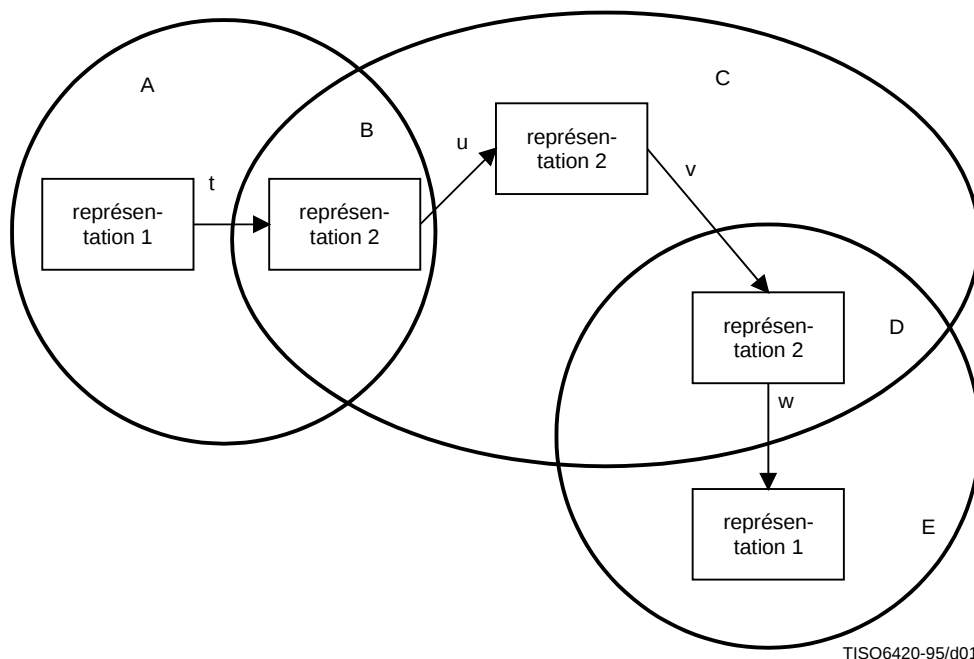


Figure B.1 – Illustration des régions protégées

Annexe C

Représentation des informations

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

On réalise la communication ou la mise en mémoire d'un élément d'information en utilisant une *représentation* de cet élément d'information (par exemple, le nombre dix-sept peut être codé sous la forme «17 décimal», «11 hexadécimal», «neuvième entier impair», «septième nombre premier» ou «289 (17*17)». On peut obtenir des informations à partir de la représentation ou des attributs de la représentation de cet élément d'information, c'est-à-dire comme indiqué ci-après:

- 1) en inspectant une valeur de données lorsqu'on connaît les conventions de représentation et les informations connexes;
- 2) en déterminant si un élément de données existe ou non;
- 3) par la taille d'un élément de données;
- 4) par les variations dynamiques des représentations.

Par exemple, on pourrait déduire l'information «le Roi est mort» comme suit:

- en inspectant une expression booléenne dont la valeur est vraie lorsque le roi est mort, fausse dans le cas contraire;
- en déterminant l'existence ou la non-existence d'un fichier appelé «Avis de décès du Roi» dans un répertoire de fichiers;
- en inspectant une liste de monarques décédés et en constatant que sa longueur s'est accrue;
- en établissant qu'un compteur, indiquant le nombre de jours où le pays a été sans monarque, change quotidiennement.

La mise en correspondance entre un élément d'information et une certaine représentation de cet élément d'information est définie par un ensemble de *règles de représentation*. Les règles de représentation indiquent:

- comment les informations sont codées sous forme de données;
- comment on peut faire en sorte que des données livrent les informations qui y sont codées;
- quelles modifications contextuelles explicites ou implicites il faut effectuer chaque fois que des informations sont codées (par exemple, la création d'un fichier peut entraîner des modifications de répertoire).

Les mécanismes de confidentialité traités par ce cadre de sécurité protègent un élément d'information:

- 1) en protégeant une représentation de l'élément d'information contre toute divulgation, c'est-à-dire en s'assurant qu'elle se trouve dans un *environnement* approprié; ou
- 2) en protégeant les règles de représentation contre toute divulgation.

On peut considérer que la force des environnements varie selon l'étendue de la protection contre toute divulgation assurée aux représentations placées dans ces environnements. On peut considérer également que la force des différents ensembles de règles de représentation varie selon la difficulté de la divulgation des règles de représentation à des entités non autorisées.

Le concept de *contexte de protection de la confidentialité* sert de base pour la description des différents types de mécanisme de confidentialité. Un contexte de protection de la confidentialité (pour tout élément d'information) est une représentation particulière de cet élément d'information existant dans un environnement particulier.

On comprend mieux le comportement des mécanismes de confidentialité lorsqu'on sait que le transfert d'informations implique potentiellement le passage par une séquence de différents contextes de protection de la confidentialité.

Un changement de représentation ou un changement d'environnement constitue un passage d'un contexte de protection de la confidentialité à un autre. Un changement de représentation se fera généralement vers une représentation plus forte (plus protectrice) ou vers une représentation plus faible (moins protectrice). De même, un changement d'environnement se fera généralement vers un environnement plus fort (plus protecteur) ou vers un environnement plus faible (moins protecteur).

L'Annexe B donne un exemple de passage par différents contextes de protection de la confidentialité.

Annexe D

Voies occultes

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

Le terme de voies occultes désigne des mécanismes qui ne sont pas conçus pour les communications et que l'on peut utiliser pour transférer de l'information par des moyens qui violent la politique de sécurité.

Les attaques par voie occulte sont des attaques effectuées à l'intérieur d'un système par l'émetteur de certaines données. Pour de telles tentatives, l'attaquant n'est pas contraint d'utiliser des moyens particuliers de transfert des informations tels que ceux qui sont, en général, prévus spécialement à cet effet. Dans un environnement suffisamment complexe, il existe généralement un ou plusieurs moyens de transfert des informations en dehors des mécanismes prévus pour communiquer les données ainsi que pour les stocker et les extraire. Ces moyens sont appelés «voies occultes».

De nombreuses voies occultes impliquent la modulation autorisée d'états ou d'événements qui est visible pour des entités non autorisées à recevoir des informations en provenance de la source de cette modulation. Les informations sont transférées dans le cadre d'une entente commune, entre la source et le destinataire, sur la signification à attribuer à cette modulation.

Parmi les exemples de voie, dans les mécanismes de communication de données, on peut citer l'attribution d'une signification:

- aux différentes tailles disponibles d'unités PDU (N);
- aux différentes adresses de destination pouvant être reçues ou interceptées par le destinataire de la voie occulte sur les connexions (N) ou les transmissions en mode sans connexion (N);
- aux différentes durées disponibles entre la transmission d'unités PDU (N) sur la même connexion (N) ou à partir de la même entité (N).

Le dernier exemple est celui d'une voie occulte à base de temps.

Parmi les exemples de voie, dans les mécanismes de stockage et d'extraction des données, on peut citer l'attribution d'une signification:

- au nom donné à une zone de mise en mémoire;
- à la présence ou à l'absence de données stockées spécifiquement dénommées;
- au volume de données stockées;
- à la capacité d'accepter de nouvelles données à stocker;
- à la durée pendant laquelle des données spécifiquement dénommées sont (ou non) mises en mémoire.

Les voies où, comme dans le premier de ces exemples, les données (un nom) peuvent être stockées, puis extraites, sont appelées «voies occultes de stockage».

On peut spécifier et modéliser les ressources de système et les protocoles de communication sous la forme d'objets abstraits pour obtenir un certain nombre d'opérations primitives spécifiques. A titre d'exemple, on peut donc citer, plus généralement, l'attribution d'une signification:

- au choix d'une opération parmi celles qui sont disponibles;
- à l'ordre dans lequel les primitives de service sont utilisées;
- à la durée entre les utilisations d'une opération, lorsque ces utilisations sont potentiellement visibles pour le destinataire de la voie occulte.

La confidentialité des données ne peut être garantie que lorsque tous les moyens de transfert de l'information (y compris les voies occultes) sont identifiés et que chacun d'eux est contrôlé par l'utilisation d'un mécanisme de confidentialité approprié à ce moyen.

Dans bien des cas, l'interdiction complète des voies occultes n'est pas réalisable (pour des raisons d'ordre technique, organisationnel, économique ou autres). Il est cependant possible de réduire, à des niveaux jugés acceptables, la vitesse à laquelle l'information peut être acheminée par ces voies.

Annexe E

Description générale des fonctions de confidentialité

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

Description générale des fonctions de sécurité			Elément	Entité: initiateur, vérificateur, confidentialité-TTP		
				Fonction:		
			But du service	Objet d'information: données protégées par la confidentialité		
A C T I V I T É		Entité	Autorité de domaine de sécurité (SDA)			
		Fonction				
	Activité relative à la gestion	– Installation des informations de gestion		– Listage des informations de gestion		
		– Modification des informations de gestion		– Désactivation des informations de gestion		
		– Suppression des informations de gestion		– Réactivation des informations de gestion		
		Entité	Initiateur		Vérificateur	Confidentialité-TTP
		Fonction				
	Activité relative à l'exploitation	– Dissimulation des données		– Révélation des données		– Certificat d'entité
		– Etiquette de sécurité		– Etiquette de sécurité		
	I N F O R M A T I O N	Elément de données entrée/sortie géré par la SDA		– Clés publiques – Clés symétriques – Etiquette de sécurité		
Type d'information utilisé dans l'opération		– Information de confidentialité «dissimulation» (HCI) – Information de confidentialité «révélation» (RCI)				
Informations de contrôle		– Type de mécanisme protégé par la confidentialité – Niveau de protection par la confidentialité				

La présente annexe utilise les concepts suivants.

E.1 Entités de confidentialité

La confidentialité dans les systèmes ouverts implique l'intervention des entités suivantes:

E.1.1 Initiateur

Entité qui génère des données protégées par la confidentialité en vue de leur transmission ou de leur mise en mémoire.

E.1.2 Vérificateur

Entité qui extrait des informations à partir des données protégées par la confidentialité.

E.1.3 Tierce partie de confiance (TTP) pour les fonctions de confidentialité

Entité qui distribue des informations de confidentialité «dissimulation» ou «révélation» aux entités échangeant des données protégées par la confidentialité.