



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1121

(04/2004)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION
ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des télécommunications

**Cadre général des technologies de la sécurité
pour les communications mobiles de données
de bout en bout**

Recommandation UIT-T X.1121

RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	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
Définitions 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 des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.379
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DES TÉLÉCOMMUNICATIONS	X.1000–

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1121

Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout

Résumé

La présente Recommandation décrit les problèmes de sécurité observés dans le domaine des communications mobiles de données de bout en bout, ainsi que les besoins de sécurité considérés du point de vue de l'utilisateur du service mobile et du fournisseur de services d'application (ASP, *application service provider*). Par ailleurs, la présente Recommandation indique le niveau d'intervention, dans les modèles de communications de données de bout en bout, des techniques de sécurité qui assurent certaines fonctions de sécurité.

Source

La Recommandation UIT-T X.1121 a été approuvée le 29 avril 2004 par la Commission d'études 17 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies 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.

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.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2005

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1 Domaine d'application	1
2 Références normatives.....	1
3 Définitions	1
3.1 Architecture de sécurité du modèle de référence OSI	1
3.2 Définitions additionnelles.....	2
4 Abréviations.....	3
5 Aperçu général.....	3
6 Modèles de communication de données mobiles de bout en bout	3
6.1 Modèle général de communication de données mobiles de bout en bout entre un utilisateur mobile et un ASP	4
6.2 Modèle passerelle de communication mobile de bout en bout entre utilisateur mobile et ASP	4
7 Caractéristiques des communications de données mobiles de bout en bout	5
8 Menaces sur la sécurité dans un environnement mobile	5
8.1 Menaces sur la sécurité d'ordre général.....	5
8.2 Menaces sur la sécurité spécifiques du contexte mobile	6
8.3 Relation entre les menaces sur la sécurité et les modèles de communication de bout en bout	7
9 Prescriptions de sécurité pour les communications de données mobiles de bout en bout	8
9.1 Prescriptions de sécurité du point de vue de l'utilisateur mobile.....	8
9.2 Prescriptions de sécurité du point de vue du fournisseur de services d'application.....	12
9.3 Relations entre les prescriptions de sécurité et les menaces sur la sécurité ...	15
10 Fonctions de sécurité permettant de répondre aux prescriptions de sécurité concernant spécifiquement les communications mobiles.....	16
11 Technologies de sécurité applicables aux communications de données mobiles de bout en bout	19

Recommandation UIT-T X.1121

Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout

1 Domaine d'application

La présente Recommandation définit les prescriptions de sécurité, du point de vue de l'utilisateur mobile et du fournisseur de services d'application de couche supérieure du modèle de référence OSI, applicables aux communications mobiles de données de bout en bout entre un terminal mobile de réseau mobile et un serveur d'application de réseau ouvert.

La présente Recommandation définit un cadre général de technologies de sécurité pour les communications mobiles de données de bout en bout.

La présente Recommandation ne spécifie pas de façon détaillée les éléments du réseau mobile, à l'exception de l'accès, par l'intermédiaire d'un réseau hertzien, à un terminal mobile connecté à un réseau ouvert.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut d'une Recommandation.

La référence à un document figurant dans cette Recommandation ne donne pas à ce document en tant que tel le statut d'une Recommandation.

- Recommandation UIT-T Q.1701 (1999), *Cadre général des réseaux IMT-2000*.
- Recommandation UIT-T Q.1711 (1999), *Modèle fonctionnel de réseau pour les IMT-2000*.
- Recommandation UIT-T Q.1761 (2004), *Convergence des systèmes fixes et des systèmes IMT-2000: principes et prescriptions*.
- Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.
- Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures*.
- 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*.

3 Définitions

3.1 Architecture de sécurité du modèle de référence OSI

Les termes et expressions suivants sont définis dans la Rec. UIT-T X.800:

- a) contrôle d'accès;
- b) authentification;

- c) information d'authentification;
- d) échange d'authentification;
- e) autorisation;
- f) disponibilité;
- g) confidentialité;
- h) cryptographie;
- i) intégrité des données;
- j) authentification de l'origine des données;
- k) chiffrement;
- l) intégrité;
- m) clé;
- n) échange de clés;
- o) gestion de clés;
- p) non-répudiation;
- q) notarisation;
- r) mot de passe;
- s) respect de la vie privée.

3.2 Définitions additionnelles

La présente Recommandation définit les termes et expressions suivants:

3.2.1 anonymat: l'accès aux services est anonyme lorsqu'il n'est pas possible d'avoir accès aux données personnelles concernant l'utilisateur et son comportement – lieu de l'utilisateur, fréquence d'utilisation du service, etc.

3.2.2 lecture par-dessus l'épaule: obtention illicite d'informations dans un lieu fréquenté, par observation du mouvement du clavier, lecture indiscreète sur l'écran du mobile ou écoute du signal sonore émis par le terminal.

3.2.3 terminal mobile: entité dotée d'une fonction d'accès hertzien et qui peut être connecté à un réseau mobile pour des communications de données avec des serveurs d'application ou d'autres terminaux mobiles.

3.2.4 réseau mobile: réseau fournissant des points d'accès hertzien à des terminaux mobiles.

3.2.5 utilisateur mobile: entité (personne) utilisant et exploitant un terminal mobile pour la réception de divers services assurés par des fournisseurs de services d'application.

3.2.6 service d'application: service mobile de type télébanque, commerce en ligne, etc.

3.2.7 serveur d'application: entité connectée à un réseau ouvert pour la transmission de données à des terminaux mobiles.

3.2.8 fournisseur de services d'application (ASP, *application service provider*): entité (personne ou groupe) fournissant des services d'application aux utilisateurs mobiles par l'intermédiaire d'un serveur d'application.

3.2.9 passerelle de sécurité mobile: entité relayant les données transmises entre un terminal mobile et un serveur d'application, qui peut modifier les paramètres de sécurité ou le protocole de communication entre un réseau mobile et un réseau ouvert ou inversement, et qui est capable d'assurer diverses fonctions de gestion de la politique de sécurité pour les communications mobiles de données de bout en bout.

3.2.10 gestion de la politique de sécurité: fonction de gestion ou de négociation d'un ensemble de règles pour la fourniture de services de sécurité classés pouvant être implémenté au niveau de la passerelle de sécurité mobile ou d'un autre serveur.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

ASP	fournisseur de services d'application (<i>application service provider</i>)
DoS	déni de service (<i>denial of service</i>)
IMT-2000	télécommunications mobiles internationales 2000 (<i>international mobile telecommunications 2000</i>)
LAN	réseau local (<i>local area network</i>)
OSI	interconnexion des systèmes ouverts (<i>open systems interconnection</i>)
PDA	assistant personnel électronique (<i>personal data assistant</i>)
PIN	numéro d'identification personnel (<i>personal identification number</i>)

5 Aperçu général

Les terminaux mobiles dotés de capacités de communication de données (téléphone mobile IMT-2000, ordinateur personnel portable ou PDA avec carte radio) sont largement diffusés, et l'on dispose de divers services d'application (par exemple commerce mobile) pour ces terminaux dans le réseau mobile. S'agissant de commerce électronique, la sécurité est nécessaire et indispensable.

Du point de vue de l'opérateur mobile, plusieurs questions se posent (par exemple, architecture de sécurité des réseaux téléphoniques mobiles de type IMT-2000). Toutefois, il importe également de s'intéresser au point de vue de l'utilisateur mobile et à celui du fournisseur de services d'application.

En ce qui concerne la sécurité des communications mobiles du point de vue de l'utilisateur mobile ou du fournisseur de services d'application, l'un des plus importants aspects est celui de la sécurité de données transmises de bout en bout entre un terminal mobile et un serveur d'application.

En outre, pour ce qui est du système mobile connectant un réseau mobile à un réseau ouvert, il est nécessaire de considérer la sécurité des couches supérieures (couches Application, Présentation et Session) du modèle de référence OSI, du fait qu'il existe un grand nombre d'applications de réseau mobile (par exemple, réseau téléphonique mobile IMT-2000, réseau local hertzien, Bluetooth) ou de réseau ouvert.

La présente Recommandation décrit les problèmes de sécurité qui se posent dans le contexte des communications de données de bout en bout, ainsi que les besoins de sécurité du point de vue de l'utilisateur mobile et du fournisseur de services d'application. Par ailleurs, elle indique les points d'intervention, dans les modèles de communication de données mobiles de bout en bout, des techniques de sécurité qui entrent en jeu dans certaines fonctions de sécurité.

6 Modèles de communication de données mobiles de bout en bout

Avant de décrire les technologies de la sécurisation des communications mobiles, il faut définir des modèles de communication de données mobiles de bout en bout. De tels modèles permettent de clarifier la relation entre les diverses entités et les points auxquels il convient d'adapter les technologies de sécurisation relevant du contexte mobile.

6.1 Modèle général de communication de données mobiles de bout en bout entre un utilisateur mobile et un ASP

La Figure 1 illustre le modèle général de la communication de données mobiles de bout en bout entre un utilisateur mobile et un ASP.

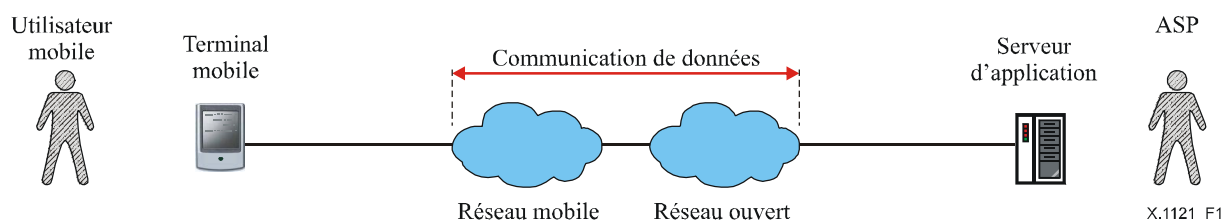


Figure 1/X.1121 – Modèle général de communication de données mobiles de bout en bout entre un utilisateur mobile et un ASP

Ce modèle comprend six éléments: utilisateur mobile, terminal mobile, réseau mobile, réseau ouvert, serveur d'application et ASP.

Par ailleurs, on observe cinq relations dans ce modèle respectivement entre utilisateur mobile et terminal mobile, terminal mobile et réseau mobile, réseau mobile et réseau ouvert, réseau ouvert et serveur d'application, enfin terminal mobile et serveur d'application.

6.2 Modèle passerelle de communication mobile de bout en bout entre utilisateur mobile et ASP

La Figure 2 illustre un autre modèle (le modèle passerelle) de communication de données mobiles de bout en bout, entre un utilisateur mobile et un ASP.

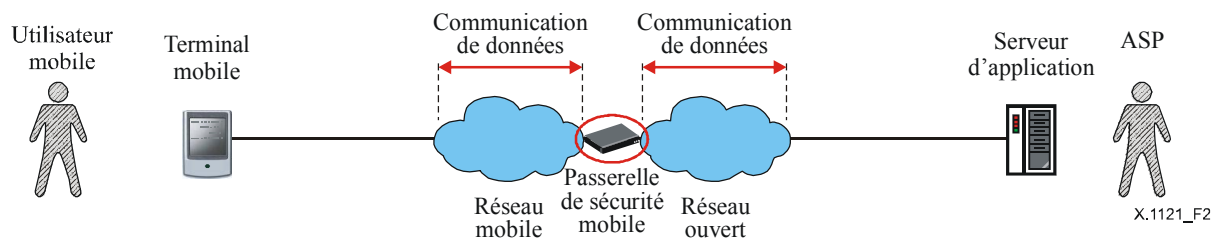


Figure 2/X.1121 – Modèle passerelle de communication de données mobiles de bout en bout entre un utilisateur mobile et un ASP

Ce modèle comprend sept éléments distincts: utilisateur mobile, terminal mobile, réseau mobile, réseau ouvert, serveur d'application, ASP et passerelle de sécurité mobile.

Par ailleurs, on observe sept relations dans ce modèle, respectivement entre l'utilisateur mobile et le terminal mobile, le terminal mobile et le réseau mobile, le réseau mobile et la passerelle de sécurité mobile, la passerelle de sécurité mobile et le réseau ouvert, le réseau ouvert et le serveur d'application, le terminal mobile et la passerelle de sécurité mobile, et enfin la passerelle de sécurité mobile et le serveur d'application.

7 Caractéristiques des communications de données mobiles de bout en bout

Les communications de données mobiles de bout en bout, présentent diverses caractéristiques qui les distinguent des communications de données générales de bout en bout dans un réseau ouvert. Les caractéristiques sont les suivantes:

les communications mobiles reposent sur des communications hertziennes

Les communications mobiles de données de bout en bout se faisant par voie hertzienne, sont plus instables que des communications de données de bout en bout par des moyens filaires sur un réseau ouvert.

En outre, cette instabilité est rendue encore plus grande par le fait que l'utilisateur mobile peut par définition se déplacer pendant la communication de données mobiles de bout en bout.

Les communications hertziennes peuvent être assurées par diffusion entre le terminal et le réseau mobile;

les terminaux mobiles sont généralement peu encombrants

D'une manière générale, les terminaux mobiles utilisés pour les communications de données mobiles de bout en bout sont plus petits que les équipements que l'on utilise habituellement pour la communication de données de bout en bout dans un réseau ouvert (par exemple, ordinateur de bureau). En conséquence,

- la saisie ou l'extraction des données sont difficiles;
il est difficile de saisir des données au clavier et de visualiser un grand nombre de données simultanément du fait que l'écran est de dimensions réduites (tout particulièrement dans le cas des petits terminaux portatifs);
- les processeurs sont moins performants que ceux des ordinateurs de bureau;
- la capacité correspondante, pour les applications, est donc limitée (taille mémoire, alimentation électrique, etc.);

les terminaux mobiles sont utilisés par des usagers mobiles

8 Menaces sur la sécurité dans un environnement mobile

On distingue deux catégories de menaces sur la sécurité, tout d'abord les risques généraux, que l'on peut retrouver dans tout réseau ouvert, et en second lieu les risques spécifiques qui tiennent aux caractéristiques de l'environnement mobile.

8.1 Menaces sur la sécurité d'ordre général

Les communications de données mobiles de bout en bout étant avant tout des communications de données de bout en bout, on observe en la matière les mêmes menaces sur la sécurité que dans les réseaux ouverts.

8.1.1 Ecoute de conversation

Le principal problème qui se pose dans le contexte des réseaux ouverts est celui des écoutes de conversation effectuées subrepticement: une personne peut sans se faire remarquer intercepter les données transmises (fuite de données).

8.1.2 Brouillage des communications

Il y a brouillage d'une communication lorsqu'un signal brouilleur émis de façon intentionnelle ou non intentionnelle perturbe la liaison de communication à l'émission ou à la réception, ce qui rend la liaison inefficace. La conséquence peut en être un déni de service.

8.1.3 Adjonction et modification de données

Des données peuvent être ajoutées, modifiées ou supprimées, pendant leur transmission entre le terminal mobile et le serveur d'application, par une entité non autorisée (personne, programme, ordinateur). Par exemple, des données peuvent être injectées sur une liaison à des fins de détournement de la connexion ou de manipulation malveillante (il y a alors déni de service ou intrusion de tierce partie).

8.1.4 Interruption

On parle d'interruption en cas de destruction d'un composant de terminal mobile ou d'élément de réseau. Exemple: destruction d'un élément matériel, disque dur, etc.; coupure de ligne de communication; mise hors d'usage du système de gestion des fichiers d'un terminal mobile ou d'un élément de réseau dans l'infrastructure du réseau mobile.

8.1.5 Accès non autorisé

On entend par contrôle d'accès la capacité à limiter et à contrôler l'accès à un serveur d'application par l'intermédiaire d'une liaison de communication. Il y a menace lorsqu'une entité non autorisée réussit à accéder à un serveur d'application en se faisant passer pour un utilisateur mobile réel. Il est nécessaire d'identifier, ou d'authentifier, l'entité qui cherche à obtenir l'accès.

8.1.6 Répudiations

Il y a répudiation lorsque l'expéditeur ou le destinataire, selon le cas, ne reconnaît pas avoir expédié ou reçu le message.

8.2 Menaces sur la sécurité spécifiques du contexte mobile

Diverses menaces sur la sécurité découlent spécifiquement des caractéristiques des communications mobiles, dans le cas de communications hertziennes et de radiodiffusion de données entre un terminal mobile et un réseau mobile. Le principal problème que pose un réseau hertzien réside dans sa sensibilité aux attaques anonymes.

Les menaces sur la sécurité spécifiques du contexte mobile sont énumérées ci-après.

8.2.1 Ecoute de conversation

L'écoute de conversation est plus facile dans le cas de communications mobiles, car il suffit d'intercepter le signal radioélectrique et de décoder les données transmises (fuite de données).

8.2.2 Brouillage de communication

Ici encore, le brouillage de données est plus facile dans le cas d'une liaison entre un terminal mobile et un réseau mobile. On distingue deux types d'attaques de ce type, d'une part le brouillage qui vise le terminal mobile et d'autre part le brouillage qui vise un élément de réseau. Dans le premier cas, on "fait passer" le terminal mobile agresseur pour le terminal mobile agréé, et dans le second cas, on usurpe l'identité de l'élément de réseau homologué qui assure la connexion avec le terminal mobile par l'intermédiaire de l'interface radioélectrique.

8.2.3 Lecture par-dessus l'épaule

Vol d'informations par observation attentive du clavier ou de l'écran du terminal mobile de l'utilisateur légitime, ou encore écoute subreptice des informations auditives, dans un endroit fréquenté.

8.2.4 Perte de terminal mobile

La sécurité peut également être menacée en cas de perte du terminal mobile par l'utilisateur en déplacement (perte ou destruction de l'information mémorisée dans le terminal mobile).

8.2.5 Vol de terminal mobile

Pendant que l'utilisateur mobile se déplace, son terminal mobile peut également être volé, ce qui peut poser divers problèmes: perte des informations mémorisées dans le terminal mobile, suppression de données consécutives à l'accès non autorisé au terminal volé.

8.2.6 Interruption imprévue de la communication

La communication risque d'être interrompue lorsque la liaison n'est pas stable ou lorsque l'alimentation électrique cesse d'être rassurée (risque d'effacement de données).

8.2.7 Erreur de lecture

Le risque de confusion ou d'erreur à la lecture est particulièrement important, compte tenu des dimensions réduites des terminaux mobiles, et la pratique illicite de l'usurpation ("masquerading") de l'identité du fournisseur de services d'application peut entraîner des vols de données.

8.2.8 Erreur de saisie

La saisie pose un problème de sécurité du fait qu'il est difficile d'entrer des données sur le clavier ou le pavé numérique de dimensions très réduites d'un terminal mobile. Il peut en résulter par exemple un refus d'authentification de l'utilisateur.

8.3 Relation entre les menaces sur la sécurité et les modèles de communication de bout en bout

Les menaces sur la sécurité interviennent en différents points précis des modèles. Les Tableaux 1 et 2 font apparaître la relation entre les menaces et les entités fonctionnelles des modèles.

Ces tableaux font apparaître que les menaces sur la sécurité qui se posent sont les mêmes au niveau du serveur d'application qu'au niveau de la passerelle de sécurité mobile. Ils montrent également que l'on peut observer les mêmes menaces sur la sécurité dans la relation entre le terminal mobile et le serveur d'application, entre le terminal mobile et la passerelle de sécurité mobile et enfin entre le serveur d'application et la passerelle de sécurité mobile.

Tableau 1/X.1121 – Relations entre les menaces générales sur la sécurité et les modèles

Entités, relations	Menaces	Ecoute de conversation	Brouillage de communication	Adjonction/ Modification	Interruption	Accès non autorisé	Répudiation
Terminal mobile					X	X	
Serveur d'application			X		X	X	
Relation entre l'utilisateur mobile et le terminal mobile							
Relation entre le terminal mobile et le serveur d'application		X	X	X	X		X
Passerelle de sécurité mobile					X	X	
Relation entre le terminal mobile et la passerelle de sécurité mobile		X	X	X	X		X
Relation entre le serveur d'application et la passerelle de sécurité mobile		X	X	X	X		X

**Tableau 2/X.1121 – Relations entre les menaces sur la sécurité
"spécifiquement mobiles" et les modèles**

Entités, relations	Menaces	Ecoute de conversation	Brouillage de communication	Lecture par-dessus l'épaule	Perte ou vol de terminal	Interruption imprévue	Erreur de lecture/ erreur de saisie
Terminal mobile			X		X		
Serveur d'application							
Relation entre l'utilisateur mobile et le terminal mobile				X			X
Relation entre le terminal mobile et le serveur d'application	X	X				X	
Passerelle de sécurité mobile			X				
Relation entre le terminal mobile et la passerelle de sécurité mobile	X	X				X	
Relation entre le serveur d'application et la passerelle de sécurité mobile	X	X				X	

9 Prescriptions de sécurité pour les communications de données mobiles de bout en bout

On distingue deux types de prescriptions de sécurité pour les communications de données mobiles de bout en bout, selon que l'on considère le point de vue de l'utilisateur mobile ou le point de vue du fournisseur de services d'application.

9.1 Prescriptions de sécurité du point de vue de l'utilisateur mobile

Au niveau des applications, les attentes et les besoins de l'utilisateur sont très divers. Mais la plupart des utilisateurs d'application mobile attendent tout simplement de l'application qu'elle fonctionne et qu'elle soit conviviale. Dans la plupart des cas, on attend également des applications et des fournisseurs de services un traitement sécurisé et confidentiel des données personnelles. En conséquence, l'utilisateur mobile fixe certaines conditions de sécurité dans les domaines suivants:

- gestion de l'identité;
- confidentialité des données;
- intégrité des données;
- authentification;
- contrôle d'accès;
- non-répudiation;
- anonymat;
- protection de la sphère privée;
- facilité d'utilisation;
- disponibilité.

9.1.1 Gestion de l'identité

La gestion de l'identité concerne essentiellement la protection des données relatives à l'identité de l'utilisateur. Il s'agit donc d'un élément très important de la sphère privée. Des pseudonymes peuvent être utilisés dans les communications. En ce qui concerne le service mobile, l'essentiel est de générer (ou de faire générer), d'actualiser, de supprimer (ou de faire supprimer) et d'appliquer des clés conformément à la politique de sécurité de l'utilisateur mobile.

9.1.2 Confidentialité des données

Les prescriptions de confidentialité des données, pour l'utilisateur mobile, couvrent les éléments suivants:

Confidentialité des données transmises entre un terminal mobile et un serveur d'application

Confidentialité de la totalité des données, ou de certaines données, transmises entre un terminal mobile et un serveur d'application.

Confidentialité des données mémorisées dans un terminal mobile

Confidentialité de la totalité des données, ou de certaines données, mémorisées dans un terminal mobile.

Confidentialité des données mémorisées dans un serveur d'application

Confidentialité de la totalité des données, ou de certaines données, associées à l'utilisateur mobile, mémorisées dans un serveur d'application.

Dans le "modèle passerelle", les critères de confidentialité des données de l'utilisateur mobile couvrent également:

Confidentialité des données transmises entre un terminal mobile et une passerelle de sécurité mobile

Confidentialité de la totalité des données, ou de certaines données, transmises entre un terminal mobile et une passerelle de sécurité mobile.

Confidentialité des données transmises entre un serveur d'application et une passerelle de sécurité mobile

Confidentialité de la totalité des données, ou de certaines données, échangées entre un serveur d'application et une passerelle de sécurité mobile.

Confidentialité des données mémorisées dans une passerelle de sécurité mobile

Confidentialité de la totalité des données, ou de certaines données, mémorisées dans une passerelle de sécurité mobile.

9.1.3 Intégrité des données

Les prescriptions d'intégrité des données, pour l'utilisateur mobile, couvrent les éléments suivants:

Intégrité des données transmises entre un terminal mobile et un serveur d'application

Intégrité de toutes les données communiquées entre un terminal mobile et un serveur d'application.

Intégrité des données mémorisées dans un terminal mobile

Intégrité de toutes les données mémorisées dans un terminal mobile.

Intégrité des données mémorisées dans un serveur d'application

Intégrité de toutes les données mémorisées dans un serveur d'application et qui concernent l'utilisateur mobile (par exemple, données personnelles relatives à l'utilisateur mobile).

Dans le "modèle passerelle", les prescriptions d'intégrité applicables aux données de l'utilisateur mobile couvrent également:

Intrégrité des données transmises entre un terminal mobile et une passerelle de sécurité mobile

Assure l'intégrité de toutes les données transmises entre un terminal mobile et une passerelle de sécurité mobile.

Intrégrité des données transmises entre un serveur d'application et une passerelle de sécurité mobile

Assure l'intégrité de toutes les données transmises entre un serveur d'application et une passerelle de sécurité mobile.

Intrégrité des données mémorisées par la passerelle de sécurité mobile

Assure l'intégrité de toutes les données mémorisées par une passerelle de sécurité mobile associée à l'utilisateur mobile.

9.1.4 Authentification

On distingue deux types d'authentification: l'authentification de l'entité et l'authentification du message. Dans le premier cas, l'entité prouve son identité à l'entité homologue. Dans le cas de l'authentification du message, il s'agit de prouver l'origine des données ou la réception des données. Les prescriptions d'authentification de l'utilisateur mobile couvrent les éléments suivants:

Authentification du fournisseur de services d'application

Type d'authentification d'entité confirmant l'identité d'un ASP et établissant ainsi qu'il n'y a ni usurpation d'identité ni répétition non autorisée d'une connexion précédente.

Authentification de l'utilisateur mobile

Type d'authentification d'entité établissant l'identité de l'utilisateur d'un terminal mobile par activation de divers dispositifs d'authentification de l'utilisateur: empreinte digitale, mot de passe, PIN, et garantissant ainsi la protection contre tout accès non autorisé à partir d'un terminal mobile perdu ou volé.

Authentification des données reçues

Type d'authentification de message confirmant la source des données communiquées. Cet élément n'implique pas la présence d'une protection contre la duplication ou la modification des données.

9.1.5 Contrôle d'accès

Les prescriptions de contrôle d'accès de l'utilisateur mobile couvrent les éléments suivants:

Contrôle d'accès au terminal mobile

Confère une protection contre l'accès non autorisé à un terminal mobile ou l'utilisation non autorisée d'un terminal mobile.

Le contrôle d'accès doit être conforme aux politiques de sécurité de l'utilisateur mobile.

Contrôle d'accès du serveur d'application

Protection contre l'accès non autorisé d'un serveur d'application aux données émises par un utilisateur mobile (par exemple, données personnelles concernant l'utilisateur mobile).

Le contrôle d'accès doit être conforme aux politiques de sécurité de l'utilisateur mobile.

Dans le "modèle passerelle", les prescriptions de protection du contrôle d'accès de l'utilisateur mobile couvrent également:

Contrôle d'accès au niveau d'une passerelle de sécurité mobile

Protection, au niveau d'une passerelle de sécurité mobile, contre tout accès non autorisé aux données émises par un utilisateur mobile (par exemple, informations personnelles concernant l'utilisateur mobile).

Le contrôle d'accès doit être conforme aux politiques de sécurité de l'utilisateur mobile.

9.1.6 Non-répudiation

Il existe deux variantes de cet élément:

Non-répudiation avec preuve d'origine

Prouve que les données reçues ont pour origine un ASP donné. Cet élément est nécessaire pour la protection contre toute tentative, de la part de l'ASP, de répudiation abusive de l'expédition des données.

Non-répudiation avec preuve de remise

Prouve que les données ont été remises à un ASP. Cet élément est nécessaire pour assurer la protection contre toute tentative ultérieure, de la part de l'ASP, de répudiation abusive de la réception des données.

Les prescriptions de non-répudiation sont associées aux prescriptions suivantes: confidentialité de communications des données entre un terminal mobile et le serveur d'application, intégrité des données transmises entre un terminal et un serveur d'application, intégrité des données mémorisées dans un terminal mobile, authentification d'utilisateur mobile et contrôle d'accès au terminal mobile.

Le "modèle passerelle" est associé aux prescriptions suivantes: confidentialité des données transmises entre un terminal et une passerelle de sécurité mobile, confidentialité des données transmises entre une passerelle de sécurité mobile et un serveur d'application, intégrité des données transmises entre un terminal mobile et une passerelle de sécurité mobile, intégrité des données transmises entre une passerelle de sécurité mobile et un serveur d'application, intégrité des données mémorisées au niveau d'une passerelle de sécurité mobile.

9.1.7 Anonymat

Lorsqu'un message est envoyé, l'ASP ne peut pas identifier l'utilisateur mobile (ni le terminal mobile).

9.1.8 Protection du contrôle d'accès

Prévention des fuites d'information et impossibilité, pour une personne non autorisée, d'obtenir les informations.

Les prescriptions de protection du contrôle d'accès sont associées aux prescriptions suivantes: confidentialité des données transmises entre un terminal mobile et un serveur d'application, confidentialité des données mémorisées dans le terminal mobile, confidentialité des données mémorisées au niveau du serveur d'application, contrôle d'accès au terminal mobile et contrôle d'accès au serveur d'application.

Le "modèle passerelle" est associé aux prescriptions suivantes: confidentialité des données transmises entre un terminal mobile et une passerelle de sécurité mobile, confidentialité des données transmises entre un terminal mobile et une passerelle de sécurité mobile, confidentialité des données transmises entre une passerelle de sécurité mobile et un serveur d'application, confidentialité des données mémorisées au niveau d'une passerelle de sécurité mobile et contrôle d'accès à une passerelle de sécurité mobile.

9.1.9 Facilité d'utilisation

Facilité d'utilisation d'une application, prévention des erreurs de lecture ou de saisie.

9.1.10 Disponibilité

Capacité de l'utilisateur mobile à recevoir un service d'application en tout lieu et en tout temps.

9.2 Prescriptions de sécurité du point de vue du fournisseur de services d'application

Les entreprises qui proposent leurs services aux utilisateurs mobiles doivent protéger leurs systèmes contre toute forme de fraude. En raison des spécificités des équipements mobiles, l'authentification de l'abonné et les mécanismes de règlement doivent être gérés soigneusement. Par ailleurs, lorsqu'un service est fourni aux utilisateurs mobiles, les éléments non-répudiation et traçabilité du service ne peuvent pas être évités. En conséquence, les prescriptions du fournisseur de services d'application portent sur les domaines suivants:

- confidentialité des données,
- intégrité des données,
- authentification,
- contrôle d'accès,
- non-répudiation,
- disponibilité.

9.2.1 Confidentialité des données

Au niveau du fournisseur de services d'application, les prescriptions relatives à la confidentialité des données couvrent les éléments suivants:

Confidentialité des données transmises entre un terminal mobile et un serveur d'application

Assure la confidentialité de la totalité des données, ou de certaines données, transmises entre un terminal mobile et un serveur d'application.

Confidentialité des données mémorisées dans un terminal mobile

Assure la confidentialité de la totalité des données, ou de certaines données, ou des contenus, envoyés par le fournisseur de services d'application et mémorisés dans un terminal mobile.

Confidentialité des données mémorisées au niveau du serveur d'application

Assure la confidentialité de toutes les données mémorisées au niveau du serveur d'application.

Dans le "modèle passerelle", les prescriptions de confidentialité des données au niveau de l'ASP couvrent également les éléments suivants:

Confidentialité des données transmises entre un terminal mobile et une passerelle de sécurité mobile

Assure la confidentialité de la totalité des données, ou de certaines données, transmises entre un terminal mobile et une passerelle de sécurité mobile.

Confidentialité des données transmises entre un serveur d'application et une passerelle de sécurité mobile

Assure la confidentialité de la totalité des données, ou de certaines données, transmises entre un serveur d'application et une passerelle de sécurité mobile.

Confidentialité des données mémorisées au niveau d'une passerelle de sécurité mobile

Assure la confidentialité de la totalité des données, ou de certaines données (ou des contenus), transmises par l'ASP et mémorisées au niveau d'une passerelle de sécurité mobile.

9.2.2 Intégrité des données

Au niveau du fournisseur de services d'application, les prescriptions d'intégrité des données couvrent les éléments suivants:

Intégrité des données transmises entre un terminal mobile et un serveur d'application

Assure l'intégrité de toutes les données transmises entre un terminal mobile et un serveur d'application.

Intégrité des données mémorisées au niveau d'un terminal mobile

Assure l'intégrité de toutes les données ou de tous les contenus envoyés par l'ASP et mémorisés dans un terminal mobile.

Intégrité des données mémorisées au niveau du serveur d'application

Assure l'intégrité de toutes les données mémorisées au niveau du serveur d'application.

Dans le "modèle passerelle", les prescriptions d'intégrité des données au niveau du fournisseur de services d'application couvrent également les éléments suivants:

Intégrité des données transmises entre un terminal mobile et une passerelle de sécurité mobile

Assure l'intégrité de la totalité (ou d'une partie) des données transmises entre un terminal mobile et une passerelle de sécurité mobile.

Intégrité des données transmises entre un serveur d'application et une passerelle de sécurité mobile

Assure l'intégrité de toutes les données transmises entre un serveur d'application et une passerelle de sécurité mobile.

Intégrité des données mises en mémoire au niveau d'une passerelle de sécurité mobile

Assure l'intégrité de toutes les données ou de tous les contenus envoyés par l'ASP et mémorisées au niveau d'une passerelle de sécurité mobile.

9.2.3 Authentification

Au niveau de l'ASP, la prescription d'authentification couvre également l'authentification de l'entité (utilisateur mobile et terminal mobile) et l'authentification du message (données reçues).

Authentification de l'utilisateur mobile

Type d'authentification d'entité servant à confirmer l'identité d'un utilisateur mobile afin d'avoir la certitude qu'il n'y a pas de tentative d'usurpation d'identité ou de répétition non autorisée d'une connexion antérieure par un utilisateur mobile.

Authentification du terminal mobile

Type d'authentification d'entité servant à confirmer l'identité d'un terminal mobile afin d'avoir la certitude qu'un terminal mobile est doté de la fonctionnalité nécessaire pour accéder à un service d'application.

Authentification des données reçues

Type d'authentification de message servant à confirmer la source des données communiquées. Il ne s'agit pas d'une demande de protection contre la duplication ou la modification des données.

9.2.4 Contrôle d'accès

La prescription de contrôle d'accès au niveau de l'ASP se compose du contrôle d'accès au serveur d'application et du contrôle d'accès au terminal mobile.

Contrôle d'accès au serveur d'application

Confère une protection contre tout accès non autorisé à un serveur d'application ou toute utilisation non autorisée d'un serveur d'application.

Le contrôle d'accès doit être conforme aux politiques de sécurité du fournisseur de services d'application.

Contrôle d'accès au terminal mobile

Confère une protection contre tout accès non autorisé aux données ou aux contenus envoyés par l'ASP au terminal mobile.

Le contrôle d'accès doit être conforme aux politiques de sécurité du fournisseur de services d'application.

Dans le "modèle passerelle", les prescriptions de contrôle d'accès à l'ASP couvrent également:

Contrôle d'accès à une passerelle de sécurité mobile

Confère une protection contre tout accès non autorisé aux données ou aux contenus envoyés par l'ASP à une passerelle de sécurité mobile.

Le contrôle d'accès doit être conforme aux politiques de sécurité du fournisseur de service d'accès.

9.2.5 Non-répudiation

Il existe deux modalités de cet élément, qui peuvent intervenir ensemble ou séparément:

Non-répudiation avec preuve d'origine

Utilisé pour prouver que les données reçues ont pour origine un utilisateur mobile donné. Egalement requis pour assurer une protection contre toute tentative, de la part de l'utilisateur mobile, à l'effet de nier avoir envoyé les données ou le contenu.

Non-répudiation avec preuve de remise

Cet élément est utilisé pour prouver que les données ont été remises à l'utilisateur mobile. Egalement requis pour conférer une protection contre toute tentative ultérieure, par l'utilisateur mobile, à l'effet de nier avoir envoyé les données ou le contenu.

Au niveau de l'ASP, les prescriptions de non-répudiation sont liées aux prescriptions suivantes: confidentialité des données transmises entre un terminal mobile et un serveur d'application, intégrité des données transmises entre un terminal mobile et un serveur d'application, intégrité des données mémorisées dans un terminal mobile, authentification de l'utilisateur mobile et contrôle d'accès au terminal mobile.

Le "modèle passerelle" est associé aux prescriptions suivantes: confidentialité des données transmises entre un terminal mobile et une passerelle de sécurité mobile, confidentialité des données transmises entre une passerelle de sécurité mobile et un serveur d'application, intégrité des données transmises entre un terminal mobile et une passerelle de sécurité mobile, intégrité des données transmises entre une passerelle de sécurité mobile et un serveur d'application, intégrité des données mémorisées au niveau de la passerelle de sécurité mobile.

9.2.6 Disponibilité

Confère à l'utilisateur mobile autorisé la capacité de recevoir un service d'application en tout lieu et en tout temps.

9.3 Relations entre les prescriptions de sécurité et les menaces sur la sécurité

Chaque prescription de sécurité est une contre-mesure face à certaines menaces sur la sécurité. La relation entre les prescriptions de sécurité et les menaces sur la sécurité est illustrée aux Tableaux 3 et 4.

Tableau 3/X.1121 – Relations entre les prescriptions de sécurité et les menaces générales sur la sécurité

Prescriptions \ Menaces	Ecoute de conversation	Brouillage de communication	Adjonction/Modification	Interruption	Accès non autorisé	Répudiation
Gestion de l'identité	X				X	X
Confidentialité des données transmises	X					
Confidentialité des données mémorisées					X	
Intégrité des données transmises			X			
Intégrité des données mémorisées					X	
Authentification d'entité			X		X	X
Authentification de message			X			
Contrôle d'accès			X		X	
Non-répudiation						X
Anonymat					X	
Protection de la sphère privée	X				X	
Facilité d'utilisation						
Disponibilité		X		X		

Tableau 4/X.1121 – Relations entre les prescriptions de sécurité et les menaces spécifiques sur la sécurité des communications mobiles

Prescriptions \ Menaces	Ecoute de conversation	Brouillage de communication	Lecture par-dessus l'épaule	Perte/vol de terminal	Interruption imprévue	Erreur de lecture/de saisie
Gestion de l'identité	X					
Confidentialité des données transmises	X					
Confidentialité des données mémorisées				X		
Intégrité des données transmises						
Intégrité des données mémorisées				X		
Authentification d'entité				X		
Authentification de message						
Contrôle d'accès				X		
Non-répudiation						
Anonymat				X		
Protection de la sphère privée	X		X	X		
Facilité d'utilisation						X
Disponibilité		X			X	

10 Fonctions de sécurité permettant de répondre aux prescriptions de sécurité concernant spécifiquement les communications mobiles

Pour satisfaire aux prescriptions de sécurité concernant spécifiquement les communications de données mobiles de bout en bout, on peut utiliser les différentes fonctions de sécurité suivantes:

- cryptage;
- échange de clés;
- signature numérique;
- contrôle d'accès;
- intégrité des données;
- échange d'authentifications;
- notarisation.

Cryptage

La fonction de cryptage peut assurer la confidentialité soit des données transmises, soit des données mémorisées.

Les algorithmes de cryptage peuvent être réversibles ou irréversibles. On distingue deux grandes catégories générales d'algorithmes de cryptage réversibles:

- a) cryptage symétrique (avec clé secrète), dans lequel la connaissance de la clé de cryptage implique la connaissance de la clé de décryptage et inversement;
- b) cryptage asymétrique (par exemple, par clé publique), dans lequel la connaissance de la clé de cryptage n'implique pas la connaissance de la clé de décryptage, et inversement. Dans un tel système, les deux clés sont souvent dénommées respectivement "clé publique" et "clé privée".

Les algorithmes de cryptage irréversibles peuvent utiliser une clé et, lorsque tel est le cas, cette clé peut être publique ou secrète.

La capacité de traitement ou la mémoire des terminaux mobiles étant limitées, il est difficile, parfois, d'appliquer les fonctions de cryptage existantes, et tout particulièrement les algorithmes asymétriques, utilisés dans les réseaux ouverts actuels. Lorsque l'on veut continuer d'utiliser des fonctions de cryptage appliquées dans un serveur de réseau ouvert, on utilise souvent le modèle passerelle.

Echange de clés

La fonction d'échange de clés permet de partager une clé dans des applications de cryptage, particulièrement dans le cas de cryptage par algorithme symétrique.

Signature numérique

La fonction de signature numérique a deux applications:

- a) signature d'élément de données;
- b) vérification d'élément de données signé.

Dans la première procédure, on utilise des informations privées (c'est-à-dire uniques et confidentielles), connues du seul signataire. Dans la seconde procédure, on utilise des informations accessibles au public mais à partir desquelles il n'est pas possible de déduire les données confidentielles connues du signataire.

La procédure de signature se fait soit par cryptage des données soit par établissement d'une valeur de vérification cryptographique des données, les informations confidentielles connues du signataire étant alors utilisées comme clé privée.

La procédure de vérification fait intervenir des procédures et des informations publiques; il s'agit de déterminer si la signature a été générée correctement sur la base des informations privées connues du signataire.

La caractéristique essentielle de la fonction de signature est que la signature ne peut être établie qu'à partir des informations confidentielles dont dispose le signataire. Ainsi, lorsque la signature est vérifiée, on peut par la suite prouver à une tierce partie (par exemple, juge ou arbitre), à tout moment, que seul le détenteur unique des informations confidentielles était en mesure d'établir la signature.

En ce qui concerne la fonction de cryptage, en raison des performances de traitement ou des mémoires limitées des terminaux mobiles, il est difficile d'implémenter les fonctions de signature numérique actuellement utilisées dans les réseaux ouverts.

Contrôle d'accès

La fonction de contrôle d'accès peut faire intervenir l'identité authentifiée d'une entité ou des informations relatives à une entité (par exemple, appartenance à un ensemble d'entités connues) ou encore les capacités d'une entité, pour déterminer et faire appliquer les droits d'accès de l'entité. Si l'entité cherche à utiliser une ressource non autorisée ou une ressource autorisée mais avec un type d'accès inadéquat, la fonction de contrôle d'accès rejette la tentative et peut aussi signaler l'incident aux fins de déclenchement d'une alarme et/ou d'enregistrement dans le cadre d'un audit de sécurité.

La fonction de contrôle d'accès peut reposer sur l'utilisation des éléments suivants:

- a) bases d'informations de contrôle d'accès, dans lesquelles les droits d'accès des entités homologues sont mémorisés dans une base de données;
- b) informations d'authentification, par exemple mot de passe, dont la détention et la présentation prouvent que l'entité qui demande l'accès est habilitée à le faire;
- c) capacités, dont la détention et la présentation établissent le droit d'accéder à l'entité ou à la ressource définie par la capacité;
- d) étiquettes de sécurité, qui, associées à une entité, peuvent servir à accorder ou à refuser l'accès, en général en fonction d'une politique de sécurité;
- e) heure de la tentative d'accès;
- f) trajet de la tentative d'accès;
- g) durée de l'accès;
- h) localisation physique de la tentative d'accès.

La fonction de contrôle d'accès peut être appliquée soit au niveau d'entités homologues d'une association de communication soit au niveau d'une passerelle de sécurité mobile.

Le contrôle d'accès prévu au niveau de l'entité d'origine ou de la passerelle de sécurité mobile sert à déterminer si l'expéditeur est autorisé à communiquer avec le destinataire et/ou à utiliser les ressources de communication requises.

Intégrité des données

On considère ici deux aspects de l'intégrité des données: l'intégrité d'un élément de données ou d'un champ unique et l'intégrité d'un flux d'unités de données ou de champs. En général, on utilise différentes technologies pour assurer ces deux types de fonctions d'intégrité, bien qu'il ne soit pas pratique d'assurer la seconde en l'absence de la première.

La détermination de l'intégrité d'un élément de données unique fait intervenir deux processus, l'un au niveau de l'entité expéditrice et l'autre au niveau de l'entité réceptrice. L'entité expéditrice associe aux données une quantité qui est fonction de l'élément de données lui-même. Cette quantité peut être une information supplémentaire, par exemple un code de vérification de bloc ou une valeur de vérification cryptographique, et elle peut être cryptée. L'entité réceptrice génère une quantité correspondante et compare le résultat à la quantité reçue pour déterminer si l'élément de données a été modifié pendant le transit. Ce seul processus ne confère pas de protection contre la répétition d'un élément de données unique.

La protection de l'intégrité d'une séquence d'éléments de données (c'est-à-dire contre les risques de désorganisation, de perte, de répétition et d'insertion ou de modification) implique l'adjonction d'une forme d'ordre explicite: numérotation de séquence, timbre horaire, enchaînement cryptographique.

Echange d'authentications

Diverses techniques de sécurité peuvent être appliquées aux échanges d'authentications, par exemple:

- a) utilisation d'informations d'authentification, par exemple mot de passe fourni par l'entité expéditrice et vérifié par l'entité réceptrice;
- b) technologies cryptographiques;
- c) utilisation des caractéristiques et/ou des détentions de l'entité.

La fonction d'échange d'authentications peut être incorporée pour assurer l'authentification des entités homologues. Lorsque la fonction n'authentifie pas l'entité, il y a rejet ou terminaison de la connexion, et, éventuellement, inscription d'une entrée dans l'audit de sécurité et/ou envoi d'un rapport au centre de gestion de la sécurité.

Lorsque des techniques cryptographiques sont utilisées, ces techniques peuvent être combinées à des protocoles de prise de contact (protection contre la répétition, c'est-à-dire garantie d'émission directe).

Pour les échanges d'authentications, la technologie de sécurité sera choisie en fonction des circonstances, parmi les moyens suivants:

- a) timbre horaire et horloges synchronisées;
- b) prise de contact bi et tridirectionnelle (respectivement pour authentification unilatérale et authentification mutuelle);
- c) fonctions de non-répudiation (signature numérique et/ou notarisation).

Notarisation

Les propriétés des données communiquées entre plusieurs entités (intégrité, origine, heure et destination) peuvent être garanties par une fonction de notarisation. L'assurance requise est alors fournie par une tierce partie, un agent assermenté qui représente les entités en communication et qui détient les informations nécessaires pour donner l'assurance requise de façon vérifiable. Chaque transmission peut faire intervenir des fonctions de signature numérique, de cryptage et d'intégrité, selon les besoins du service fourni par l'agent assermenté. Lorsqu'une telle fonction de notarisation est demandée, les données sont communiquées entre les entités par l'intermédiaire des instances de communication protégées et de l'agent assermenté.

Ces fonctions de sécurité permettent de répondre à certaines des prescriptions de sécurité. Le Tableau 5 fait apparaître les relations entre les fonctions et les prescriptions de sécurité.

Tableau 5/X.1121 – Relation entre les prescriptions et les fonctions de sécurité

Prescriptions \ Fonctions	Cryptage	Echange de clés	Signature numérique	Contrôle d'accès	Intégrité des données	Echange d'authentifications	Notarisation
Gestion d'identité	X	X	X			X	
Confidentialité des données transmises	X	X		X		X	
Confidentialité des données mémorisées	X			X			
Intégrité des données transmises	X	X	X	X	X	X	
Intégrité des données mémorisées	X		X	X	X		
Authentification d'entité	X		X			X	
Authentification de message	X	X	X		X	X	
Contrôle d'accès				X		X	
Non-répudiation			X			X	X
Anonymat	X						
Facilité d'utilisation				X			
Protection de la sphère privée	X			X		X	
Disponibilité				X		X	

11 Technologies de sécurité applicables aux communications de données mobiles de bout en bout

Pour réaliser les fonctions de sécurité définies au § 10, on utilise diverses technologies de sécurité applicables aux communications de données mobiles de bout en bout (technologies de sécurisation dans le service mobile). Ces technologies de sécurisation applicables aux communications mobiles sont classées par référence aux fonctions de sécurité assurées par la technologie en question, au lieu d'application. Du fait qu'une technologie de sécurité s'applique à une entité ou à une relation entre entités dans les modèles de communication de données mobiles de bout en bout, les lieux ou points d'application des technologies désignent les entités ou les relations entre les entités. Les Tableaux 1 et 2 indiquent les lieux d'apparition des menaces dans les modèles de communication de données mobiles de bout en bout. Les Tableaux 3 et 4 indiquent les prescriptions de sécurité, c'est-à-dire les contre-mesures applicables en fonction de la menace considérée, et le Tableau 5 indique les fonctions de sécurité qui répondent aux prescriptions de sécurité. La relation entre les fonctions de sécurité et les points d'application de ces fonctions dans les différents modèles peut alors être représentée comme au Tableau 6, lequel montre donc les points d'application, dans les modèles, des technologies de sécurité spécifiquement mobiles qui permettent d'obtenir certaines fonctions de sécurité.

Certaines technologies de sécurité mobile peuvent ne réaliser qu'une partie des fonctions de sécurité requises ou n'être appliquées qu'en un point donné. Par exemple, l'algorithme cryptographique à courbe elliptique peut être utilisé pour réaliser une fonction d'échange de clés dans la relation entre l'utilisateur et un terminal mobile. Les technologies d'authentifications biométriques peuvent servir à réaliser une fonction d'échange d'authentifications dans la relation entre l'utilisateur et un terminal mobile. Les systèmes à clé publique permettent de réaliser toutes les fonctions de sécurité dans la relation entre le terminal mobile et le serveur, la relation entre le terminal mobile et la passerelle de sécurité mobile et la relation entre le serveur et la passerelle de sécurité mobile.

Tableau 6/X.1121 – Relation entre les technologies de sécurité mobile et les modèles

Fonctions réalisées par la technologie Lieu d'application de la technologie	Terminal mobile	Serveur d'application passerelle de sécurité mobile	Relation entre l'utilisateur mobile et le terminal mobile	Relation entre le terminal mobile et le serveur d'application, autres relations
Cryptage	X	X	X	X
Echange de clés				X
Signature numérique	X	X		X
Contrôle d'accès	X	X	X	X
Intégrité des données	X	X		X
Echange d'authentifications	X	X	X	X
Notarisations				X

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication