Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1127

(09/2017)

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

Applications et services sécurisés (1) – Sécurité des télécommunications mobiles

Exigences et architecture fonctionnelles de sécurité pour les mesures de protection contre le vol de téléphones mobiles

Recommandation UIT-T X.1127

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	**X.1120–X.1139**
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1127

Exigences et architecture fonctionnelles de sécurité pour les mesures de protection contre le vol de téléphones mobiles

Résumé

La Recommandation UIT-T X.1127 traite essentiellement des exigences fonctionnelles de sécurité et de l'architecture fonctionnelle concernant les mécanismes de protection contre le vol de smartphones, compte tenu des exigences générales décrites par la Global System Mobile Association (GSMA).

Les smartphones, qui connaissent un développement rapide, sont devenus des éléments pratiquement indispensables de notre vie quotidienne. Malheureusement, un grand nombre d'utilisateurs de smartphones se sont fait voler leur téléphone. Un mécanisme de protection contre le vol de smartphones, à savoir un outil de neutralisation à distance, destiné à être utilisé en cas de perte ou de vol, devrait être doté de fonctionnalités permettant:

– de supprimer à distance les données de l'utilisateur autorisé qui se trouvent sur le smartphone;

– de rendre le smartphone inutilisable pour un utilisateur non autorisé;

– d'empêcher la réactivation sans l'autorisation de l'utilisateur autorisé, dans la mesure où cela est techniquement possible; et

– de rendre de nouveau utilisable le smartphone s'il est récupéré par l'utilisateur autorisé, et de restaurer les données de l'utilisateur se trouvant dans le smartphone dans la mesure du possible.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1127	06-09-2017	17	11.1002/1000/13259

Mots clés

Mesures de protection contre le vol, téléphone mobile, exigences de sécurité.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) 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 développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

© UIT 2018

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	1
3	Définitions	1
3.1	Termes définis ailleurs	1
3.2	Termes définis dans la présente Recommandation	2
4	Abréviations et acronymes	2
5	Conventions	3
6	Aperçu des mesures de protection contre le vol	3
6.1	Mesures de protection contre le vol	3
6.2	Exigences de haut niveau concernant les mesures de protection contre le vol	5
7	Architecture fonctionnelle des mesures de protection contre le vol de téléphones mobiles	5
7.1	Menaces sur les mesures de protection contre le vol de téléphones mobiles	5
7.2	Principales fonctions de sécurité pour les mesures de protection contre le vol de téléphones mobiles	6
7.3	Architecture fonctionnelle des mesures de protection contre le vol de dispositifs mobiles	6
7.4	Mécanismes pour les mesures de protection contre le vol de téléphones mobiles	8
8	Exigences fonctionnelles de sécurité	10
8.1	Vue d'ensemble	10
8.2	Exigences fonctionnelles de sécurité applicables au propriétaire du dispositif mobile	11
8.3	Exigences fonctionnelles de sécurité applicables au serveur autorisé	11
8.4	Exigences fonctionnelles de sécurité applicables au dispositif mobile volé	12
8.5	Exigences fonctionnelles de sécurité applicables au serveur de sauvegarde	12
Appendice I – Exigences générales applicables aux mesures de protection contre le vol		13
I.1	Propriétaire du dispositif	13
I.2	Serveur	14
I.3	Dispositif mobile	14
I.4	Fabrication du dispositif	15
Appendice II – Exigences de sécurité additionnelles applicables à la protection contre le vol		16
II.1	Exigences applicables au serveur de sauvegarde	16
Appendice III – Menaces propres à la protection contre le vol		17
III.1	Menaces entre le propriétaire du dispositif mobile et le serveur autorisé	17
III.2	Menaces entre le serveur autorisé et l'agent de désactivation de la protection contre le vol	17

III.3 Menaces entre l'agent de désactivation de la protection contre le vol et le serveur de sauvegarde 17
Appendice IV – Scenario relatif aux mesures de protection contre le vol 18
IV.1 Types de fonctions de désactivation du dispositif mobile 18
IV.2 Activation du dispositif mobile volé/perdu 18
IV.3 Scénario de désactivation du dispositif mobile volé/perdu 18
Appendice V – Profil de protocole TLS pour les mesures de protection contre le vol 19
V.1 Exigences relatives au protocole TLS 19
V.2 Suites de chiffrement TLS pour l'interopérabilité 19
V.3 Certificats numériques 19
Appendice VI – Aperçu de la gestion des dispositifs OMA 21
VI.1 Spécification de la gestion des dispositifs OMA 21
Bibliographie 22

Recommandation UIT-T X.1127

Exigences et architecture fonctionnelles de sécurité pour les mesures de protection contre le vol des téléphones mobiles

1 Domaine d'application

La présente Recommandation traite des exigences et de l'architecture fonctionnelles de sécurité concernant les mesures de protection contre le vol de smartphones (à savoir un outil de neutralisation à distance), qui permet aux utilisateurs de supprimer à distance leurs données personnelles ou de désactiver les smartphones volés ou perdus.

Il est prévu que les exigences fonctionnelles de sécurité et l'architecture fonctionnelle définies dans la présente Recommandation soient applicables aux smartphones qui sont dotés de fonctionnalités de protection contre le vol correspondant aux attentes des clients et des fabricants de smartphones et des opérateurs de services mobiles.

La présente Recommandation porte essentiellement sur les exigences fonctionnelles, l'architecture fonctionnelle et les mécanismes de protection contre le vol. Elle utilise un modèle de référence comprenant le propriétaire du dispositif, le serveur autorisé, le serveur de sauvegarde et les dispositifs volés ou perdus. Les menaces particulières qui pèsent sur la protection contre le vol sont décrites dans l'Appendice III. La présente Recommandation ne modifie pas les exigences générales applicables aux fonctionnalités de protection contre le vol des smartphones mises au point par la GSMA [b-GSMA].

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification des entités*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 nettoyage des données [b-NIST SP 800-88]: mesures prises pour rendre irrécupérables les données écrites se trouvant dans des supports, à l'aide de moyens simples ou exceptionnels.

3.1.2 garantie d'authentification d'entité (EAA, *entity authentication assurance*) [UIT-T X.1254]: degré de confiance atteint au cours de la procédure d'authentification, selon lequel l'entité est ce qu'elle est ou ce qu'elle devrait être (cette définition repose sur la définition de la "garantie d'authentification" donnée dans la norme [b-UIT-T X.1252]).

NOTE – La confiance est fondée sur le degré de confiance dans le lien entre l'entité et l'identité qui est présentée.

3.1.3 identité [b-UIT-T X.1250]: représentation d'une entité sous la forme d'un ou de plusieurs éléments d'information qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux

fins de l'IdM, le terme identité désigne l'identité contextuelle (sous-ensemble d'attributs), c'est-à-dire que la diversité des attributs est limitée par un cadre avec des frontières définies (le contexte) dans lequel l'entité existe et interagit.

NOTE – Chaque entité est représentée par une identité holistique, qui comprend tous les éléments d'information possibles caractérisant cette entité (les attributs). Toutefois, l'identité holistique est théorique et échappe à toute description et utilisation pratique, car le nombre de tous les attributs possibles est indéfini.

3.1.4 neutralisation à distance (kill switch) [b-GSMA]: moyens permettant de désactiver les fonctions cruciales d'un dispositif mobile

NOTE – Il s'agit pour l'essentiel d'une fonction intégrée au dispositif de l'équipement mobile qui, lorsqu'elle est activée, par exemple par un message qui lui est envoyé dans un certain format, aura pour conséquence que le dispositif mobile cessera de fonctionner comme prévu, et ne pourra être réactivé ou réutilisé que si le propriétaire du dispositif autorise la réactivation de ce dispositif.

3.1.5 téléphone mobile [b-UIT-T X-Sup.19]: appareil électronique utilisé pour faire des appels téléphoniques et envoyer des messages textuels dans un vaste espace géographique par un accès radio aux réseaux publics de téléphonie mobile, tout en permettant à l'utilisateur de se déplacer.

3.1.6 téléphone intelligent [b-UIT-T X-Sup.19]: téléphone mobile doté de puissantes capacités de calcul, d'une connectivité hétérogène et d'un système d'exploitation évolué qui fournit une plate-forme pour les applications de tierce partie.

3.1.7 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

3.1.8 tunnel [b-ISO/CEI 27033-1]: trajet de données entre des dispositifs raccordés à un réseau, qui est établi sur une infrastructure de réseau existante.

NOTE – Des tunnels peuvent être créés au moyen de techniques telles que l'encapsulation de protocole, la commutation par étiquette ou les circuits virtuels.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 éléments matériels du dispositif (device hardware): éléments physiques qui forment ensemble un dispositif mobile en fonctionnement comprenant un écran, des touches, des cartes de circuits imprimés, des puces, des cartes SIM, un stockage amovible, etc.

3.2.2 éléments logiciels du dispositif (device software): il s'agit de tous les progiciels du dispositif et de la carte SIM, y compris les applications, le système d'exploitation, l'amorceur, la mémoire d'amorçage, et les micrologiciels.

3.2.3 utilisateur du dispositif: utilisateur autorisé du dispositif mobile.

3.2.4 tunnellisation sécurisée: protocole qui permet le transfert sécurisé de données ou de messages d'un emplacement de réseau vers un autre.

NOTE – La tunnellisation sécurisée prend généralement en charge l'authentification de l'entité, l'intégrité du message et la confidentialité du message.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ATM distributeur automatique (*automated teller machine*)

CRL liste de révocation de certificats (*certificate revocation list*)

DDoS déni de service réparti (*distributed denial-of-service*)

DER règles de codage distinctives (*distinguished encoding rules*)

DM gestion des dispositifs (*device management*)

EAA garantie d'authentification d'entité (*entity authentication assurance*)

GPS système mondial de localisation (*global positioning system*)

GSMA Groupe Speciale Mobile Association

HTTP protocole de transfert hypertexte (*hyper text transfer protocol*)

LoA niveau de garantie (*level of assurance*)

MAC code d'authentification de message (*message authentication code*)

OCSP protocole de statut du certificat en ligne (*online certificate status protocol*)

OMA Open Mobile Alliance

OTP mot de passe à usage unique (*one-time password*)

PII informations d'identification personnelle (*personally identifiable information)*

PKI infrastructure de clé publique (*public key infrastructure*)

SIM module d'identité d'abonné (*subscriber identity module*)

SMS-SC centre de services – service de messages courts (*short message service – service centre*)

SSL couche de connecteurs sécurisés (*secure socket layer*)

TCP protocole de commande de transmission (*transmission control protocol*)

TFA authentification à trois facteurs (*three-factor authentication*)

TLS sécurité dans la couche transport (*transport layer security*)

U universel

UICC carte à circuit intégré universelle (*universal integrated circuit card*)

USSD données de service complémentaire non structurées (*unstructured supplementary service data*)

2FA authentification à deux facteurs (*2-factor authentication*)

5 Conventions

La présente Recommandation emploie les formes verbales ci-après lors de la formulation des dispositions:

a) "Doit" désigne une obligation.

b) "Devrait" désigne une recommandation.

c) "Peut" désigne une autorisation.

d) "Pourrait" désigne une possibilité ou une capacité

6 Aperçu des mesures de protection contre le vol

6.1 Mesures de protection contre le vol

Les téléphones intelligents (smartphones), qui connaissent un développement rapide, sont devenus des éléments indispensables de notre vie quotidienne. Malheureusement, des millions d'utilisateurs de smartphones se sont fait voler leur téléphone. Un mécanisme de protection contre le vol de smartphones, à savoir un outil de neutralisation à distance, devrait être doté de fonctionnalités permettant:

– de supprimer à distance les données personnelles de l'utilisateur qui se trouvent sur le smartphone en cas de perte ou de vol;
– de rendre le smartphone inutilisable pour un utilisateur non autorisé;
– de stocker au besoin les données personnelles de l'utilisateur dans le serveur de sauvegarde, qui sont exploitées par les opérateurs de services cellulaires ou les fabricants de dispositifs;
– d'empêcher la réactivation sans l'autorisation de l'utilisateur autorisé; et
– de rendre de nouveau utilisable le smartphone s'il est récupéré par l'utilisateur autorisé et de restaurer les données personnelles de l'utilisateur se trouvant dans le smartphone, dans la mesure du possible, depuis le serveur de sauvegarde.

Un logiciel de protection contre le vol, installé dans un dispositif mobile, peut désactiver un combiné volé ou perdu.

Lorsque le propriétaire d'un dispositif se rend compte que son dispositif mobile est perdu ou volé, deux scénarios sont possibles pour lancer l'exécution des fonctions de désactivation:

1) le propriétaire du dispositif se met en rapport avec son opérateur de services cellulaires, qui demande la désactivation du dispositif mobile; et
2) le propriétaire du dispositif lance une application sur un autre dispositif mobile, ou accède à un outil de désactivation qui rend inutilisable le dispositif mobile volé ou perdu.

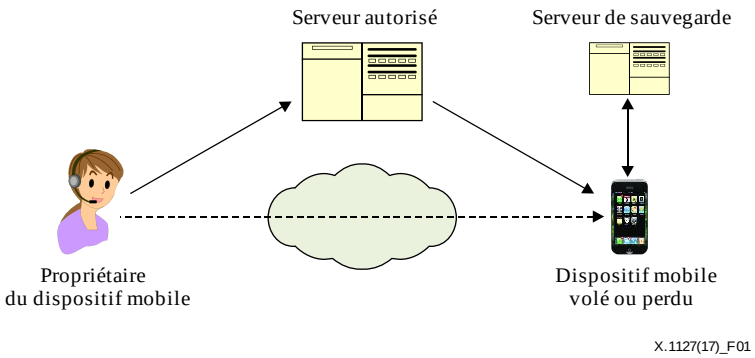


Figure 1 – Modèle de référence des mesures de protection contre le vol

La Figure 1 décrit le modèle de référence des mesures de protection contre le vol pour les dispositifs mobiles. Le serveur autorisé prend en charge la fonction de désactivation des dispositifs mobiles, volés ou perdus, et est géré par les fournisseurs de services cellulaires ou les fabricants de dispositifs. Le serveur autorisé envoie l'instruction de désactivation au dispositif volé ou perdu. Le serveur de sauvegarde rétablit les données personnelles du dispositif mobile à la demande du propriétaire du dispositif.

La communication entre le dispositif mobile perdu ou volé et le serveur autorisé devrait être protégée au moyen d'un tunnel sécurisé (par exemple une couche de connecteurs sécurisés (SSL)). De plus, la communication entre le dispositif mobile perdu ou volé et le serveur de sauvegarde devrait être protégée au moyen d'un tunnel sécurisé (par exemple une couche SSL).

La présente Recommandation s'appuie sur le cadre de garantie d'authentification de l'entité (EAA) pour la gestion de la garantie EAA décrite dans la Recommandation [UIT-T X.1254]. Ce cadre EAA définit quatre niveaux de garantie (LoA) pour l'authentification de l'entité. Chacun des niveaux LoA décrit le degré de confiance dans les processus qui conduisent à la procédure d'authentification et intègrent cette procédure elle-même, offrant ainsi des garanties quant au fait que l'entité qui emploie une identité donnée est bien l'entité à laquelle cette identité a été attribuée.

Il se peut que certaines juridictions demandent que le logiciel de protection contre le vol soit installé ou puisse être téléchargé. Ainsi, aux Etats-Unis, la Californie exige que des logiciels de protection contre le vol soient installés sur les nouveaux téléphones, mais les utilisateurs auront la possibilité de désactiver cette fonction, même si elle sera activée par défaut. Etant donné que la fonction de protection contre le vol repose sur la possibilité de refus, et non pas sur l'acceptation expresse, il est à prévoir que de nombreux autres clients auront recours aux mesures de protection contre le vol, ce qui permettra une possibilité de protection accrue d'un dispositif mobile donné.

6.2 Exigences de haut niveau concernant les mesures de protection contre le vol

Les exigences de sécurité de haut niveau concernant les mesures de protection contre le vol lors du transfert de messages de protection contre le vol entre le serveur autorisé et le dispositif mobile sont les suivantes:

– authentification de l'entité;
– intégrité du message;
– détection de répétitions et intégrité de séquence;
– preuve de la réception et preuve de l'exécution;
– confidentialité du message; et
– indication des mécanismes de sécurité utilisés.

7 Architecture fonctionnelle des mesures de protection contre le vol de téléphones mobiles

7.1 Menaces sur les mesures de protection contre le vol de téléphones mobiles

Le présent paragraphe décrit un ensemble de menaces de sécurité identifiées, qui sont prises en compte par certaines exigences ou certains mécanismes décrits dans la présente Recommandation. Le modèle des menaces de sécurité et d'autres éléments fondamentaux reposent sur les Recommandations UIT-T suivantes:

– [b-UIT-T X.800]: définit les éléments d'architecture généraux liés à la sécurité qui peuvent être appliqués de façon appropriée dans les cas où il est nécessaire de protéger les communications entre des systèmes ouverts;
– [b-UIT-T X.805]: définit l'architecture de sécurité de réseau pour assurer la sécurité du réseau de bout en bout.

Les Recommandations [b-UIT-T X.800] et [b-UIT-T X.805] mettent en évidence les menaces suivantes pour la sécurité des réseaux:

– destruction d'informations ou d'autres ressources;
– altération ou modification d'informations;
– vol, suppression ou perte d'informations ou d'autres ressources;
– divulgation d'informations;
– interruption de services.

La présente Recommandation identifie les menaces ci-après propres aux mesures de protection contre le vol de téléphones mobiles:

– demande non autorisée de suppression de données se trouvant dans un téléphone mobile désactivé;
– demande non autorisée de désactivation du téléphone mobile;
– divulgation non autorisée de données sensibles se trouvant dans un téléphone mobile
– perte des données de l'utilisateur se trouvant dans un téléphone mobile;

– accès ou modification non autorisé des fonctions ou des données d'un dispositif désactivé;

– divulgation non autorisée des données de l'utilisateur et des logiciels échangés entre le dispositif et l'opérateur de réseau ou l'outil de désactivation utilisé dans le cadre de la mesure de protection contre le vol.

Les risques sont les suivants:

– les pirates pourraient trouver un moyen d'intercepter des instructions de désactivation et éteindre le dispositif mobile;

– les données personnelles stockées dans le serveur de sauvegarde ou en transit entre le dispositif mobile et le serveur de sauvegarde pourraient être divulguées.

7.2 Principales fonctions de sécurité pour les mesures de protection contre le vol de téléphones mobiles

Les fonctions permettant de désactiver un dispositif mobile ne doivent être exécutées que depuis un serveur autorisé ou un outil de désactivation prenant en charge la fonction de désactivation. Pour satisfaire à cette exigence, les cinq fonctions ci-après sont nécessaires:

1) connexion de communication sécurisée entre le dispositif et le serveur;

2) authentification de l'entité par le serveur du dispositif;

3) authentification de l'entité par le dispositif du serveur et le serveur autorisé à exécuter la fonction;

4) localisation du dispositif mobile volé; et

5) sauvegarde/suppression sécurisée des données sur un téléphone mobile désactivé.

Il conviendrait de prévoir un mécanisme, par l'intermédiaire du site web de la personne, permettant aux propriétaires de dispositifs de gérer les informations d'identification personnelle (PII) devant être stockées par le propriétaire du dispositif. L'application installée dans le dispositif mobile pourra être fournie au propriétaire du dispositif. L'application de protection contre le vol pourra permettre aux propriétaires de dispositifs de sélectionner les données contenant des informations PII pour la protection contre le vol et comporter des sauvegardes automatiques des données contenant des informations PII dans une solution de stockage basée sur le nuage. La procédure à suivre pour assurer cette gestion comprend les trois mesures suivantes:

1) installation d'applications sur le dispositif mobile;

2) inscription sur le site web par les prestataires de services mobiles ou les fabricants de dispositifs;

3) gestion (c'est-à-dire suppression, téléchargement, mise en ligne) des informations PII stockées dans le serveur de sauvegarde par l'intermédiaire du site web de la personne.

7.3 Architecture fonctionnelle des mesures de protection contre le vol de dispositifs mobiles

L'architecture fonctionnelle des mesures de protection contre le vol de dispositifs mobiles repose sur l'architecture de sécurité décrite dans la norme [b-3GPP TS 33.102]. La Figure 2 décrit l'architecture de sécurité composée des cinq groupes de sécurité suivants:

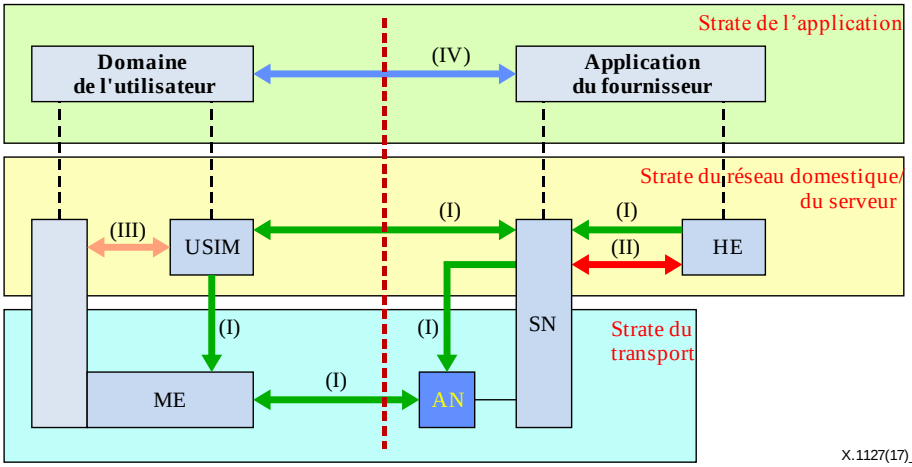
1) sécurité de l'accès au réseau (I): ensemble des fonctions de sécurité qui fournissent aux utilisateurs un accès sécurisé aux services 3G et assurent en particulier une protection contre les attaques se produisant sur la liaison d'accès (radioélectrique);

2) sécurité dans le domaine de réseau (II): ensemble des fonctions de sécurité qui permettent à des noeuds dans le domaine du fournisseur d'échanger en toute sécurité des données de signalisation et d'assurer une protection contre les attaques se produisant dans le réseau filaire;

3) sécurité dans le domaine de l'utilisateur (III): ensemble des fonctions de sécurité qui sécurisent l'accès aux stations mobiles;

4) sécurité dans le domaine de l'application (IV): ensemble des fonctions de sécurité qui permettent à des applications dans le domaine de l'utilisateur et dans le domaine du fournisseur d'échanger des messages en toute sécurité;

5) visibilité et configurabilité de la sécurité (V): ensemble des fonctions qui permettent à l'utilisateur de savoir si une fonction de sécurité fonctionne ou non et si l'utilisation et la fourniture de services devraient dépendre de la fonction de sécurité.



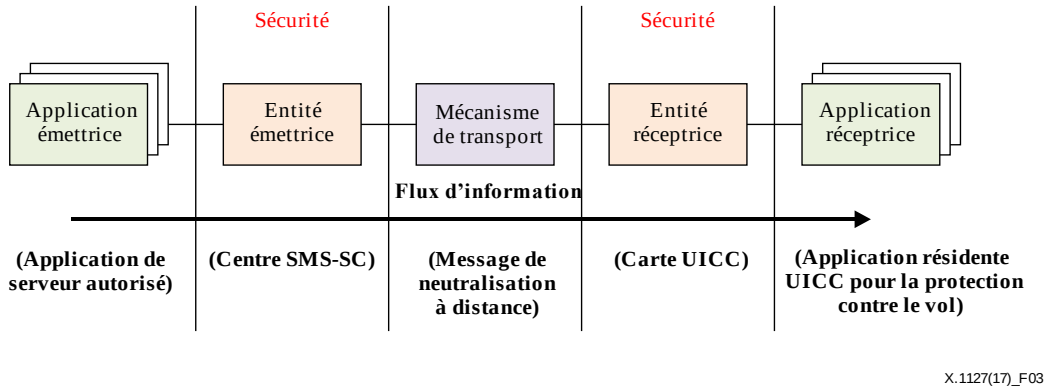
NOTE – La Figure 2 est reprise de la norme [b-3GPP TS 33.102].

Figure 2 – Architecture de sécurité

L'application relative aux mesures de protection contre le vol figurant dans le dispositif mobile fait partie de l'ensemble des applications qui résident dans le domaine de l'utilisateur, alors que la fonction de protection contre le vol du fournisseur de services fait partie de l'ensemble des applications résidant dans l'application du fournisseur.

Le modèle de référence de sécurité pour les mesures de protection contre le vol est fondé sur le modèle décrit dans la norme [b-3GPP TS 22.048]. L'application émettrice est une entité qui génère un message d'application à envoyer, tandis que l'entité émettrice est l'entité d'où provient le paquet sécurisé (par exemple, centre de services – service de messages courts (SMS-SC), carte à circuit intégré universelle (UICC), point d'entrée des données de service complémentaire non structuré (USSD) ou serveur de l'utilitaire spécialisé du module d'identité d'abonné (SIM) universel (U)), et dans laquelle les mécanismes de sécurité sont demandés. L'entité émettrice génère les paquets sécurisés devant être envoyés. Les paquets sécurisés sont transmis par l'intermédiaire du tunnel sécurisé au niveau du transport ou du tunnel sécurisé au niveau de l'application.

L'application réceptrice est l'entité à laquelle le message d'application est destiné, tandis que l'entité réceptrice est l'entité dans laquelle le paquet sécurisé est reçu (par exemple centre SMS-SC, carte UICC, point d'entrée USSD, ou utilitaire spécialisé du module SIM (U).



NOTE – La Figure 3 est reprise de la norme [b-3GPP TS 22.048].

Figure 3 –Modèle de référence de sécurité

Dans la présente Recommandation, l'architecture de sécurité est fondée sur le modèle de référence décrit dans la Figure 1, sur l'architecture de sécurité décrite dans la Figure 2 et sur le modèle de référence de sécurité décrit dans la Figure 3.

7.4 Mécanismes pour les mesures de protection contre le vol de téléphones mobiles

7.4.1 Mécanismes de communication sécurisée

Le dispositif volé ou perdu devrait jouer le rôle de serveur d'authentification d'un client de tunnel sécurisé.

Le canal de communication entre le client et le serveur devrait être conforme aux six exigences suivantes en matière de sécurité:

1) Confidentialité: le tunnel sécurisé devrait faire en sorte que les données ne puissent être lues par des entités entité non autorisées. Pour ce faire, les données sont chiffrées au moyen d'un algorithme cryptographique et d'une clé secrète, valeur que connaissent uniquement les deux entités qui échangent des données. Les données ne peuvent être déchiffrées que par une entité qui possède la clé secrète.

2) Intégrité: le tunnel sécurisé devrait déterminer si les données ont été modifiées (délibérément ou non) pendant le transit. L'intégrité des données doit être assurée en générant une valeur de code d'authentification de message (MAC), qui est une somme de contrôle cryptographique à clé des données. Si les données sont modifiées et que la valeur de code MAC est recalculée, les anciennes et nouvelles valeurs de code MAC seront différentes.

3) Authentification d'homologue: chaque point d'extrémité doit confirmer l'identité de l'autre. Point d'extrémité avec lequel il souhaite communiquer, ce qui garantit que le trafic du réseau et les données sont envoyées depuis le serveur escompté. En général, l'authentification du tunnel sécurisé est effectuée dans un seul sens, en authentifiant le serveur auprès du client, mais un tunnel sécurisé exige l'authentification pour les deux points d'extrémité.

4) Protection contre les répétitions: les mêmes données ne doivent pas être fournies plusieurs fois et les données ne doivent pas être fournies dans le désordre. Un numéro de séquence ou un compteur pourrait être utilisé à la source d'un message. La source ou le message ajoute un numéro de séquence à son paquet à partir de 0 et augmente chaque fois qu'il/elle envoie un autre message.

5) Protection contre l'analyse du trafic: une personne surveillant le trafic du réseau ne doit pas déterminer le contenu du trafic de réseau ou le volume d'informations échangées. Un tunnel sécurisé peut également dissimuler les parties qui sont en communication, tandis que la couche SSL laisse cette information exposée. La fréquence de la communication peut

également être protégée en fonction de la mise en oeuvre. Néanmoins, le nombre de paquets échangés peut être compté.

6) Contrôle d'accès: les points d'extrémité du tunnel sécurisé doivent procéder à un filtrage pour faire en sorte que seuls les utilisateurs autorisés puissent accéder à des ressources de réseau données. En outre, les points d'extrémité du tunnel sécurisé peuvent autoriser ou bloquer certains types de trafic de réseau, par exemple en autorisant l'accès au serveur web, mais en refusant le partage de fichiers.

Pour satisfaire aux exigences ci-dessus, il est recommandé d'utiliser la sécurité dans la couche transport (TLS) pour sécuriser la communication entre le dispositif mobile et le serveur autorisé. Le protocole TLS est un protocole qui assure un tunnel de communication sécurisé sur des réseaux. Il permet à des applications client/serveur de communiquer de façon à empêcher l'écoute clandestine, l'altération volontaire, ou la falsification de messages. Le protocole TLS est positionné au-dessus de protocoles de transport fiables (par exemple le protocole de commande de transmission (TCP)), et est utilisé pour l'encapsulation de divers protocoles de niveau supérieur (par exemple le protocole de transfert hypertexte (HTTP)).

Le protocole TLS comprend trois phases principales:

1) la négociation entre homologues pour la prise en charge des algorithmes;
2) l'échange de clés et l'authentification;
3) le chiffrement symétrique et l'authentification de messages.

Le profil détaillé du protocole TLS est donné dans l'Appendice V.

En outre, la présente Recommandation préconise l'utilisation du canal de communication sécurisée fondé sur le protocole de l'Open Mobile Alliance (OMA).

7.4.2 Mécanismes d'authentification mutuelle

L'authentification sert à confirmer les identités d'entités en communication. Il existe trois types de facteurs d'authentification:

1) facteur lié à la connaissance: ("quelque chose que seul l'utilisateur connaît"), par exemple des mots de passe;
2) facteur lié à la possession ("quelque chose que seul l'utilisateur possède"), par exemple les cartes de guichet automatique (ATM); et
3) facteur lié à l'inhérence ("uniquement ce que l'entité est"), par exemple la biométrie.

La norme [b-UIT-T X.1158] décrit trois types de méthodes d'authentification:

1) l'authentification à facteur unique (SFA) est la méthode classique qui exige uniquement un nom d'utilisateur et un mot de passe avant d'accorder l'accès à l'utilisateur;
2) l'authentification à deux facteurs (2FA) repose sur l'utilisation d'une combinaison de deux facteurs d'authentification différents. Ces facteurs peuvent être quelque chose qu'un utilisateur connaît, quelque chose qu'un utilisateur possède ou ce qu'est un utilisateur. Un bon exemple nous est fourni dans la vie courante, lorsqu'un utilisateur veut retirer de l'argent à un distributeur automatique, seule la combinaison correcte d'une carte bancaire (quelque chose que l'utilisateur possède) et d'un numéro d'identification personnelle (PIN), c'est-à-dire quelque chose qu'un utilisateur connaît permettent d'effectuer la transaction.

3) l'authentification à trois facteurs (TFA) repose sur l'utilisation de la combinaison de trois facteurs différents indépendants: ce qu'un utilisateur connaît (mot de passe), ce qu'un utilisateur possède (jeton de sécurité) et ce qu'est un utilisateur (vérification biométrique).

L'authentification à plusieurs facteurs repose sur l'utilisation d'une combinaison d'au moins deux facteurs différents indépendants. Les authentifications 2FA et TFA sont des exemples d'authentification à plusieurs facteurs.

7.4.3 Mécanismes de suppression de données sécurisées

On entend par nettoyage des données un processus qui rend impossible l'accès aux données cibles sur les supports pour un niveau d'effort donné. Les normes [b-NIST SP 800-88] et [b-NIST SP 800-88] prévoient les trois catégories de nettoyage suivantes:

1) opération de libération: cette opération applique des techniques logiques pour nettoyer les données dans tous les emplacements de stockage adressables par l'utilisateur, afin d'assurer une protection contre des techniques simples de récupération des données non intrusives; en général, elle est appliquée par l'intermédiaire des commandes normalisées "lecture de données" et "écriture de données" dans le dispositif de stockage, par exemple au moyen de la réécriture d'une nouvelle valeur ou de l'utilisation d'une option du menu pour réinitialiser le dispositif afin de rétablir les paramètres d'origine (lorsque la réécriture n'est pas prise en charge);
2) opération d'élimination: cette opération applique des techniques physiques ou logiques qui rendent impossible la récupération des données cibles au moyen des techniques de laboratoire les plus modernes;
3) opération de destruction: rend impossible la récupération des données cibles au moyen des techniques de laboratoire les plus modernes et a pour conséquence l'impossibilité d'utiliser le support pour le stockage de données.

L'opération de libération se superpose au support en utilisant des logiciels approuvés au niveau de l'organisation et procède à la vérification des données remplacées en surécriture. Le schéma de libération devrait être au moins un passage d'écriture unique avec une valeur des données fixe, par exemple uniquement des zéros. Plusieurs passages d'écriture ou des valeurs plus complexes peuvent être utilisés à titre facultatif.

8 Exigences fonctionnelles de sécurité

8.1 Vue d'ensemble

– Il est obligatoire que l'architecture fonctionnelle repose sur le cadre EAA décrit dans la Recommandation [UIT-T X.1254].
– L'architecture fonctionnelle doit impérativement fournir un tunnel sécurisé (par exemple, le protocole TLS décrit dans la norme [b-IETF RFC 6460] ou le canal de communication sécurisé fondé sur le protocole OMA) pour la communication entre composants.
– L'architecture fonctionnelle doit impérativement assurer une gestion de clés sécurisée (fondée par exemple sur l'infrastructure de clé publique (PKI) décrite dans la norme [b-UIT-T X.509]) pour la prise en charge de tunnels sécurisés.
– Il est obligatoire que l'architecture fonctionnelle prenne en charge au moins le mécanisme d'authentification de l'entité de niveau de garantie 2 décrit dans la Recommandation [UIT-T X.1254].
– L'architecture fonctionnelle doit impérativement prendre en charge au moins l'inscription d'entités de niveau de garantie 2 décrite dans la Recommandation [UIT-T X.1254].

– L'architecture fonctionnelle doit impérativement prendre en charge au moins la gestion des justificatifs d'identité d'une entité de niveau de garantie 2 décrite dans la Recommandation [UIT-T X.1254].
– L'architecture fonctionnelle doit impérativement prendre en charge l'authentification de message pour les messages transférés.
– L'architecture fonctionnelle doit impérativement prendre en charge la protection contre les attaques par répétition pour les messages transférés.
– L'architecture fonctionnelle doit impérativement prendre en charge la capacité de sauvegarde des données du dispositif dans le serveur de réseau sécurisé.
– L'architecture fonctionnelle doit impérativement assurer une autorisation forte (commande d'accès).
– L'architecture fonctionnelle doit impérativement prendre en charge les mécanismes de sécurité décrits dans la norme [b-3GPP TS 22.048].
– L'architecture fonctionnelle doit impérativement assurer la gestion des identités pour le propriétaire du dispositif mobile, le serveur autorisé et les dispositifs mobiles volés.

8.2 Exigences fonctionnelles de sécurité applicables au propriétaire du dispositif mobile

– Le propriétaire du dispositif mobile doit impérativement être authentifié auprès du serveur autorisé sur la base au moins d'une authentification 2FA (par exemple, identité/mot de passe et mot de passe à usage unique (OTP) décrit dans la Recommandation [UIT-T X.1254]).
– Le propriétaire du dispositif mobile doit impérativement être identifié au moyen d'au moins l'inscription d'entité de niveau de garantie 2 décrite dans la Recommandation [UIT-T X.1254].
– Il est obligatoire que l'architecture fonctionnelle du propriétaire du dispositif authentifie le serveur d'autorisation en utilisant au moins le mécanisme d'authentification de niveau de garantie 2 décrit dans la Recommandation [UIT-T X.1254].
– Il est obligatoire que l'architecture fonctionnelle du propriétaire du dispositif prenne en charge un tunnel sécurisé (par exemple le protocole TLS décrit dans la norme [b-IETF RFC 6460] ou un canal de communication sécurisé reposant sur le protocole OMA) pour la communication du message transféré avec le serveur autorisé.

8.3 Exigences fonctionnelles de sécurité applicables au serveur autorisé

– Il est obligatoire que l'architecture fonctionnelle du serveur autorisé authentifie le propriétaire du dispositif en utilisant au moins un mécanisme d'authentification 2FA (par exemple les authentifications de niveau de garantie 3 décrites dans la Recommandation [UIT-T X.1254]).
– L'architecture fonctionnelle du serveur autorisé doit impérativement être authentifiée par le dispositif mobile volé en utilisant au moins un mécanisme d'authentification 2FA (par exemple les authentifications de niveau de garantie 3 décrites dans la Recommandation [UIT-T X.1254]).
– Il est obligatoire que l'architecture fonctionnelle du serveur autorisé prenne en charge un tunnel sécurisé (par exemple le protocole TLS décrit dans la norme [b-IETF RFC 6460] ou un canal de communication sécurisé reposant sur le protocole OMA) pour la communication du message avec le propriétaire du dispositif mobile.
– Il est obligatoire que l'architecture fonctionnelle du serveur autorisé prenne en charge un tunnel sécurisé pour la communication du message transféré avec le dispositif mobile volé.

8.4 Exigences fonctionnelles de sécurité applicables au dispositif mobile volé

– Il est obligatoire que l'architecture fonctionnelle du dispositif mobile volé prenne en charge un tunnel sécurisé (par exemple le protocole TLS décrit dans la norme [b-IETF RFC 6460] ou un canal de communication sécurisé reposant sur le protocole OMA) pour la communication du message transféré avec le serveur autorisé.

– L'architecture fonctionnelle du dispositif mobile volé doit impérativement être authentifiée auprès du serveur autorisé en utilisant au moins un mécanisme d'authentification 2FA (par exemple les authentifications de niveau de garantie 3 décrites dans la Recommandation [UIT-T X.1254]).

– L'architecture fonctionnelle du dispositif mobile volé doit impérativement authentifier le serveur autorisé en utilisant au moins un mécanisme d'authentification 2FA (par exemple les authentifications de niveau de garantie 3 décrites dans la Recommandation [UIT-T X.1254]).

– L'architecture fonctionnelle du dispositif mobile volé doit impérativement demander une fonctionnalité de sauvegarde de toutes les données du dispositif qui appartiennent au propriétaire à un serveur de réseau sécurisé.

– L'architecture fonctionnelle du dispositif mobile volé doit impérativement mettre en oeuvre les mécanismes de commande d'accès pour lancer les instructions reçues en provenance du serveur autorisé.

– L'architecture fonctionnelle du dispositif mobile volé doit impérativement protéger les données ou les fonctions contre l'accès et l'utilisation par une entité non autorisée.

– L'architecture fonctionnelle du dispositif mobile volé doit impérativement prendre en charge l'opération de libération pour la suppression sécurisée des données décrite au paragraphe 7.4.3, une fois qu'elle reçoit l'instruction de suppression des données dans le dispositif mobile en provenance du serveur autorisé.

8.5 Exigences fonctionnelles de sécurité applicables au serveur de sauvegarde

– Il est obligatoire que l'architecture fonctionnelle du serveur de sauvegarde prenne en charge un tunnel sécurisé pour le transfert de messages à l'aide du dispositif mobile.

– L'architecture fonctionnelle du serveur de sauvegarde doit impérativement authentifier le dispositif mobile à l'aide d'un mécanisme d'authentification robuste, qui doit assurer la sauvegarde des données du dispositif, le cas échéant.

– L'architecture fonctionnelle du serveur de sauvegarde doit impérativement être authentifiée par le dispositif mobile au moyen d'un mécanisme d'authentification robuste.

– L'architecture fonctionnelle du serveur de sauvegarde doit impérativement prendre en charge la capacité de sauvegarder les données appropriées du dispositif en provenance du dispositif mobile;

– L'architecture fonctionnelle du serveur de sauvegarde doit impérativement fournir des ressources suffisantes (c'est-à-dire le stockage) au dispositif mobile.

Appendice I

Exigences générales applicables aux mesures de protection contre le vol

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

La norme [b-GSMA] décrit les exigences générales en matière d'informations pour les mesures de protection contre le vol. Le présent Appendice décrit ces exigences.

I.1 Propriétaire du dispositif

– Afin de confirmer que le dispositif a été irrémédiablement perdu ou volé (les coordonnées GPS (système mondial de localisation) montrent par exemple que le dispositif se trouve dans un lieu inconnu du propriétaire), le propriétaire est tenu d'engager la procédure de désactivation du service, après avoir pris les mesures suivantes:
  - signalisation du dispositif pour qu'il émette une tonalité forte pendant une période prolongée (30 secondes à 3 minutes), afin de permettre au propriétaire de localiser le dispositif, à supposer qu'il soit tout près;
  - affichage d'un message sur l'écran verrouiller/l'écran d'accueil demandant la restitution du dispositif;
  - détermination de l'emplacement du dispositif au moyen du GPS (ou de toute autre technique de localisation si cette fonctionnalité est prise en charge par le dispositif) et indiquant l'emplacement sur une carte.
– Il est obligatoire que le propriétaire "refuse expressément" la fonction de désactivation du dispositif, mais il est tenu de "donner son accord" par défaut.
– Pendant le démarrage initial et la configuration du dispositif mobile, il est recommandé de dispenser au propriétaire une brève formation pratique, afin de le sensibiliser aux règles générales de sécurité à respecter lors de l'utilisation et du stockage du nouveau dispositif Il devrait être nécessaire de suivre cette formation pratique jusqu'au bout avant l'activation du service.
– Il est recommandé que le propriétaire du dispositif soit à même d'accéder à une fonction de désactivation du dispositif et de demander une telle fonction en ayant recours à des capacités de libre-service, sans qu'il soit nécessaire de passer par l'opérateur de réseau
– Il est recommandé qu'un propriétaire de dispositif ne puisse réactiver un dispositif si celui-ci a été désactivé par l'opérateur.
– Le propriétaire peut demander une fonctionnalité destinée à sauvegarder toutes les données du dispositif qui appartiennent au propriétaire (données personnelle) dans un serveur de réseau sécurisé.
– Le propriétaire doit impérativement avoir la possibilité de rendre inaccessibles à distance toutes les données du dispositif.
– Le propriétaire doit impérativement avoir la possibilité de supprimer à distance les données de l'utilisateur (par exemple des images, des vidéos, un répertoire téléphonique, des messages électroniques) se trouvant dans le dispositif. Si les données de l'utilisateur sont fortement chiffrées, il suffit de supprimer la clé de chiffrement du dispositif.
– En cas de dispositifs volés ou perdus enregistrés sur un réseau visité (itinérance), le propriétaire pourra être informé que des coûts additionnels seront à sa charge s'il souhaite demander des fonctions de sauvegarde des données, de désactivation du dispositif ou de rétablissement de celui-ci.

– Il est obligatoire qu'un utilisateur non autorisé ne puisse accéder aux fonctions d'un dispositif désactivé ou aux données se trouvant dans ce dispositif.

– Une fonction permettant d'afficher un message personnalisé sur l'écran d'accueil/écran verrouiller du dispositif, lorsque le dispositif n'est pas en possession du propriétaire, devrait être mise à la disposition du propriétaire.

I.2 Serveur

– Un opérateur de réseau doit impérativement authentifier une demande émanant du propriétaire d'un dispositif avant de lancer la désactivation d'un dispositif.

– La demande d'un propriétaire visant à désactiver un dispositif doit impérativement être authentifiée et n'est requise que pour commander le dispositif qui est enregistré pour ce propriétaire.

– L'emplacement des serveurs prenants en charge la fonction de désactivation et l'accès à ces serveurs doit impérativement être sécurisé.

– Il est recommandé que seul le personnel autorisé possédant une formation suffisante puisse accéder aux fonctions de désactivation et demander ces fonctions.

– Le serveur doit impérativement créer et conserver des journaux de toutes les demandes de désactivation reçues.

– Lors du rétablissement du service d'un dispositif réactivé qui était auparavant désactivé, les données et les applications sauvegardées du propriétaire doivent impérativement être rétablies dans le dispositif.

– Les données du propriétaire qui ont été sauvegardées doivent impérativement être stockées en toute sécurité et la confidentialité ainsi que l'intégrité des données doivent être garanties.

– Une fois qu'un propriétaire a demandé la désactivation de son dispositif, il peut s'attendre que la fonction procède à l'exécution en moins de 15 minutes, si le dispositif peut être authentifié avec succès.

– Le rétablissement de la configuration d'origine ne peut servir à contourner des mesures de protection contre le vol.

I.3 Dispositif mobile

– Il faut impérativement vérifier que la demande de désactivation d'un dispositif est authentique avant de passer aux prochaines étapes en vue de la désactivation du dispositif.

– Le mécanisme de désactivation d'un dispositif mobile doit impérativement être exécuté depuis un serveur autorisé prenant en charge la fonction de désactivation. Afin de satisfaire à cette exigence, les mesures suivantes sont nécessaires:

  • connexion sécurisée entre le dispositif et le serveur;

  • authentification du dispositif par le serveur;

  • authentification du serveur par le dispositif, le serveur étant autorisé à exécuter la fonction.

– Le dispositif mobile, lors du démarrage et de la configuration initiale, est tenu de guider expressément le propriétaire tout au long de la configuration des fonctionnalités de protection contre le vol ainsi que des autres fonctions de sécurité pertinentes, par exemple les mécanismes de commande d'accès du dispositif.

– Le dispositif doit impérativement être capable de faire réactiver le service par le propriétaire légitime après celui-ci a été désactivé. Il ne doit pas pouvoir être réactivé par quiconque autre que le propriétaire légitime.

– Il est recommandé que la fonction de désactivation du dispositif soit utilisable lorsqu'un dispositif n'est pas connecté à un réseau mobile terrestre public, mais à l'Internet.

– En cas de dispositif perdu ou volé enregistré dans un réseau visité (itinérance), toutes les fonctions de sauvegarde des données, de désactivation du dispositif et de rétablissement du dispositif doivent impérativement fonctionner de manière satisfaisante.

I.4 Fabrication du dispositif

– Il est recommandé aux fabricants de dispositifs de poursuivre la mise en oeuvre et de concevoir des mesures pour décourager et empêcher la réinitialisation non autorisée d'un dispositif perdu ou volé à un état dans lequel il peut être utilisé par une personne autre que le propriétaire.

Appendice II

Exigences de sécurité additionnelles applicables à la protection contre le vol

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.).

II.1 Exigences applicables au serveur de sauvegarde

– Le mécanisme doit impérativement être exécuté depuis un serveur de sauvegarde prenant en charge le stockage des informations PII des dispositifs mobiles volés/perdus. Afin de satisfaire ces exigences, les mesures suivantes sont nécessaires:

- connexion sécurisée entre le dispositif et le serveur de sauvegarde;
- authentification du dispositif mobile par le serveur de sauvegarde;
- authentification du serveur de sauvegarde par le dispositif.

Appendice III

Menaces propres à la protection contre le vol

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

III.1 Menaces entre le propriétaire du dispositif mobile et le serveur autorisé

– Usurpation de l'identité du propriétaire du dispositif. Une instruction de désactivation inappropriée est transmise au serveur autorisé par un attaquant qui usurpe l'identité du propriétaire du dispositif. Une attaque exploitant cette menace peut entraîner la désactivation de dispositifs mobiles innocents.

– Altération volontaire/écoute illicite/répétition d'un message. Une instruction de désactivation inappropriée est transmise au serveur autorisé; le contenu du message d'instruction est révélé à l'attaquant qui est capable d'écouter clandestinement la communication, ou un volume de trafic considérable est envoyé, ce qui entraîne une attaque par déni de service réparti (DDoS) contre le serveur autorisé.

– Usurpation de l'identité du serveur autorisé. Un justificatif d'authentification du propriétaire du dispositif légitime est révélé ou une instruction de désactivation du propriétaire du dispositif légitime est transmise au serveur autorisé dont l'identité est usurpée. L'attaque qui exploite cette menace peut entraîner la désactivation de dispositifs mobiles innocents.

III.2 Menaces entre le serveur autorisé et l'agent de désactivation de la protection contre le vol

– Usurpation de l'identité du serveur d'authentification. Une instruction de désactivation inappropriée est transmise au dispositif mobile volé.

– Altération volontaire/écoute illicite/répétition d'un message. Une instruction de désactivation inappropriée est transmise à l'agent de désactivation des mesures de protection contre le vol; le contenu du message d'instruction est révélé à l'attaquant, qui peut écouter clandestinement la communication, ou un volume de trafic considérable est envoyé, ce qui entraîne une attaque par déni de service réparti (DDoS) contre l'agent de désactivation.

– Usurpation de l'identité de l'agent de désactivation. Un justificatif d'authentification du serveur autorisé légitime est révélé ou une instruction de désactivation du propriétaire du dispositif légitime est transmise à l'agent de désactivation dont l'identité est usurpée.

III.3 Menaces entre l'agent de désactivation de la protection contre le vol et le serveur de sauvegarde

– Usurpation de l'identité de l'agent de désactivation de la protection contre le vol. Le message de sauvegarde stocké dans le serveur de sauvegarde est révélé à l'agent de désactivation dont l'identité est usurpée.

– Altération volontaire/écoute illicite/répétition d'un message. L'information de sauvegarde est altérée et est révélée à l'attaquant, qui est en mesure d'écouter clandestinement la communication.

– Usurpation de l'identité du serveur de sauvegarde. L'information de sauvegarde est révélée au serveur de sauvegarde dont l'identité est usurpée.

Appendice IV

Scenario relatif aux mesures de protection contre le vol

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

IV.1 Types de fonctions de désactivation du dispositif mobile

Il existe deux types de fonctions de désactivation:

1) une fonction de désactivation "stricte", qui rend un dispositif mobile volé inutilisable en permanence;
2) une fonction de désactivation "souple" qui rend uniquement un dispositif mobile inutilisable par un "utilisateur non autorisé".

IV.2 Activation du dispositif mobile volé/perdu

Les fonctionnalités de protection contre le vol nécessitent la participation active du propriétaire du dispositif mobile. Lorsqu'un propriétaire de dispositif achète un nouveau dispositif mobile et souscrit un abonnement auprès d'un prestataire de communications cellulaires, il doit configurer le dispositif mobile afin d'activer la fonction de protection contre le vol.

IV.3 Scénario de désactivation du dispositif mobile volé/perdu

Si un téléphone mobile est volé ou perdu, le propriétaire du dispositif se met en rapport avec son fournisseur de services cellulaires ou utilise un site web exploité par l'opérateur de téléphonie cellulaire, appelé serveur autorisé, pour envoyer une instruction de "désactivation du dispositif" au dispositif mobile. Cette instruction verrouillera le dispositif mobile et, si le propriétaire du dispositif le souhaite, pourra également effacer certaines données personnelles du dispositif mobile ou permettre au serveur de sauvegarde de stocker certaines données personnelles.

L'instruction de désactivation du dispositif rendra inutilisable le dispositif sur le réseau d'un fournisseur de services mobiles commerciaux ou d'un service de données mobiles commerciales dans le monde entier, même si le dispositif est éteint ou si son support de stockage des données a été supprimé.

Le seul moyen de rétablir un dispositif verrouillé sera un mot de passe fourni par le propriétaire du téléphone.

Appendice V

Profil de protocole TLS pour les mesures de protection contre le vol

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

On trouvera dans le présent Appendice un profil minimal de protocole TLS pour les mesures de protection contre le vol. L'exemple type du profil de protocole TLS est donné dans les normes [b-IETF RFC 6460] et [b-ISO/CEI 20648].

V.1 Exigences relatives au protocole TLS

– Il est recommandé que le dispositif de protection contre le vol faisant office de serveur mette en oeuvre le protocole TLS; cependant, son utilisation par les clients est facultative. Il est nécessaire de mettre en oeuvre la version 1.2 du protocole TLS (décrite dans la norme [b-IETF RFC 5246]) ou une version ultérieure.

V.2 Suites de chiffrement TLS pour l'interopérabilité

– Le dispositif de protection contre le vol ne doit pas utiliser l'algorithme MD5 ou SHA-1 en tant que code d'authentification de message avec hachage (HMAC) par défaut.

– Le dispositif de protection contre le vol ne doit pas utiliser l'algorithme RC4 comme algorithme cryptographique par défaut.

NOTE – La norme [b-IETF RFC 7465] interdit l'utilisation de l'algorithme RC4.

– Le dispositif de protection contre le vol doit impérativement prendre en charge: la sélection et l'utilisation de paires signature/ algorithme de hachage, au moyen des algorithmes de signature pris en charge dans la version 1.2 du protocole TLS, et l'utilisation de l'algorithme SHA-256 ou des valeurs de hachage de plus grande force.

– Le dispositif de protection contre le vol doit impérativement utiliser des suites de chiffrements offrant un niveau de sécurité d'au moins 112 bits. En outre, les suites de chiffrements ci-après doivent impérativement être prises en charge:

  • TLS_RSA_WITH_AES_128_CBC_SHA256 {0x00, 0x3C}.

V.3 Certificats numériques

Le dispositif de protection contre le vol doit impérativement prendre en charge des certificats de clé publique [b-UIT-T X.509] (version 3) qui sont conformes au profil de certificat et au profil d'extension de certificat définis dans la norme [b-IETF RFC 5280].

– Le serveur TLS du dispositif de protection contre le vol doit impérativement prendre en charge les certificats du serveur.

– Il est recommandé que le client TLS du dispositif de protection contre le vol prenne en charge les certificats du client.

– Le dispositif de protection contre le vol doit impérativement prendre en charge des dimensions de clés d'au moins 2048 bits, pour les certificats [b-UIT-T X.509] du serveur RSA/DSA.

– Le dispositif de protection contre le vol doit impérativement prendre en charge les formats de certificat [b-UIT-T X.509] codés selon les règles de codage distinctives (DER), [b-UIT-T X.509] codés au format base64 et [b-IETF RFC 7292] PKCS#12.

– Le dispositif de protection contre le vol doit impérativement prendre en charge la validation de certificat décrit au § 6 de la norme [IETF RFC 5280], qui se présente sous la forme d'un certificat numérique. En outre, l'une des approches ci-après doit être utilisée pour déterminer si un certificat a été supprimé:

- Option 1: utilisation de listes de révocation de certificats (CRL): listes CRL prises en charge dans le format [b-UIT-T X.509] codé selon les règles DER ou [b-UIT-T X.509] codé au format base64 et listes CRL stockées localement (la distribution n'entre pas dans le cadre de cette norme) ou extraites depuis une source extérieure (par exemple un point de distribution de liste CRL (CRLDP)).
- Option 2: utilisation d'un protocole ayant le statut de certificat, par exemple un protocole de statut du certificat en ligne (OCSP) selon l'une des modalités suivantes: utiliser directement le protocole OCSP décrit dans la norme [b-IETF RFC 6960] et utiliser indirectement le protocole OCSP par l'intermédiaire de l'extension de demande de statut de certificat au protocole TLS décrit au § 8 de la norme [b-IETF RFC 6066].

Appendice VI

Aperçu de la gestion des dispositifs OMA

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le présent Appendice donne un aperçu du protocole de gestion des dispositifs(DM) défini dans le document OMA [b-OMA-DM].

VI.1 Spécification de la gestion des dispositifs OMA

La spécification de la gestion des dispositifs OMA est conçue pour la gestion de dispositifs mobiles tels que les téléphones mobiles, les assistants numériques personnels (PDA) ou les tablettes informatiques. La gestion des dispositifs vise à prendre en charge les utilisations suivantes:

– Fourniture: configuration du dispositif (y compris une première utilisation), fonctions d'activation et de désactivation.

– Configuration du dispositif: permet d'apporter des modifications à la configuration et aux paramètres du dispositif.

– Mises à jour logicielles: permet de télécharger de nouveaux logiciels et/ou de corriger des erreurs dans le dispositif, y compris des applications et des logiciels de systèmes.

– Gestion des défaillances: permet de signaler des erreurs dans le dispositif et de consulter l'état du dispositif.

Toutes les fonctions ci-dessus sont prises en charge par la spécification de la gestion des dispositifs OMA et un dispositif peut mettre en oeuvre, à titre facultatif, toutes ses fonctions ou un sous-ensemble d'entre elles. Etant donné que la spécification de la gestion des dispositifs OMA est destinée aux dispositifs mobiles, elle est conçue de façon à tenir compte tout particulièrement des éléments suivants:

– Dispositifs peu encombrants, dans lesquels l'espace mémoire et l'espace de stockage peuvent être limités.

– Limitation de la largeur de bande de la communication, par exemple pour la connectivité sans fil.

– Sécurité très stricte, étant donné que les dispositifs sont vulnérables aux attaques logicielles; l'authentification et les problèmes font partie intégrante des spécifications.

Bibliographie

[b-UIT-T X.509] Recommandation UIT-T X.509 (2012), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

[b-UIT-T X.1158] Recommandation UIT-T X.1158 (2014), *Mécanismes d'authentification à plusieurs facteurs utilisant un dispositif mobile*.

[b-UIT-T X.1250] Recommandation UIT-T X.1250 (2009), *Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité*.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

[b-UIT-T X-Sup.19] Recommandations UIT-T de la série X – *Supplément 19 (2013), Supplément sur les aspects relatifs à la sécurité des smartphones*.

[b-ISO/CEI 20648] ISO/CEI 20648:2016, *Technologies de l'information – Spécification TLS pour les systèmes de stockage*.

[b-ISO/CEI 27000] ISO/CEI 27000:2016, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2009, *Technologies de l'information – Sécurité de réseau – Partie 1: Vue d'ensemble et concepts*.

[b-3GPP TS 22.048] 3GPP TS 22.048 (2003), *Security mechanisms for the (U)SIM Application Toolkit*, juin 2003.

[b-3GPP TS 33.102] 3GPP TS 33.102 (2009), *3G Security; Security architecture (Release 9)*, décembre 2009.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *Version 1.2 du protocole de sécurité de la couche Transport (TLS)*.

[b-IETF RFC 5280] IETF RFC 5280 (2008), *Certificat et profil de liste de révocation de certificat (CRL) de l'infrastructure de clé publique Internet X.509*.

[b-IETF RFC 6066] IETF RFC 6066 (2011), *Transport Layer Security (TLS) Extensions: Extension Definitions*.

[b-IETF RFC 6460] IETF RFC 6460 (2012), *Suite B Profile for Transport Layer Security (TLS).*

[b-IETF RFC 6960] IETF RFC 6960 (2013), *ITU-T X.509 Internet Public Key Infrastructure Online Certificate Status Protocol -– OCSP*.

[b-IETF RFC 7292] IETF RFC 7292 (2015), *PKCS #12 Personal Information Exchange Syntax v1.1*.

[b-IETF RFC 7465] IETF RFC 7465 (2015), *Prohibiting RC4 Cipher Suites*.

[b-GSMA] GSMA, *SG.24 Anti-Theft Device Feature Requirements v3.0*, 17 mai 2016.

[b-OMA-DM] Open Mobile Alliance, *OMA Device Management V1.2*, avril 2013.

[b-NIST SP 800-88] NIST, *NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization*, décembre 2014.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changements climatiques, déchets d'équipements électriques et électroniques, efficacité énergétique, 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	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation et mesures et tests associés
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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2018