Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2740

(01/2011)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

Réseaux de prochaine génération – Sécurité

Spécifications de sécurité applicables aux transactions financières mobiles à distance dans les réseaux de prochaine génération

Recommandation UIT-T Y.2740

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
Réseaux futurs	Y.3000–Y.3099

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

Recommandation UIT-T Y.2740

Spécifications de sécurité applicables aux transactions financières mobiles à distance dans les réseaux de prochaine génération

Résumé

Au cours des dernières années, des réseaux de paiement à distance très divers utilisant des réseaux mobiles ont été créés. S'ils mettent en pratique des stratégies différentes, ces réseaux sont bien souvent insuffisamment sécurisés. Dans le même temps, les réseaux de communication, notamment les réseaux mobiles, connaissent d'importants changements en évoluant vers les réseaux de prochaine génération (NGN).

Dans la présente Recommandation, on définit différentes stratégies visant à mettre au point la sécurité des systèmes pour le commerce mobile et les services bancaires mobiles dans les réseaux de prochaine génération. On définit quatre niveaux de sécurité et décrit, pour chacun d'eux, les spécifications de sécurité applicables au commerce mobile et aux services bancaires mobiles. On expose les risques probables liés au commerce mobile et aux services bancaires mobiles et précise les moyens permettant de réduire ces risques.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2740	2011-01-28	13

Mots clés

Commerce mobile, paiements à distance, paiements mobiles, sécurité, services bancaires mobiles.

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/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2740

Spécifications de sécurité applicables aux transactions financières mobiles à distance dans les réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation contient une description des risques de sécurité associés aux transactions financières mobiles à distance prises en charge dans les réseaux de prochaine génération (NGN) et spécifie des mesures permettant d'atténuer et de combattre ces risques, sur la base de quatre niveaux de sécurité. Elle énonce aussi les spécifications minimales requises pour la protection de la confidentialité des données personnelles des individus concernant les transactions financières mobiles à distance.

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

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

[UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité des réseaux NGN*.

[UIT-T Y.2741] Recommandation UIT-T Y.2741 (2011), *Architecture de sécurité applicable aux transactions financières mobiles dans les réseaux de prochaine génération*.

3 Définitions

3.1 Termes définis ailleurs

Dans la présente Recommandation, on utilise les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [UIT-T X.800]: précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.

3.1.2 application [UIT-T Y.2741]: application spéciale de services bancaires mobiles ou de commerce mobile téléchargée sur les appareils mobiles des clients (utilisateurs).

3.1.3 authentification [UIT-T X.800]: voir "authentification de l'origine des données" et "authentification de l'entité homologue".

NOTE – Dans la présente Recommandation, le terme "authentification" n'est pas associé à l'intégrité des données; le terme "intégrité des données" est utilisé à la place.

3.1.4 disponibilité [UIT-T X.800]: propriété d'être accessible et utilisable sur demande par une entité autorisée.

3.1.5 client [UIT-T Y.2741]: particulier ou personne morale ayant signé un accord contractuel portant sur l'utilisation de services de télécommunication et du système de commerce mobile.

3.1.6 confidentialité [UIT-T X.800]: propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

3.1.7 intégrité des données [UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.8 authentification de l'origine des données [UIT-T X.800]: confirmation que la source des données reçues est telle que déclarée.

3.1.9 système de paiement mobile [UIT-T Y.2741]: système de services bancaires mobiles et/ou de commerce mobile.

3.1.10 réseau de prochaine génération (NGN) [b-UIT-T Y.2001]: réseau en mode paquet, en mesure d'assurer des services de télécommunication et d'utiliser de multiples technologies de transport à large bande à qualité de service imposée et dans lequel les fonctions liées aux services sont indépendantes des technologies sous-jacentes liées au transport. Il assure le libre accès des utilisateurs aux réseaux et aux services ou fournisseurs de services concurrents de leur choix. Il prend en charge la mobilité généralisée qui permet la fourniture cohérente et partout à la fois des services aux utilisateurs.

3.1.11 respect de la vie privée [UIT-T X.800]: droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées.

NOTE – Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité.

3.1.12 répudiation [UIT-T X.800]: le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie.

3.1.13 mesure de sécurité [UIT-T X.805]: ensemble de dispositions de sécurité conçues pour prendre en compte un aspect particulier de la sécurité du réseau.

3.1.14 couche de sécurité [UIT-T X.805]: hiérarchie de l'équipement du réseau et des groupes d'équipements.

3.1.15 plans de sécurité [UIT-T X.805]: type d'activité dans le réseau, protégée par les mesures de sécurité.

3.2 Termes définis dans la présente Recommandation

Dans la présente Recommandation, on utilise le terme suivant:

3.2.1 niveau de sécurité: prescription de sécurité du système définissant l'efficacité de la protection contre les risques.

4 Abréviations et acronymes

Dans la présente Recommandation, on utilise les abréviations et acronymes suivants:

GSM système mondial de communications mobiles (*global system for mobile communications*)

MPS système de paiement mobile (*mobile payment system*)

MSISDN numéro RNIS international d'abonné mobile

NGN réseau de prochaine génération

PA-DSS norme de sécurité des données d'application de paiement (*payment application data security standard*)

PCI DSS norme de sécurité des données du secteur des cartes de paiement (*payment card industry data security standard*)

5 Conventions

Aucune.

6 Considérations relatives à la sécurité du commerce mobile et des services bancaires mobiles dans les NGN

La sécurité des systèmes de paiement mobile (MPS) dans les réseaux de prochaine génération (NGN) repose sur l'architecture du système MPS et sur les rôles des différents participants à ce système définis dans la Recommandation UIT-T Y.2741 "Architecture de sécurité applicable aux transactions financières mobiles dans les réseaux de prochaine génération" ainsi que sur l'analyse des risques qui se posent pour les participants au système MPS, présentée ci-après.

6.1 Risques fondamentaux liés aux transactions financières mobiles à distance

Le présent paragraphe ne porte pas sur les facteurs à l'origine de nouveaux risques mondiaux pour le secteur qui découlent de la mise en œuvre du système MPS par les participants, à savoir les risques stratégiques et juridiques et les risques affectant la souveraineté nationale, les marchés, les intérêts, les liquidités, la réputation, etc. Le présent paragraphe traite des risques touchant les informations qui peuvent survenir directement au moment de la réalisation de paiements mobiles à distance et qui nécessitent la mise en place de solutions de sécurité pour être réduits le plus possible:

- le risque de perte de confidentialité, autrement dit d'accès non autorisé à des informations confidentielles;
- le risque de violation de l'intégrité des données, autrement dit d'altération des informations au cours de leur transfert ou de leur traitement;
- le risque de falsification de documents électroniques (risque de non-authenticité), autrement dit de production de documents électroniques par des participants non autorisés;
- le risque de répudiation, autrement dit de déni d'être l'auteur d'un document électronique;
- le risque de destruction d'informations, à dessein ou par suite de négligences;
- le risque transactionnel, autrement dit l'incapacité de finir ou d'achever une transaction (par exemple en raison d'une mauvaise qualité de transmission).

6.2 Objectifs liés à la sécurité

Pour améliorer la sécurité des paiements mobiles et réduire le plus possible les risques qui se posent pour les participants, la solution doit permettre d'atteindre les objectifs suivants:

- réduire la possibilité d'interception d'informations personnelles ou financières au moment d'une transaction;
- réduire la possibilité d'extraction d'informations personnelles ou financières se trouvant dans des bases de données;
- réduire la possibilité de remplacement ou d'altération d'informations personnelles ou financières au moment d'une transaction;
- réduire la possibilité d'utilisation de la solution par des personnes non autorisées ou par des personnes tentant d'usurper l'identité d'autres personnes, en mettant en place une authentification unique;

- réduire la possibilité d'utilisation d'informations "volées" dans la solution;
- faire en sorte qu'il soit impossible pour la personne à l'origine d'une transaction ou pour un participant à une transaction de nier ultérieurement leurs actes;
- faire en sorte que tous les participants intermédiaires respectent les droits et obligations prévus par la loi;
- faire en sorte que la transaction se déroule complètement.

6.3 Niveaux de sécurité et moyens permettant de les prendre en charge

Dans la présente Recommandation, on définit quatre niveaux de sécurité du système MPS, sur la base de l'analyse des risques qui se posent pour les participants à ce système.

Le niveau de sécurité du système MPS est défini par l'ensemble des mises en œuvre des mesures de sécurité (voir Tableau 1). Ainsi, pour le quatrième niveau de sécurité (niveau le plus élevé), le système doit présenter le degré maximal de mise en œuvre des mesures de sécurité. Cependant, pour certaines mesures de sécurité, les exigences sont unifiées pour tous les niveaux de sécurité.

Les parties utilisant le système MPS doivent connaître le niveau de sécurité ainsi que les risques du système.

Le niveau de sécurité acceptable pour un certain risque associé à un composant donné du système est déterminé par la partie qui prend le risque en question.

Les parties peuvent de plus atténuer les risques liés à l'utilisation du système MPS par la mise en place de mesures d'exploitation qui peuvent notamment viser à limiter la fréquence ou le montant de transactions individuelles, à fournir le service aux seuls utilisateurs dont le niveau de loyauté est élevé, etc.

Le client s'identifie auprès du système MPS en utilisant un identificateur public de réseau NGN (par exemple un numéro MSISDN pour les réseaux GSM).

6.3.1 Mise en œuvre des mesures de sécurité pour tous les niveaux de sécurité

La sécurité du système MPS dépend de chaque participant au système et est obtenue grâce aux moyens physiques et administratifs mis en place pour garantir la sécurité lors du transfert, du traitement et du stockage des données. Les participants au système doivent mettre en œuvre les normes du secteur relatives à la garantie de la sécurité des informations (par exemple [b-PCI DSS], [b-PA-DSS] et autres normes).

Les huit mesures de sécurité [UIT-T X.805] utilisées pour définir les niveaux de sécurité du système MPS sont énumérées ci-après. Il est obligatoire que tous les participants au système mettent en œuvre les mesures de sécurité en rapport avec les informations échangées.

1) Contrôle d'accès: l'accès à chaque composant du système MPS ne doit être accordé que conformément au niveau d'accès défini pour les utilisateurs finals ou pour le personnel du système. Cette exigence est valable pour tous les niveaux de sécurité.

2) Authentification: l'authenticité de l'identité déclarée des entités participantes doit être vérifiée. Il s'agit de l'un des principaux facteurs permettant de réduire le risque de déni d'une personne d'être l'auteur de ses actes. En raison du grand nombre de possibilités de mise en œuvre organisationnelle et technique, les exigences minimales en termes de mécanismes d'authentification sont définies pour chaque niveau de sécurité.

   Les trois facteurs d'authentification du client (de l'utilisateur) sont les suivants:

   – le client utilise des informations que personne d'autre ne peut connaître, par exemple un mot de passe (quelque chose que le client connaît);

– le client possède quelque chose qui est à sa seule disposition et réalise certaines actions de manière univoque, par exemple il génère une signature électronique ou un code d'authentification de message (quelque chose que le client possède);
– le client utilise ses données biométriques (quelque chose qui distingue le client).

3) Non-répudiation: des moyens sont mis en place pour éviter qu'une personne ou une entité nie avoir réalisé une action particulière (par exemple avoir envoyé, transféré ou reçu des messages). Pour cela, toutes les actions des utilisateurs finals et du personnel du système font l'objet d'un enregistrement obligatoire. Les journaux d'événements ne doivent pas pouvoir être modifiés et doivent consigner toutes les actions de tous les utilisateurs. Le respect des exigences est obtenu grâce à des moyens définis par la législation ou dans des contrats mutuels et à des mécanismes d'authentification acceptés. Cette exigence est valable pour tous les niveaux de sécurité.

4) Confidentialité des données: les données utilisées dans le système sont protégées contre toute divulgation non autorisée et contre toute altération. Les exigences en matière de confidentialité sont définies sur la base de la criticité des données du système. Pour chaque niveau de sécurité, on spécifie certains moyens à mettre en place pour garantir la confidentialité et on impose des restrictions concernant le niveau de criticité des données du système.

5) Sécurité de la communication: la remise garantie d'une suite de messages dans les deux directions (vers le destinataire et vers l'expéditeur) comprend l'achèvement d'une transaction (grâce aux protocoles garantissant l'achèvement d'une transaction) et la protection des informations contre toute divulgation non autorisée au moment du transfert sur les canaux de communication. Cette exigence est valable pour tous les niveaux de sécurité.

6) Intégrité des données: l'exactitude, la précision et l'intégrité des données sont garanties grâce à la protection contre toutes modifications, suppressions, créations et reproductions non autorisées ainsi qu'à l'indication de ces activités non autorisées. L'achèvement logique d'une transaction est garanti lorsque certaines conditions sont satisfaites, la mise en œuvre se faisant au niveau application. Pour chaque niveau de sécurité, on définit certains mécanismes de garantie de l'intégrité. La garantie de l'intégrité peut être obtenue grâce à la confidentialité des données et au contrôle d'accès.

7) Disponibilité: cette mesure de sécurité vise à garantir que les personnes autorisées aient toujours accès aux données et services du système MPS. Cette exigence est valable pour tous les niveaux de sécurité et le fournisseur de services doit faire au mieux pour s'y conformer.

8) Respect de la vie privée: cette mesure de sécurité vise à garantir la sécurité des informations échangées et stockées par les participants au système. Le nombre minimal de données nécessaires pour que le système fonctionne doit être utilisé dans la solution. Les participants au système doivent empêcher l'acquisition et le transfert non autorisés des données. Le système doit garantir le respect des normes du secteur financier.

Les mesures de sécurité dont la mise en œuvre est la même pour tous les niveaux de sécurité sont les suivantes:

– contrôle d'accès;
– non-répudiation;
– sécurité de la communication;
– disponibilité.

Les mesures de sécurité suivantes ont une mise en œuvre différente suivant le niveau de sécurité:

– authentification;
– confidentialité des données;
– intégrité des données;
– respect de la vie privée.

6.3.2 Niveau de sécurité 1

Le système MPS se base sur l'authentification du client assurée par l'opérateur NGN.

La confidentialité et l'intégrité des données sont garanties par l'environnement de transfert des données (sécurité des communications) et au moment de leur stockage et de leur traitement, leur confidentialité et leur intégrité sont garanties par le mécanisme de stockage des données et par les moyens de contrôle d'accès au système.

Le respect de la vie privée est garanti par l'absence de données sensibles dans les messages transférés ainsi que par la mise en œuvre des mécanismes requis de stockage des données et des moyens de contrôle d'accès au système. Les composants du système ne doivent pas offrir de possibilités latentes d'acquisition et de transfert de données sans autorisation.

6.3.3 Niveau de sécurité 2

Pour l'utilisation des services du système, l'authentification peut être exécutée en utilisant un seul facteur d'authentification et peut donc être mise en œuvre sans l'application de protocoles cryptographiques.

Pour l'authentification, on utilise un mot de passe à usage unique, qui est généré au moyen de divers jetons (dispositif à un seul facteur correspondant à un mot de passe à usage unique, dispositif à un seul facteur correspondant au chiffrement, etc.).

La confidentialité et l'intégrité des données et le respect de la vie privée sont garantis de manière analogue au niveau 1.

6.3.4 Niveau de sécurité 3

Il faut utiliser une authentification de client à plusieurs facteurs pour l'accès aux services du système.

Le système doit utiliser plusieurs facteurs d'authentification pour authentifier le client.

Au moment du transfert des messages, la confidentialité et l'intégrité des données et le respect de la vie privée doivent être garantis grâce à un mécanisme additionnel de chiffrement des messages et à des protocoles de transfert de données qui garantissent la sécurité des données transférées par les participants intermédiaires (y compris la vérification de l'intégrité des données). Au moment du stockage et du traitement des données, leur confidentialité et leur intégrité et le respect de la vie privée sont garantis grâce à des mécanismes additionnels de chiffrement et de masquage ainsi qu'à une distribution bien définie de l'accès conformément aux privilèges et aux autorisations.

Afin de respecter les exigences de sécurité à ce niveau, le système doit utiliser des applications logicielles spéciales téléchargées sur les appareils mobiles des clients. Ces applications doivent mettre en œuvre une authentification à deux facteurs et assurer à la fois le chiffrement et le déchiffrement des données transférées.

Pour chaque authentification, il faut saisir le mot de passe ou d'autres données d'activation afin d'activer la clé d'authentification, et la copie non chiffrée de la clé d'authentification doit être effacée après chaque authentification (jeton cryptographique logiciel à plusieurs facteurs).

Tous les participants intermédiaires au système MPS doivent utiliser des moyens de sécurité qui protègent le système contre les interruptions. Dans les solutions du niveau 3, la sécurité des données

transférées sur les canaux de communication doit être assurée par des moyens cryptographiques puissants. La puissance d'une méthode cryptographique dépend de la clé de chiffrement utilisée. La longueur effective de la clé doit respecter les recommandations relatives à la longueur minimale correspondant à une puissance relative donnée.

6.3.5 Niveau de sécurité 4

C'est le niveau le plus élevé de sécurité du système. Afin de respecter les exigences de sécurité à ce niveau, le système doit utiliser des modules de sécurité matériels installés dans les appareils mobiles des clients. Ces modules de sécurité matériels doivent mettre en œuvre une authentification à deux facteurs et assurer à la fois le chiffrement et le déchiffrement des données transférées. Pour chaque authentification, il faut saisir le mot de passe ou d'autres données d'activation afin d'activer la clé d'authentification, et la copie non chiffrée de la clé d'authentification doit être effacée après chaque authentification (jeton cryptographique matériel à plusieurs facteurs). Pour le chiffrement des messages, on utilise aussi bien des algorithmes de chiffrement symétriques que des algorithmes de chiffrement asymétriques.

La mise en œuvre des autres mesures de sécurité doit correspondre entièrement au niveau 3.

Tableau 1 – Relation entre niveaux de sécurité et mise en œuvre des mesures de sécurité

Mesure de sécurité	**Niveau de sécurité**			
	Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
Contrôle d'accès	L'accès à chaque composant du système ne doit être accordé qu'aux membres autorisés du personnel du système. L'activation des applications spéciales téléchargées sur les terminaux mobiles ne devrait être permise que pour les clients autorisés.			
Authentification	L'authentification dans le système est assurée par l'environnement de transfert des données NGN.	Authentification à un seul facteur pour l'utilisation des services du système.	Authentification à plusieurs facteurs pour l'utilisation des services du système.	Abonnement en personne aux services, pour lequel sont utilisées des données personnelles avec identification obligatoire. Authentification à plusieurs facteurs pour l'utilisation des services du système. Obligation d'utiliser un module cryptographique matériel.
Non-répudiation	L'impossibilité pour la personne à l'origine d'une transaction ou pour un participant à une transaction de nier ultérieurement leurs actes est garantie grâce à des contrats juridiques explicites et implicites définis par la législation ou dans des contrats mutuels et à des mécanismes d'authentification acceptés. Toutes les actions des utilisateurs finals et du personnel du système doivent être journalisées. Les journaux d'événements ne doivent pas pouvoir être modifiés et doivent consigner toutes les actions de tous les utilisateurs.			

Tableau 1 – Relation entre niveaux de sécurité et mise en œuvre des mesures de sécurité

<table>
<tr><th rowspan="2">Mesure de sécurité</th><th colspan="4">Niveau de sécurité</th></tr>
<tr><th>Niveau 1</th><th>Niveau 2</th><th>Niveau 3</th><th>Niveau 4</th></tr>
<tr><td>Confidentialité des données</td><td colspan="2" rowspan="2">Au moment du transfert des données, la confidentialité de celles-ci est garantie par l'environnement de transfert des données (sécurité des communications) et au moment de leur stockage et de leur traitement, leur confidentialité est garantie par le mécanisme de stockage des données et par les moyens de contrôle d'accès au système.</td><td rowspan="3">Au moment du transfert des messages, la confidentialité des données est garantie grâce à un mécanisme additionnel de chiffrement des messages et à des protocoles de transfert de données qui garantissent la sécurité des données transférées par les participants intermédiaires (y compris la vérification de l'intégrité des données); au moment du stockage et du traitement des données, leur confidentialité et leur intégrité et le respect de la vie privée sont garantis grâce à des mécanismes additionnels de chiffrement et de masquage ainsi qu'à une distribution bien définie de l'accès conformément aux privilèges et aux autorisations.</td><td rowspan="3">Mise en œuvre des exigences du niveau 3 avec utilisation obligatoire de mécanismes matériels assurant le chiffrement et la sécurité des données côté client (module de chiffrement matériel).</td></tr>
<tr><td>Intégrité des données</td></tr>
<tr><td>Respect de la vie privée</td><td colspan="2">Le respect de la vie privée est garanti par l'absence de données sensibles dans les messages transférés ainsi que par la mise en œuvre des mécanismes requis de stockage des données et des moyens de contrôle d'accès au système.
Les composants du système ne doivent pas offrir de possibilités latentes d'acquisition et de transfert de données sans autorisation.</td></tr>
<tr><td>Sécurité de la communication</td><td colspan="4">La remise d'un message à son destinataire est garantie de même que la protection des informations contre toute divulgation non autorisée au moment du transfert sur les canaux de communication. Cette garantie est offerte par les fournisseurs NGN.</td></tr>
<tr><td>Disponibilité</td><td colspan="4">Il faut faire en sorte que les données et services du système soient toujours accessibles aux personnes qui sont autorisées à y accéder. La disponibilité est garantie par les fournisseurs NGN ainsi que par les fournisseurs de services MPS.</td></tr>
</table>

Bibliographie

[b-UIT-T Y.2001] Recommandation UIT-T Y.2001 (2004), *Aperçu général des réseaux de prochaine génération.*

[b-PA-DSS] Payment Card Industry (PCI), *Norme de sécurité des données d'application de paiement. Conditions et procédures d'évaluation de sécurité, Version 2.0, octobre 2010.*

[b-PCI DSS] Payment Card Industry (PCI), *Norme de sécurité des données. Conditions et procédures d'évaluation de sécurité, Version 2.0, octobre 2010.*

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	Terminaux et méthodes d'évaluation subjectives et objectives
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 prochaine génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2011