Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2741

(01/2011)

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

Réseaux de prochaine génération – Sécurité

Architecture de sécurité applicable aux transactions financières sur mobile dans les réseaux de prochaine génération

Recommandation UIT-T Y.2741

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.2741

Architecture de sécurité applicable aux transactions financières sur mobile dans les réseaux de prochaine génération

Résumé

La Recommandation UIT-T Y.2741 présente l'architecture générale d'une solution de sécurité applicable au commerce sur mobile et aux services bancaires sur mobile dans le contexte des réseaux NGN. Elle décrit les principaux participants et leurs rôles, ainsi que les scénarios de fonctionnement du commerce mobile et des services bancaires sur mobile. Cette Recommandation contient également des exemples de modèles de mise en œuvre du commerce mobile et des services bancaires sur mobile.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2741	2011-01-28	13

Mots clés

Paiements à distance, paiements sur mobile, services bancaires sur mobile, sûreté et sécurité, transactions bancaires sur mobile.

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 [avait/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.2741

Architecture de sécurité applicable aux transactions financières sur mobile dans les réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation définit l'architecture de sécurité applicable aux transactions financières sur mobile à distance pour les réseaux NGN. Sont exclues du domaine d'application toutes les autres transactions financières ainsi que les transactions qui utilisent des jetons monétaires ou non monétaires pour le transfert de valeur.

Les NGN permettent d'organiser une grande diversité de services avec une gestion souple et des fonctions de personnalisation et, ainsi, de faciliter l'accès aux services du système de paiement sur mobile (MPS).

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 Y.2740] Recommandation UIT-T Y.2740 (2011), *Spécifications de sécurité applicables aux transactions financières mobiles à distance dans les réseaux de prochaine génération*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants, définis ailleurs:

3.1.1 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.

3.2 Termes définis dans la présente Recommandation

Dans la présente Recommandation, les termes suivants sont définis:

3.2.1 application: application spéciale de commerce sur mobile ou de transaction bancaire sur mobile qui est téléchargée vers le dispositif mobile du client (de l'utilisateur).

3.2.2 compte bancaire: compte financier électronique détenu par une personne ou par une entreprise dans une banque ou dans une autre institution financière autorisée par l'autorité monétaire nationale (par exemple la banque centrale), qui peut être utilisé pour le paiement de biens et de services.

3.2.3 client: particulier ou personne morale qui a signé un accord contractuel sur l'utilisation de services de télécommunication et du système de commerce sur mobile.

3.2.4 transaction financière: événement ou clause faisant l'objet d'un contrat entre un acheteur et un vendeur pour effectuer un paiement par le biais de l'échange d'un élément d'actif.

3.2.5 environnement intersystèmes: ensemble de règles ou système permettant d'établir l'interaction de divers systèmes de services bancaires sur mobile et de commerce sur mobile.

3.2.6 dispositif mobile: dispositif électronique utilisé pour les télécommunications assurées sur des réseaux NGN sans fil.

3.2.7 transaction financière mobile: transaction financière lancée et/ou autorisée depuis un dispositif mobile.

3.2.8 système de paiement sur mobile (MPS): système regroupant les transactions bancaires sur mobile et/ou le commerce sur mobile.

3.2.9 jeton monétaire: objet électronique ou physique qui est utilisé pour le paiement et qui est représenté et mesuré dans l'unité monétaire nationale, mais qui n'est pas enregistré sur un compte bancaire ni lié directement à un compte bancaire.

Parmi les exemples de jetons monétaires électroniques, on peut citer l'argent électronique stocké dans un porte-monnaie électronique autonome, indépendant de tout compte bancaire. Parmi les exemples de jetons monétaires physiques, on peut citer les pièces de monnaie, les billets de banque, les chèques de voyage, etc.

3.2.10 jeton non monétaire: objet électronique ou physique qui est utilisé pour le paiement mais qui n'est pas représenté dans l'unité monétaire nationale. Parmi les exemples de jetons non monétaires électroniques, on peut citer les "minutes" ou les "messages SMS" non utilisés qui sont crédités sur des comptes d'abonnés NGN et que les opérateurs de réseau NGN autorisent à transférer d'un compte d'abonné à un autre.

3.2.11 identificateur de paiement: paramètre de demande requis qui identifie explicitement le destinataire du paiement. L'identificateur de marchand et l'identificateur de système de paiement sur mobile (MPS) (identificateur unique d'un système de paiement sur mobile) doivent être présents dans la mise en œuvre de l'environnement intersystèmes.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DB base de données (*database*)

ID identification

IS système informatique (*information system*)

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

NGN réseau de prochaine génération (*next generation work*)

5 Conventions

Néant.

6 Rôles, risques, participants et scénarios de paiements sur mobile dans les NGN

6.1 Rôles dans les systèmes de commerce sur mobile et de services bancaires sur mobile

Les rôles de base des participants au système MPS et les responsabilités correspondantes sont les suivants:

- Le client est un abonné mobile qui possède un instrument de paiement pour les opérations de paiement.
- L'application client est un logiciel spécial téléchargé dans le dispositif mobile du client (téléphone, carte SIM, communicateur, etc.) et conçu pour réaliser des opérations de paiement sur mobile en toute sécurité.
- L'instrument de paiement est un instrument financier utilisé pour effectuer le paiement de biens et de services.
- L'opérateur de réseau NGN offre un réseau de communication mobile utilisé pour l'interaction à distance du client avec le système MPS et pour le routage et le transfert de données.
- Le distributeur d'application client est un participant qui met des applications à la disposition des clients.
- Le fournisseur de sécurité est un participant qui assure la sécurité du transfert de données sur les canaux de communication.
- L'opérateur de système MPS (fournisseur de service, passerelle de paiement) est un participant qui assure l'interaction au sein du système MPS et offre des services de paiement à l'utilisateur final.
- L'émetteur est une institution financière qui émet des instruments de paiement.
- Le fournisseur d'authentification client valide les opérations du client.
- L'acquéreur est une institution financière qui entretient des relations avec le marchand, dont il reçoit toutes les transactions financières.
- Le système de paiement est une organisation qui assure des transactions de paiement interbancaires.

6.2 Risques et niveaux de sécurité dans le système MPS

Le présent paragraphe décrit les principaux risques pour la sécurité des informations qui peuvent surgir lorsque des paiements sur mobile à distance sont effectués. Ces risques sont notamment les suivants:

- Le risque de compromission de la confidentialité – accès de tiers non autorisés à des informations confidentielles.
- Le risque de compromission de l'intégrité – distorsion d'informations au cours de leur transfert ou de leur traitement.
- Le risque de falsification de documents électroniques – création d'un document par une partie non autorisée.
- Le risque de répudiation – fait de nier être l'auteur d'un document électronique.
- Le risque de destruction d'informations, à dessein ou par négligence.
- Le risque transactionnel – impossibilité de finir une transaction (par exemple, en raison d'une communication mobile instable).
- Quatre niveaux de sécurité, qui dépendent des mécanismes de sécurité mis en œuvre sur la base des risques, sont définis pour les systèmes (UIT-T Y.2740).

6.3 Participants et architecture du système

L'architecture MPS devrait être conforme au système déjà en place d'interrelations entre les organisations financières, juridiques et commerciales et permettre aux participants au système de réaliser des transactions de paiement sur mobile présentant le degré de sécurité nécessaire selon le niveau de risque estimé. L'architecture proposée devrait prendre en charge les schémas et spécifications déjà utilisés par les participants au système pour l'exécution de transactions de paiement.

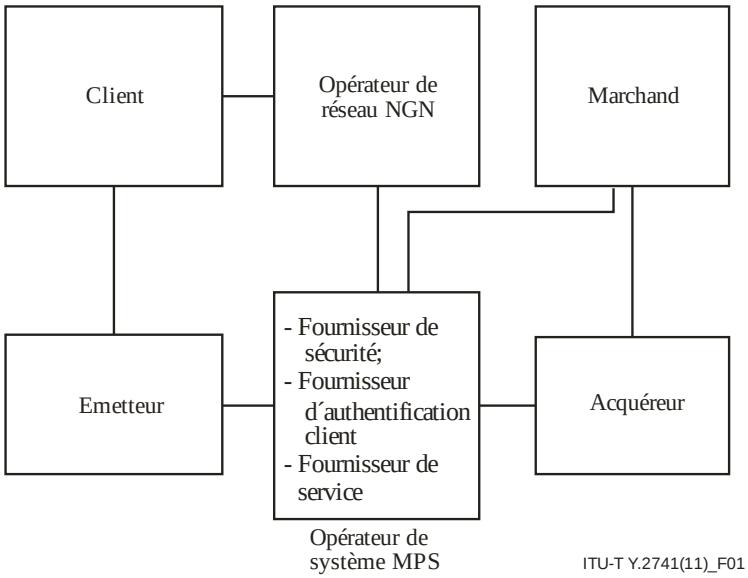


Figure 1 – Participants et architecture du système de commerce sur mobile et de services bancaires sur mobile

Tableau 1 – Participants au système de paiements sur mobile

Participant	Description, enjeu (but, objectif, intérêt)	Rôle
Client	Particulier ou personne morale qui a signé un accord contractuel concernant l'utilisation de services de télécommunication et du système de commerce sur mobile. Possède un dispositif mobile et un instrument de paiement. Principaux enjeux: accroître le nombre de services, pouvoir réaliser des transactions financières à distance en toute sécurité, élargir l'éventail des instruments de paiement.	Client
Opérateur de réseau NGN	Institution qui offre au client des services de communications numériques. Principaux enjeux: accroître le nombre de clients, élargir l'éventail de services disponibles, augmenter le trafic.	Opérateur de réseau NGN
Opérateur de système MPS	Institution qui assure une interaction à distance sécurisée entre les structures financières, le client et l'opérateur de réseau NGN dans le cadre du système de paiements sur mobile. Principaux enjeux: créer un vaste réseau de commerce mobile, augmenter le nombre de participants ainsi que le nombre de transactions à distance, garantir une sécurité maximale des opérations.	Fournisseur de sécurité, fournisseur de service, fournisseur d'authentification client
Emetteur	Institution financière et juridique qui émet des instruments de paiement et offre des services connexes.	Emetteur

Tableau 1 – Participants au système de paiements sur mobile

Participant	Description, enjeu (but, objectif, intérêt)	Rôle
	Principaux enjeux: accroître l'utilisation des instruments de paiement émis, augmenter le nombre de clients.	
Acquéreur	Institution financière et juridique qui accepte les paiements des produits ou services pour le compte d'un marchand. Principal enjeu: augmenter le nombre de transactions des marchands auxquels il offre ses services	Acquéreur
Marchand	Personne morale qui offre des biens ou des services et qui reçoit un paiement du client. Principaux enjeux: promouvoir ses biens et ses services, augmenter le nombre de clients, augmenter les possibilités de paiement de biens et services.	Marchand

Les participants peuvent combiner les rôles suivant la mise en œuvre de l'architecture.

Pour obtenir le niveau de sécurité requis décrit dans la Recommandation [UIT-T Y.2740], il peut être nécessaire d'introduire les rôles d'une application client et de distributeur d'applications client ou les deux. Le premier est téléchargé sur les dispositifs mobiles des clients, tandis que le second peut être exécuté par l'opérateur de réseau NGN, l'opérateur de paiement mobile ou une tierce partie.

Lorsque des cartes de systèmes de paiement internationaux sont utilisées comme instruments de paiement, le système de paiement joue un rôle intégral.

6.4 Scénarios d'utilisation du système de paiements sur mobile

6.4.1 Scénarios d'utilisation de base

6.4.1.1 Inscription d'un client dans le système MPS

Objet: Abonner le client au service offert par le système MPS.

Buts et objectifs des rôles de base

Client: pouvoir utiliser les services MPS.

Opérateur du système MPS: inscrire un nouveau client dans le système MPS.

Garanties maximales

L'acceptation par le client des clauses et conditions d'utilisation du système MPS est enregistrée.

Le client est enregistré dans le système informatique de l'opérateur du système MPS.

Le client reçoit le code d'activation.

Garanties minimales

L'inscription est refusée au client avec indication de la cause du refus.

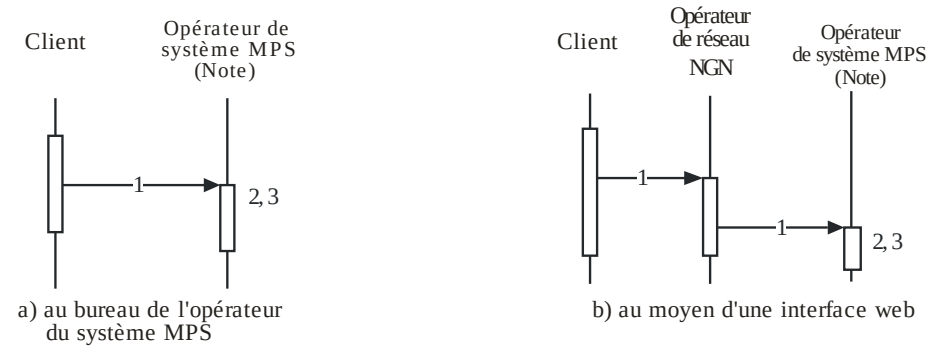
L'opérateur du système MPS enregistre l'annulation de l'inscription du client.

Données initiales du scénario

Il n'existe pas de profil de client actif dans le système MPS: le client n'a pas été inscrit dans le système MPS ou son profil a été supprimé précédemment.

Etapes de base du scénario

1) Le client lance l'inscription:
   a) au bureau de l'opérateur du système MPS;
   b) au moyen de l'interface web: le client est autorisé à accéder au site web de l'opérateur du système MPS et la demande d'inscription est envoyée.
2) Le client est authentifié dans le système MPS.
3) Le système informatique de l'opérateur du système MPS crée un profil de données du client dans la base de données.



NOTE – Fournisseur de sécurité, fournisseur d'authentification client, fournisseur de service

ITU-T Y.2741(11)_F02

Figure 2 – Inscription d'un client dans le système MPS

Autres étapes possibles du scénario

3. a. Le client a été inscrit dans le système MPS (il a un profil actif):

Le système informatique de l'opérateur du système MPS informe le client du fait qu'il est déjà inscrit pour le service.

3. b. Le client a un compte dans le système MPS mais ce compte a été bloqué:

Le système informatique de l'opérateur du système MPS active le compte du client.

3. c. Le système informatique de l'opérateur du système MPS refuse l'enregistrement:

   a) Le système informatique de l'opérateur du système MPS enregistre une tentative de connexion du client au service.
   b) Le système informatique de l'opérateur du système MPS informe le client du refus de connexion au service et en précise les raisons.

6.4.1.2 Enregistrement de l'instrument de paiement à utiliser dans le système MPS

Le client doit enregistrer son instrument de paiement. Les conditions suivantes doivent être remplies au cours de ce processus:

– Le client doit confirmer qu'il est habilité à utiliser l'instrument de paiement en cours d'enregistrement.
– Au cours de l'enregistrement de l'instrument de paiement, un nombre minimal de paramètres nécessaires pour que le client puisse réaliser une transaction de paiement à distance doivent être stockés dans la base de données de l'opérateur du système MPS.
– Les paramètres de l'instrument de paiement doivent être stockés en toute sécurité du côté de l'opérateur du système MPS de façon qu'il soit impossible d'accéder à ces paramètres sans y être autorisé et de réaliser des transactions financières qui n'ont pas été autorisées par le client.

Les moyens permettant de connecter un instrument de paiement sont décrits dans l'Appendice I.

6.4.1.3 Exécution par le client d'opérations financières dans son propre système de paiement lorsqu'il se trouve dans la zone de rattachement

***Objet**:* Permettre au client d'utiliser les services financiers du système MPS.

Buts et objectifs des rôles de base

Client: utiliser les services offerts par le marchand à distance.

Opérateur mobile: transmettre le message sur les canaux de communication.

Opérateur du système MPS: permettre au client de payer des biens et des services au moyen du système MPS.

Marchand: fournir des services à distance au client.

Emetteur: fournir l'autorisation nécessaire pour l'opération de paiement du client et lancer le règlement associé.

Acquéreur: transférer la réponse d'autorisation de l'opération au marchand.

Garanties maximales

Le client paie le service demandé au marchand.

Le marchand fournit le service.

Garanties minimales

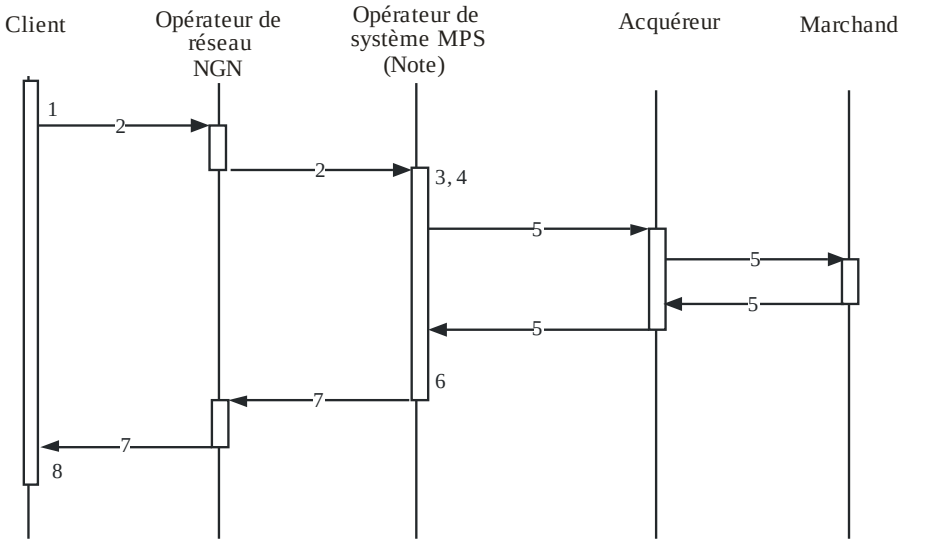
Le client se voit refuser le paiement des biens et services par l'opérateur du système MPS.

Données initiales du scénario

Le client est inscrit dans le système MPS et a un instrument de paiement enregistré dans le système MPS.

Etapes de base du scénario

1) Le client utilise son dispositif mobile pour générer une demande qui contient les paramètres de l'opération financière et ceux de l'instrument de paiement.
2) La demande est transmise sur les canaux de l'opérateur de réseau NGN.
3) L'opérateur du système MPS reçoit la demande.
4) Le client est authentifié.
5) L'opération financière demandée (versement/paiement) est effectuée sur la base des renseignements relatifs à l'instrument de paiement du client.
6) Le résultat de l'opération est envoyé au client.
7) La réponse est transmise sur les canaux de l'opérateur de réseau NGN.
8) Le client reçoit le résultat de l'opération financière.



NOTE – Fournisseur de sécurité, fournisseur d'authentification client, fournisseur de service

ITU-T Y.2741(11)_F03

Figure 3 – Exécution d'opérations financières par le client

Autres étapes possibles du scénario

6. Le client n'est pas authentifié.

7. L'opération financière est impossible

a) La transaction est annulée.

b) Le résultat du traitement de l'opération est retourné au client.

Autre scénario possible: le marchand lance un paiement

Les étapes de base du scénario sont les suivantes

1) a) Le marchand génère une offre de paiement et l'envoie à l'opérateur du système MPS;

b) l'opérateur du système MPS détermine le client et les modalités de transmission de l'offre de paiement au client;

c) la demande est envoyée au client sur les canaux de l'opérateur de réseau NGN.

2) Le client reçoit la demande sur son dispositif mobile et génère une réponse qui contient les paramètres de l'opération financière et ceux de l'instrument de paiement.

3) La demande est transmise sur les canaux de l'opérateur de réseau NGN.

4) L'opérateur du système MPS reçoit la réponse du client.

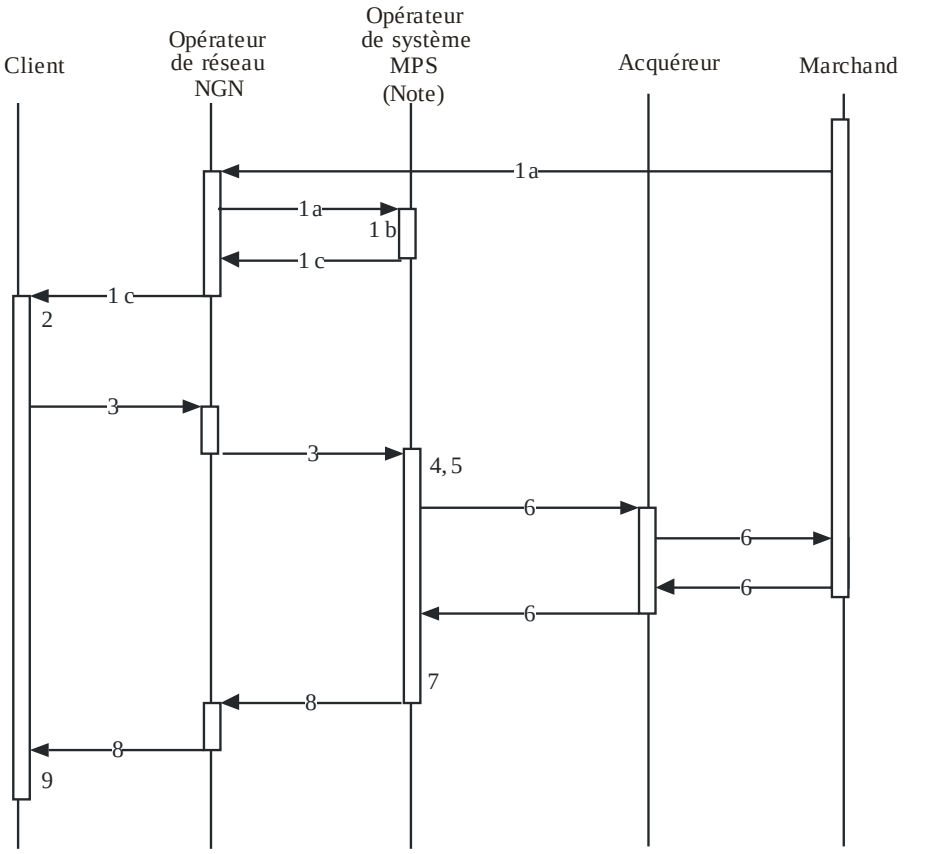
5) Authentification du client.

6) L'opération financière requise (versement/paiement) est réalisée sur la base des renseignements relatifs à l'instrument de paiement du client.

7) Le résultat de l'opération est envoyé au client.

8) La réponse est transmise via les canaux de l'opérateur de réseau NGN.

9) Le client reçoit le résultat de l'opération financière.



NOTE – Fournisseur de sécurité, fournisseur d´authentification client, fournisseur de service

ITU-T Y.2741(11)_F04

Figure 4 – Exécution de paiements lancés par le marchand

6.4.1.4 Désenregistrement de l'instrument de paiement du système MPS

Objet: Permettre au client de supprimer les données relatives à l'instrument de paiement dans le système MPS.

Buts et objectifs des rôles de base

Client: désenregistrer l'instrument de paiement du système MPS.

Opérateur mobile: transmettre le message via les canaux de communication.

Opérateur du système MPS: permettre au client de désenregistrer l'instrument de paiement.

Garanties maximales

Le client désenregistre l'instrument de paiement du système MPS.

Garanties minimales

Le client ne peut pas désenregistrer l'instrument de paiement.

Données initiales du scénario

Le client est inscrit dans le système MPS et a un instrument de paiement enregistré.

Etapes de base du scénario

1) Le client utilise son dispositif mobile pour générer une demande de désenregistrement d'un certain instrument de paiement.
2) La demande est transmise via les canaux de l'opérateur de réseau NGN.
3) L'opérateur du système MPS reçoit la demande.

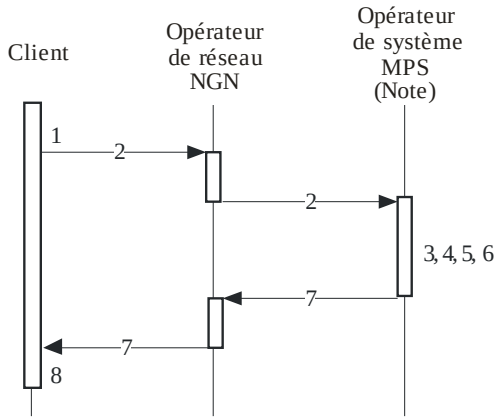
4) Le système MPS authentifie le client.

5) L'instrument de paiement est supprimé de la base de données du système informatique.

6) Le résultat du désenregistrement de l'instrument de paiement est envoyé au client.

7) La réponse est transmise via les canaux de l'opérateur de réseau NGN.

8) Le client reçoit le résultat de l'opération.



NOTE – Fournisseur de sécurité, fournisseur d´authentification client, fournisseur de service

ITU-T Y.2741(11)_F05

Figure 5 – Désenregistrement de l'instrument de paiement du système MPS

Autres étapes possibles du scénario

7. Le désenregistrement de l'instrument de paiement du système MPS est refusé:

a) Le système informatique de l'opérateur du système MPS informe le client de l'impossibilité de désenregistrer l'instrument de paiement.

6.4.1.5 Désinscription du client du système MPS

***Objet**:* Déconnecter le client des services MPS.

Buts et objectifs des rôles de base

Client: abandonner l'utilisation des services MPS.

Opérateur du système MPS: rendre les services inaccessibles au client.

Garanties maximales

L'annulation par le client des services MPS est enregistrée.

Les services MPS deviennent inaccessibles pour le client.

Garanties minimales

La déconnexion des services est refusée au client; la raison est indiquée.

Le client annule la déconnexion des services MPS.

Données initiales du scénario

Le client est inscrit dans le système MPS.

Etapes de base du scénario

1) Le client lance la déconnexion des services

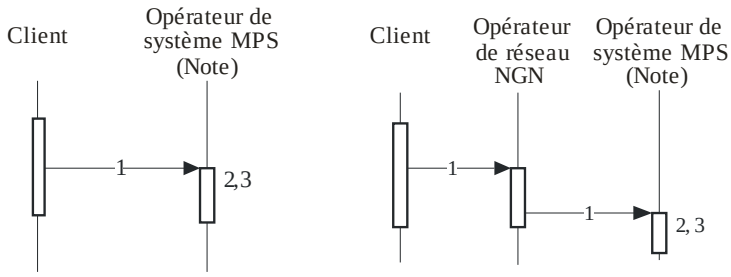
- au bureau de l'opérateur du système MPS;

- au moyen de l'interface web: le client est autorisé à accéder au site web de l'opérateur du système MPS et ordonne la déconnexion du service.

2) Le client est authentifié dans le système MPS.

3) Le système informatique de l'opérateur du système MPS insère les modifications de statut du client dans la base de données (le profil est bloqué).

4) Le client ne peut pas utiliser les services MPS sans réinscription.



a) au bureau de l'opérateur du système MPS

b) au moyen d'une interface web

NOTE – Fournisseur de sécurité, fournisseur d'authentification client, fournisseur de service

ITU-T Y.2741(11)_F06

Figure 6 – Désinscription du client du système MPS

Autres étapes possibles du scénario

1. Une application de paiement est utilisée dans le système MPS

Le client lance la désinscription du système MPS dans l'application.

3. Le client ne peut pas être déconnecté des services MPS

Le système informatique de l'opérateur du système MPS informe le client du fait que le service ne peut pas être déconnecté pour le moment.

6.4.2 Scénario d'utilisation avec application de paiement

6.4.2.1 Réception de l'application de paiement

***Objet**:* Permettre au client d'utiliser l'application dans le système MPS.

Buts et objectifs des rôles de base

Client: recevoir l'application de paiement à utiliser dans le dispositif mobile.

Distributeur d'applications client: fournir au client l'application.

Garanties maximales

Le client reçoit l'application.

Garanties minimales

L'application est refusée au client.

Il est impossible pour le client d'utiliser l'application reçue en raison de certaines caractéristiques techniques du dispositif mobile.

Données initiales du scénario

Le client est inscrit dans le système MPS et il lui est possible techniquement d'utiliser l'application.

Etapes de base du scénario

1) Le client reçoit l'application en provenance du distributeur d'applications client:
   - au bureau du distributeur d'applications client;
   - au moyen de l'interface web (sur le site web du distributeur d'applications client).
2) Le client peut utiliser l'application sur le dispositif mobile.

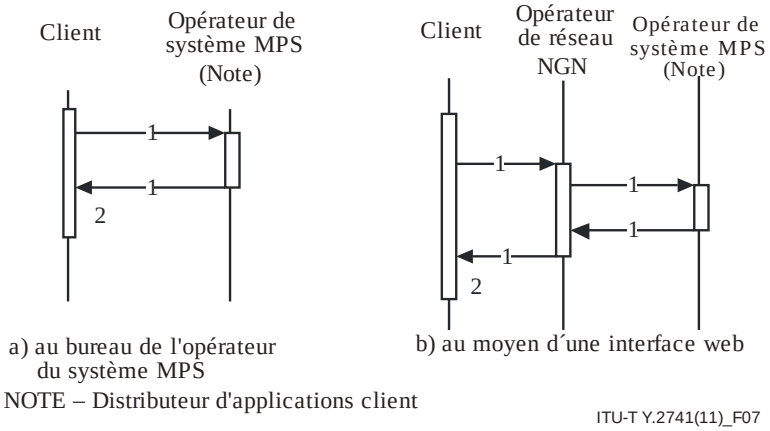


Figure 7 – Réception de l'application de paiement

Autres étapes possibles du scénario

1. a. Le client reçoit une version mise à jour de l'application

Le client a reçu l'application auparavant.

1. b. Le client ne reçoit pas l'application

Le client demande l'aide du service d'assistance du distributeur d'applications client.

6.4.2.2 Activation de l'application de paiement

Objet: Activer l'application de paiement du client.

Buts et objectifs des rôles de base

Client: pouvoir utiliser les services MPS au moyen de l'application.

Opérateur du système MPS: valider l'utilisation de l'application de paiement donnée dans le système MPS par le client donné.

Opérateur mobile: transmettre le message via les canaux de communication.

Garanties maximales

Le client active l'application.

Les clés du client sont chargées dans l'application.

Les clés du client sont insérées dans la base de données du système informatique de l'opérateur du système MPS.

Garanties minimales

L'activation de l'application est refusée au client; la cause du refus est indiquée.

Données initiales du scénario

Le client est inscrit dans le système MPS et a le code d'activation et l'application dans le dispositif mobile.

Etapes de base du scénario

1) Le client sélectionne "activation" dans le menu de l'application.
2) Le client présente à l'application le code d'activation reçu pendant la procédure d'inscription.
3) L'application génère et envoie une demande au système MPS.
4) La demande est transmise via les canaux de l'opérateur de réseau NGN.
5) L'opérateur du système MPS reçoit la demande. Le code d'activation est vérifié.
6) Les clés du client sont générées et stockées dans la base de données du système informatique du fournisseur du système MPS.
7) Les clés et le résultat de l'activation sont envoyés au client.
8) La réponse est transmise via les canaux de l'opérateur de réseau NGN.
9) L'application du client reçoit le message et stocke les clés du client, et le résultat de l'activation est présenté au client.
10) Le client reçoit l'accès aux services MPS dans l'application.

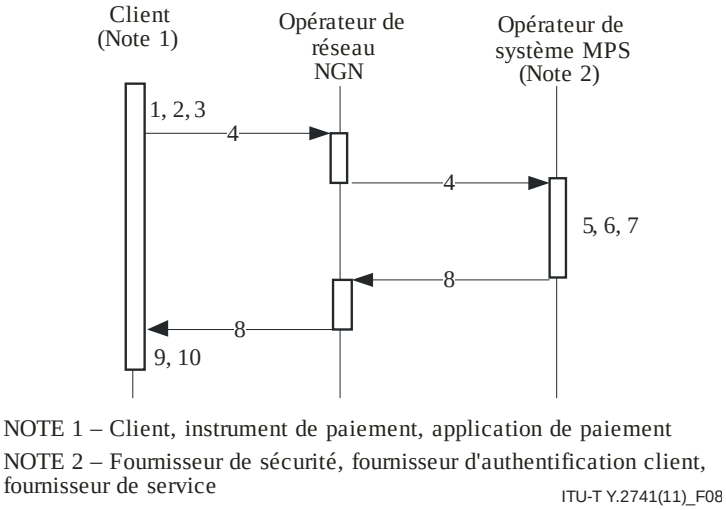


Figure 8 – Activation de l'application de paiement

Autres étapes possibles du scénario

5. Erreur dans la validation du code d'activation:

a) Le système informatique de l'opérateur du système MPS informe le client que le code d'activation saisi est incorrect.

b) Le compte du client est bloqué si la limite du nombre de tentatives pour saisir le code d'activation est dépassée.

6.4.3 Scénarios d'utilisation avec interaction intersystèmes

La présente Recommandation traite de questions générales et décrit les principaux scénarios de l'interaction.

6.4.3.1 Exécution de transactions financières lorsque le client est en itinérance

***Objet**:* Permettre au client d'utiliser le service MPS activé lorsqu'il se trouve en dehors de la zone de couverture de l'opérateur (zone de rattachement).

Buts et objectifs des rôles de base

Client: pouvoir payer des services au moyen du système MPS lorsqu'il se trouve en dehors de la zone de rattachement.

Opérateur mobile: transmettre le message via les canaux de communication.

Opérateur de système MPS: permettre au client de payer des biens et des services au moyen du système MPS.

Marchand: offrir des services à distance au client.

Emetteur: fournir une autorisation pour l'opération de paiement du client et lancer le règlement associé.

Acquéreur: transférer la réponse d'autorisation de l'opération au marchand.

Garanties maximales

Le client paye le service demandé au marchand.

Le marchand fournit le service.

Garanties minimales

Le client se voit refuser le paiement des biens et services par l'opérateur du système MPS.

Données initiales du scénario

Le client est inscrit dans le système MPS; il est en itinérance (en dehors de la zone de rattachement) et a un instrument de paiement enregistré.

Etapes de base du scénario

Les étapes de base du scénario sont analogues à celles décrites dans le scénario de la transaction financière à l'intérieur de la zone de rattachement. La demande du client et le résultat de transaction de la zone d'itinérance vers la zone de rattachement sont assujettis aux règles d'itinérance et ne sont pas traités dans la présente Recommandation.

6.4.3.2 Exécution par le client d'opérations financières dans un autre système MPS

***Objet**:* Permettre au client d'utiliser les services d'un système MPS différent dans lequel le client n'est pas inscrit.

Buts et objectifs des rôles de base

Client: pouvoir payer les services demandés à un marchand situé dans la zone de couverture d'un système MPS différent.

Opérateur mobile: transmettre le message sur les canaux de communication.

Opérateur de système MPS: permettre au client de payer des biens et des services au moyen d'un autre système MPS.

Marchand: fournir des services à distance au client.

Emetteur: fournir l'autorisation pour l'opération de paiement du client et lancer le règlement associé.

Acquéreur: transférer la réponse d'autorisation de l'opération au marchand.

Garanties maximales

Le client paye le service demandé au marchand.

Le marchand fournit le service.

Garanties minimales

Le client se voit refuser le paiement des biens et services par l'opérateur du système MPS.

Données initiales du scénario

Le client est inscrit dans le système MPS, à un instrument de paiement enregistré et connaît les renseignements relatifs au marchand qui sont nécessaires pour la transaction de paiement.

Etapes de base du scénario

1) Le client génère une demande au moyen de son téléphone mobile. La demande contient les paramètres de transaction financière (identificateur de paiement) et les paramètres de l'instrument de paiement.
2) La demande est transmise sur les canaux de communication de l'opérateur.
3) L'opérateur du système MPS reçoit la demande.
4) Le client est authentifié.
5) L'opérateur du système MPS est identifié par l'identificateur de paiement.
6) La demande est transmise au destinataire (l'opérateur d'un système MPS différent) sur les canaux sécurisés intersystèmes.
7) La transaction financière requise est exécutée sur la base des renseignements relatifs à l'instrument de paiement du client.
8) Le résultat de la transaction est envoyé au système MPS de rattachement du client.
9) Le système MPS génère la réponse destinée au client.
10) La réponse est transmise sur les canaux de communication de l'opérateur.
11) Le client reçoit le résultat de la transaction.

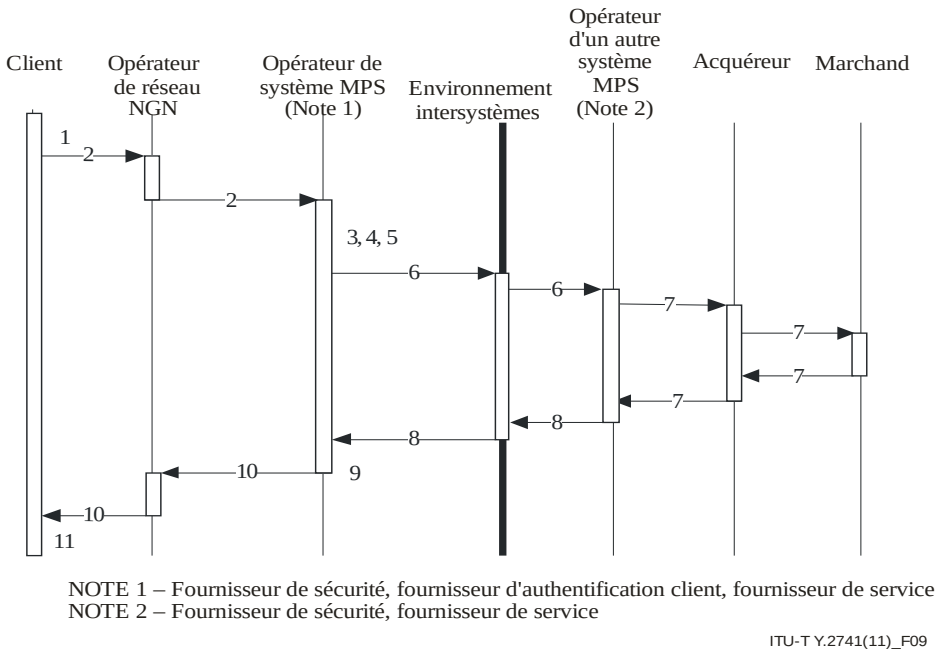


Figure 9 – Exécution par le client d'opérations financières dans un autre système MPS

Autres étapes possibles du scénario

4. Le client n'est pas authentifié.

5. Le système MPS ne peut pas être identifié.

7. L'opération financière est impossible:

a) La transaction est annulée.

b) Le résultat d'exécution de l'opération est retourné au client.

7 Abandon des systèmes de paiement utilisant des jetons

Certains opérateurs ont introduit des services qui permettent le transfert de jetons monétaires ou non monétaires comme paiement de biens et de services, dans (et parfois entre) les systèmes de facturation des opérateurs de réseaux NGN.

Bien que ces services soient souvent présentés comme favorables au développement d'économies immatures avec une forte proportion de personnes sans compte bancaire, à long terme ils risquent de perturber les systèmes fiscaux et monétaires de ces économies.

Les pays en développement sont confrontés à de très nombreux problèmes de criminalité liée à l'argent liquide. La mise en place de systèmes bancaires électroniques dans ces pays permet de réduire la quantité d'argent liquide en circulation et, par conséquent, de réduire la criminalité liée à l'argent liquide.

Les opérateurs de réseaux NGN offrant des services de paiement par jeton devraient donc prévoir le passage de ces systèmes de paiement par jeton à des systèmes utilisant des transactions financières pour l'échange de valeur.

Appendice I

Enregistrement d'un instrument de paiement dans le système

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

***Objet**:* Permettre au client d'utiliser son instrument de paiement dans le système MPS.

Buts et objectifs des rôles de base

Client: pouvoir bénéficier du système MPS au moyen d'un instrument de paiement.

Opérateur mobile: transmettre le message via les canaux de communication.

Opérateur de système MPS: approuver l'utilisation de l'application de paiement donnée dans le système MPS par le client donné.

Fournisseur d'authentification client: authentifier le client et son instrument de paiement.

Garanties maximales

Le client a la possibilité de bénéficier du système MPS pour utiliser l'instrument de paiement.

Garanties minimales

Le client se voir refuser l'utilisation de l'instrument de paiement.

Données initiales du scénario

Le client est inscrit dans le système MPS et a un instrument de paiement.

Etapes de base du scénario

1) Le client utilise son dispositif mobile pour transmettre les paramètres de l'instrument de paiement à l'opérateur du système MPS.
2) La demande est transmise sur les canaux de l'opérateur de réseau NGN.
3) L'opérateur du système MPS reçoit la demande.
4) Le système informatique de l'opérateur du système MPS génère un montant aléatoire.
5) L'opérateur du système MPS envoie au système acquéreur une demande de réservation de ce montant pour l'instrument de paiement. L'acquéreur envoie une demande d'autorisation à l'émetteur de l'instrument de paiement. Le client contacte l'émetteur pour connaître le montant et confirmer qu'il est le propriétaire légitime de l'instrument de paiement.
6) L'émetteur de l'instrument de paiement authentifie le client en utilisant ses moyens d'authentification standard.
7) Après l'authentification, l'émetteur informe le client de la valeur du montant réservé.
8) Le client transmet la valeur à l'opérateur du système MPS via l'application client.
9) La demande est transmise via les canaux de l'opérateur de réseau NGN.
10) Après avoir reçu du client la valeur du montant réservé, l'opérateur du système MPS la compare à la valeur générée précédemment.
11) Sous réserve que les deux montants coïncident, l'opérateur du système MPS stocke les informations sur l'instrument de paiement en vue d'une utilisation future dans la mémoire sécurisée, et envoie une notification avec le résultat de l'opération au client.
12) Simultanément, la demande est envoyée à l'émetteur (via l'acquéreur) afin d'annuler la réservation du montant pour l'instrument de paiement.

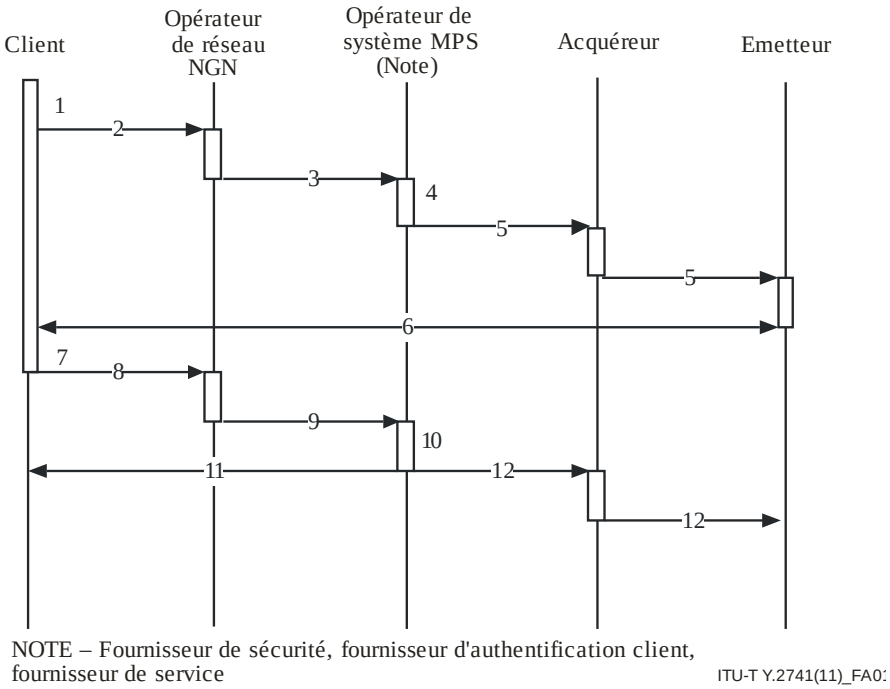


Figure I.1 – Enregistrement d'un instrument de paiement dans le système MPS

Autres étapes possibles du scénario

10. La valeur du montant réservé précédemment ne coïncide pas avec celui saisi par le client.

Le client reçoit une notification d'erreur. Lorsque le nombre de tentatives ayant échoué dépasse trois, le profil du client du dispositif mobile est bloqué dans le système MPS. Le montant réservé est annulé.

Appendice II

Modèles de mise en œuvre de systèmes de commerce sur mobile et de services bancaires sur mobile

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

Le présent Appendice donne des exemples de modèles de mise en œuvre de systèmes de commerce sur mobile et de services bancaires sur mobile suivant le niveau de sécurité mis en œuvre.

Les termes suivants sont utilisés dans le présent Appendice:

Un **canal de transmission de message** est un moyen permettant de transférer une demande d'un client visant à exécuter une opération financière (transfert d'argent) qui nécessite un accès à distance aux instruments de paiement. Parmi les exemples de canaux de transmission de message, on peut citer les messages SMS, les demandes USSD, la communication par lots (GPRS, EDGE, données 3G, HSDPA etc.)

Un **instrument de paiement** est un ensemble de mesures juridiques permettant d'exécuter un versement, en espèces ou non, afin d'effectuer un paiement. Parmi les exemples d'instruments de paiement, on peut citer les comptes bancaires, les comptes d'opérateur et les cartes bancaires.

Les **opérations disponibles** sont les opérations disponibles dans le système pour un certain niveau de sécurité.

Les **restrictions** sont les limitations relatives à l'utilisation du système qui découlent du modèle de risques accepté et qui sont définies par la législation ou dans des contrats mutuels.

Un **téléphone prédéfini** est un numéro de téléphone indiqué précédemment par le client dans un formulaire spécial du fournisseur de service.

Un **téléphone ad hoc** est un numéro de téléphone indiqué par le client directement lors de la réalisation d'un paiement.

Un **compte prédéfini** est un numéro de compte indiqué précédemment par le client dans un formulaire spécial du fournisseur de service.

Un **compte ad hoc** est un numéro de compte indiqué par le client directement lors de la réalisation d'un paiement.

Un **paiement prédéfini** est un paiement réalisé en utilisant les paramètres fournis précédemment dans le cadre desquels un destinataire de paiement peut être sélectionné à partir de la liste définie par le fournisseur de service MPS (par exemple un paiement réalisé par une personne auprès d'une entreprise pour les services fournis).

Un **paiement ad hoc** est un paiement réalisé par le client pour des services qui ne figurent pas dans la liste définie par le fournisseur de service MPS à condition qu'il soit possible techniquement de réaliser ce type de paiement. Condition préalable: il est obligatoire soit que le fournisseur de service ait un canal lui permettant d'interfonctionner avec le fournisseur de système MPS soit que le service soit fourni par un autre fournisseur de système MPS et qu'un interfonctionnement soit mis en place entre les deux.

Un **paiement automatique** est un paiement ordinaire lancé automatiquement par le fournisseur de service MPS avec le consentement préalable du client.

Un **paiement automatique avec confirmation** est un paiement ordinaire lancé automatiquement par le fournisseur de service MPS avec le consentement du client.

Un **paiement lancé par le marchand** est un paiement dont les paramètres sont déterminés et saisis par le marchand. Le client peut soit confirmer soit rejeter le traitement du paiement proposé.

Un **service d'information** est un ensemble de services d'information fournis par le fournisseur de système MPS qui ne sont pas associés à l'exécution d'opérations financières (par exemple visualisation du solde d'un instrument de paiement, fourniture d'informations de référence).

Modèles de mise en œuvre de systèmes de commerce sur mobile et de services bancaires sur mobile

Les modèles possibles de mise en œuvre de systèmes de commerce sur mobile et de services bancaires sur mobile suivant le niveau de sécurité mis en œuvre sont présentés ci-dessous. Chaque modèle de mise en œuvre impose certaines exigences concernant l'instrument de paiement, les opérations disponibles, les restrictions et l'application utilisés dans le système.

II.1 Mise en œuvre du système sans utilisation de l'application client

Elle correspond aux niveaux 1 et 2 de sécurité du système (voir la Recommandation [UIT-T Y.2740]).

Canal de transmission de message: messages SMS en clair, demandes USSD,

Instrument de paiement: paiements à partir des comptes bancaires et des comptes d'opérateur prédéfinis dans l'accord de service.

Opérations disponibles: paiements uniquement au bénéfice de destinataires définis précédemment dans le contrat. La liste des opérations possibles devrait être spécifiée lors de la signature du contrat:

- Paiement pour un téléphone prédéfini
- Paiement dans un compte prédéfini
- Réalisation d'un paiement prédéfini
- Réalisation de paiements automatiques
- Réalisation de paiements automatiques avec confirmation
- Service d'information.

Restrictions: limites maximales de paiement qui peuvent inclure des limites concernant le montant d'une transaction ou des limites concernant les transactions intrajournalières; restriction concernant les transactions financières disponibles, qui se traduit par des paiements uniquement pour les services convenus précédemment.

II.2 Mise en œuvre du système avec utilisation de l'application client

Elle correspond aux niveaux 3 et 4 de sécurité du système (voir la Recommandation [UIT-T Y.2740]).

Canal de transmission de message: messages SMS, communication par lots (GPRS, EDGE, données 3G, HSDPA, etc.). Le canal de transmission de message et le message transmis doivent être chiffrés au moyen d'un chiffrement puissant.

Instrument de paiement: paiements à partir des comptes bancaires et des comptes d'opérateur prédéfinis dans l'accord de service; paiements au moyen de cartes bancaires ou de cartes de systèmes de paiement internationaux (pour les paiements, des données critiques sont transmises sur les canaux de communication).

Opérations disponibles: une connexion à distance au système est possible; une large gamme de paiements sont disponibles pour divers services connectés au système; il est possible d'augmenter considérablement le nombre d'opérations mises en œuvre dans le système MPS (introduction de nouveaux paiements et de nouveaux services; connexion de nouveaux marchands); la liste des paiements disponibles peut être définie avec souplesse à la fois par le fournisseur de service et par

le client; différents systèmes MPS peuvent interfonctionner pour la fourniture de services. Les opérations qu'il est possible de mettre en œuvre sont les suivantes:

- Paiement pour un téléphone prédéfini
- Paiement dans un compte prédéfini
- Réalisation d'un paiement prédéfini
- Réalisation de paiements automatiques
- Réalisation de paiements automatiques avec confirmation
- Service d'information
- Paiement pour un téléphone ad hoc
- Paiements dans un compte ad hoc
- Paiements ad hoc
- Paiements lancés par un marchand

Restrictions: les restrictions relatives aux paiements sont déterminées dans les contrats mutuels conclus par les participants au système.

Application: il est obligatoire d'utiliser l'application pour garantir la sécurité (chiffrement des messages) et une utilisation correcte du système.

Bibliographie

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

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