International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2741

(01/2011)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

Architecture of secure mobile financial transactions in next generation networks

Recommendation ITU-T Y.2741

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2741

Architecture of secure mobile financial transactions in next generation networks

Summary

Recommendation ITU-T Y.2741 specifies the general architecture of a security solution for mobile commerce and mobile banking in the context of NGN. It describes the key participants, their roles, and the operational scenarios of the mobile commerce and mobile banking systems. It also provides examples of the implementation models of mobile commerce and mobile banking systems.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2741	2011-01-28	13

Keywords

Mobile banking, mobile commerce, mobile payments, remote payments, safety and security.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2741

Architecture of secure mobile financial transactions in next generation networks

1 Scope

This Recommendation defines the security architecture pertaining to remote mobile financial transactions for NGN. The scope excludes all other financial transactions, as well as transactions that use monetary or non-monetary tokens for transfer of value.

By organizing a wide range of services with a flexible management and personalization functions, NGN can provide convenient access to mobile payment system (MPS) services.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2740] Recommendation ITU-T Y.2740 (2011), *Security requirements for mobile remote financial transactions in next generation networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 next generation network (NGN) [b-ITU-T Y.2001]: A packet-based network able to provide telecommunication services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 application: A special mobile banking or mobile commerce application uploaded to the client's (user's) mobile device.

3.2.2 bank account: An electronic funds account held by a private individual or a corporate entity in a bank or other financial institution authorized by the country's national monetary authority (e.g., central bank) that can be used for payment for goods and services.

3.2.3 client: A private individual or a corporate entity that has signed a contractual agreement on the use of telecommunication services and the system of mobile commerce.

3.2.4 financial transaction: An event or a condition covered under the terms of the contract between a buyer and a seller to exchange an asset for payment.

3.2.5 intersystem environment: A set of rules or a system that enables the establishment of the interaction of various mobile bank and mobile commerce systems.

3.2.6 mobile device: An electronic device used for telecommunications over wireless NGN network.

3.2.7 mobile financial transaction: A financial transaction initiated and/or authorized using a mobile device.

3.2.8 mobile payment system (MPS): Mobile banking and/or mobile commerce systems.

3.2.9 monetary token: Electronic or physical artifact used for payment that is represented and measured in the country's national currency units, that however is not stored in, or directly linked to a bank account.

An example of an electronic monetary token is electronic cash stored in a stand-alone electronic wallet that is not mirrored by a bank account. Examples of physical monetary tokens include coins, banknotes, traveller's checks, etc.

3.2.10 non-monetary token: Electronic or physical artifact used for payment but not represented in national currency units. Examples of electronic non-monetary tokens are unused 'minutes' or 'SMS messages' held in NGN subscriber accounts that the NGN operators allow to be transferred from one subscriber account to another.

3.2.11 payment ID: A required request parameter that explicitly identifies the payment recipient. Merchant ID and mobile payment system (MPS) ID (a unique identifier of a mobile payment system) must be present in the implementation of the intersystem environment.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DB DataBase

ID Identification

IS Information System

MPS Mobile Payment System

NGN Next Generation Network

5 Conventions

None.

6 Roles, risks, participants, and scenarios of mobile payments in NGN

6.1 Roles within the mobile commerce and mobile banking systems

The basic roles of the MPS participants and their responsibilities are:

- The client is a mobile subscriber who possesses a payment instrument for the payment operations.
- The client application is the special software uploaded to the client's mobile device (phone, SIM card, communicator, etc.) and designed for conducting secure mobile payment operations.
- The payment instrument is a financial instrument used to perform payment for goods and services.

- The NGN operator provides the mobile communication network for remote interaction of the client with the MPS, data routing and transfer.
- The client application distributor is a participant that makes applications available to the clients.
- The security provider is a participant that provides security of the data transfer over communications channels.
- The MPS operator (service provider, payment gateway) is a participant that ensures interaction within the MPS and provides payment services to the end user.
- The issuer is a financial institution that issues payment instruments.
- The client authentication provider validates the client operation.
- The acquirer is a financial institution that maintains merchant relationships and receives all financial transactions from the merchant.
- The payment system is an organization that ensures interbank payment transactions.

6.2 Risks in the MPS and MPS security levels

This clause describes the basic information security risks that may arise when conducting (i.e., performing) remote mobile payments. These risks include, but are not limited to:

- The risk of compromised confidentiality – unauthorized third party access to confidential information.
- The risk of compromised integrity – information distortion during the process of its transfer or processing.
- The risk of forging of electronic documents – a document is generated by an unauthorized party.
- The risk of repudiation – the denial of authorship of an electronic document.
- The risk of information destruction, either intentional or by negligence.
- Transactional risk – the failure to finish a transaction (e.g., due to unstable mobile communication).
- Depending on the implemented risk-based security mechanisms, there are systems with four security levels [ITU-T Y.2740].

6.3 Participants and the system architecture of mobile commerce and mobile banking

The MPS architecture should be compliant with the already existing system of interrelations between financial, legal and commercial organizations and enable system participants to make mobile payment transactions with the necessary degree of security based on the estimated risk level. The proposed architecture should support schemes and specifications already used by the system participants for performing payment transactions.

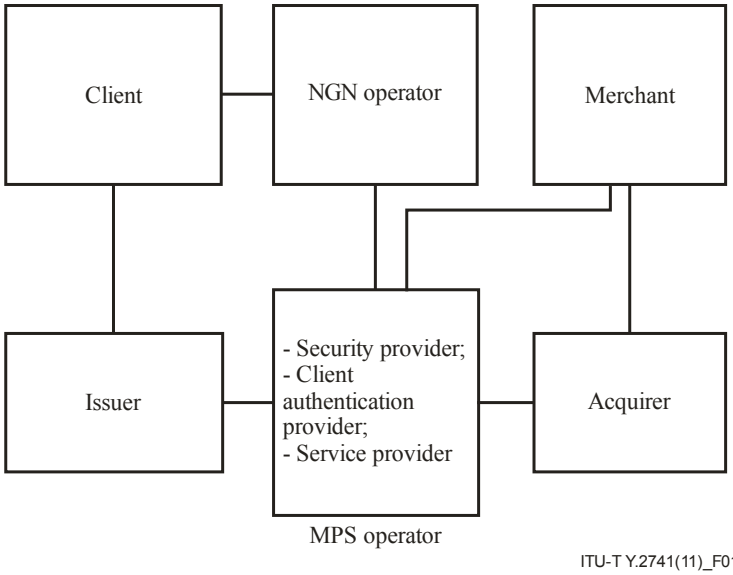


Figure 1 – Participants and the system architecture of the mobile commerce and the mobile banking

Table 1 – Mobile payments system participants

Participant	Description, concern (goal, objective, interest)	Role
Client	Private individual or corporate entity that has signed a contractual agreement on the use of telecommunication services and the system of mobile commerce. Possesses a mobile device and a payment instrument. Principal concern: increase the number of services, get the possibility to perform secure remote financial transactions, expand the scope of payment instruments.	Client
NGN operator	An institution that provides the client with digital communication services. Principal concern: increase the number of clients, extend the range of the available services, increase traffic.	NGN operator
MPS operator	An institution that ensures secure remote interaction of the financial structures, the client and the NGN operator within the mobile payment system. Principal concern: create an extensive network of mobile commerce, increase the number of participants as well as the number of remote transactions, ensure maximum operations security.	Security provider, service provider, client authentication provider
Issuer	Financial and legal institution that issues and services payment instruments. Principal concern: increase the use of the issued payment instruments, increase the number of clients.	Issuer
Acquirer	Financial and legal institution that accepts payments for the products or services on behalf of a merchant. Principal concern: increase the number of transactions of the merchants it services.	Acquirer

Table 1 – Mobile payments system participants

Participant	Description, concern (goal, objective, interest)	Role
Merchant	Corporate entity that provides goods or services and receives payment from the client. Principal concern: promote its goods and services, increase the number of clients, increase the possible ways of payment for the goods and services.	Merchant

The participants may combine the roles depending on the architecture implementation.

Obtaining the required security level described in [ITU-T Y.2740] may require the introduction of the roles of a client application, a client applications distributor, or both. The former is uploaded to clients mobile devices; the latter can be performed by the NGN operator, the mobile payment operator, or by a third party.

When cards of international payment systems are used as payment instruments, the role of the payment system is integral.

6.4 The mobile payment system usage scenarios

6.4.1 Basic usage scenarios

6.4.1.1 Enrol client in MPS

***Aim**:* To subscribe the client to the service within the MPS.

The basic roles: their goals and objectives

Client: to get the opportunity to use the MPS services.

MPS operator: to enrol a new client in the MPS.

Maximum guarantees

The client's consent to the terms and conditions of the MPS use is registered;

The client is registered in the IS of the MPS operator;

The client receives the activation code.

Minimum guarantees

Enrolment is denied to the client with the indication of the cause of denial;

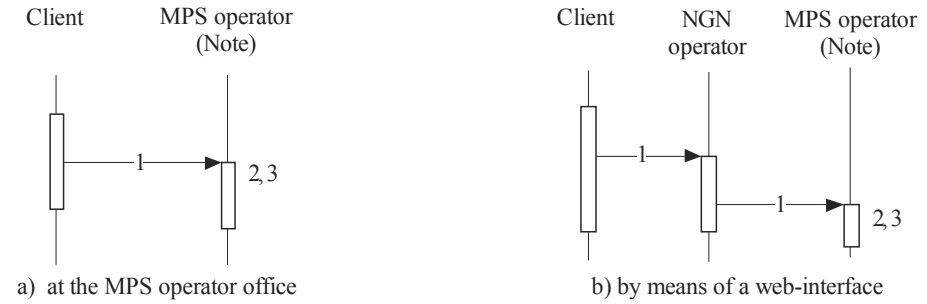
The MPS operator logs the client's cancellation of the enrolment.

Initial data of the scenario

There is no active client profile in the MPS: the client has not been enroled in the MPS or his/her profile has been removed earlier.

Basic steps of the scenario

1. The client initiates the enrolment:
   a) at the office of the MPS operator;
   b) by means of the web-interface: the client is authorized at the MPS operator's website and the request for enrolment is sent.
2. The client is authenticated within the MPS.
3. The MPS operator IS creates client's data, profile in the DB.



NOTE – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F02

Figure 2 – Enrol client in MPS

Alternative steps of the scenario

3. a. The client has been enroled in the MPS (has an active profile):

The MPS operator IS informs the client that the service has been enroled before.

3. b. The client has an account within the MPS but it has been blocked:

The MPS operator IS activates the client's account.

3. c. The MPS operator IS denies registration:

a) The MPS operator IS logs an attempt to connect the service to the client;

b) The MPS operator IS informs the client on the denial to connect the service and specifies the reasons.

6.4.1.2 Enrol payment instrument to be used in the MPS

The client shall register his or her payment instrument. The following conditions shall be met in the process:

– the client shall confirm the authority of using the payment instrument being registered;

– in the process of the registration of the payment instrument, a minimum necessary number of parameters for conducting a remote payment transaction by the client shall be stored into the MPS operator DB;

– the parameters of the payment instrument shall be securely stored on the MPS operator's side in a way that excludes unauthorized access and provides the impossibility of conducting the financial transactions that have not been authorized by the client.

The means of connecting a payment instrument are described in Appendix I.

6.4.1.3 Perform financial operations by the client in home zone within its own payment system

Aim: To provide the possibility to the client to use the financial services of the MPS.

The basic roles: their goals and objectives

Client: to use the services offered by the merchant remotely.

Mobile operator: to transmit the message over communication channels.

MPS operator: to enable the client to pay for the goods and services by means of the MPS.

Merchant: to provide remote services to the client.

Issuer: to provide authorization for and initiate settlement of the client's payment operation.

Acquirer: to transfer authorization response for the operation of the merchant.

The maximum guarantees

The client pays for the service of the merchant.

The merchant provides the service.

The minimum guarantees

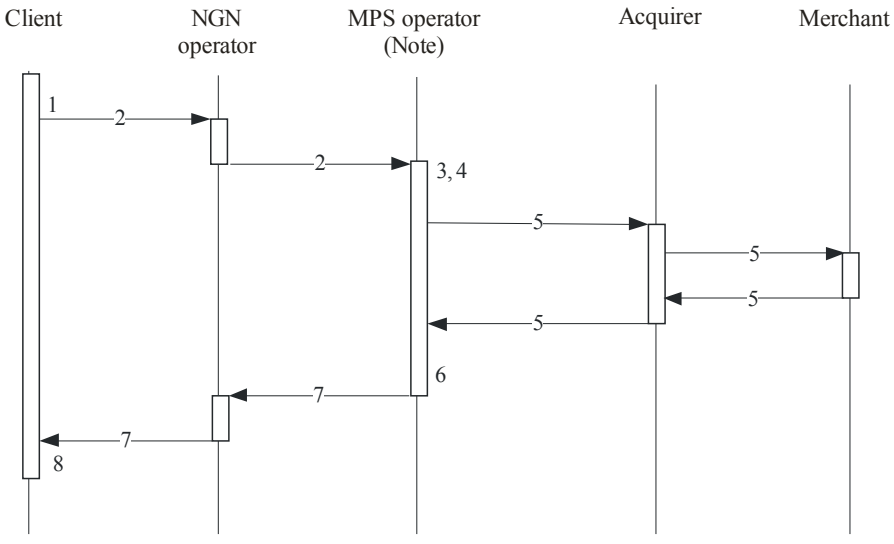
The client is denied to pay for the goods and services of the MPS operator.

Initial data of the scenario

The client is registered in the MPS and has a payment instrument enroled into the MPS.

Basic steps of the scenario

1. By means of his/her mobile device, the client generates a request that contains the parameters of the financial operation and payment instrument;
2. The request is transmitted via the NGN operator channels;
3. The MPS operator receives the request;
4. The client is authenticated;
5. The required financial operation (remittance/payment) is performed using the client's payment instrument details;
6. The operation result is sent to the client;
7. The response is transmitted via the NGN operator channels;
8. The client receives the result of the financial operation.



NOTE – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F03

Figure 3 – Performing financial operations by the client

Alternative steps of the scenario

6. The client is not authenticated

7. The financial operation is not possible

a) Transaction rollback is executed;

b) The operation processing result is returned to the client.

Alternative scenario: the merchant initiates a payment

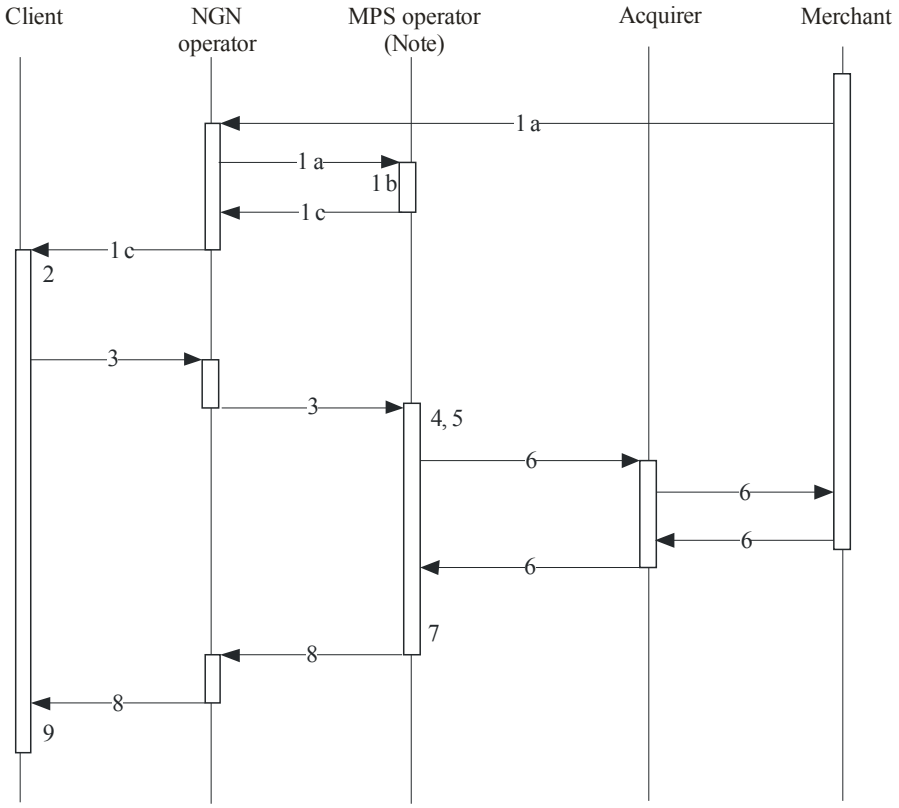
The basic steps of the scenario are as follows

1. a) the merchant generates a payment offer and sends it to the MPS operator;

   b) the MPS operator determines the client and the way to deliver the payment offer to the client;

   c) the request is sent to the client over the NGN operator channels.

2. The client receives the request through his/her mobile device and generates the response that contains the financial operation parameters as well as the parameters of the payment instrument;
3. The request is transmitted via the NGN operator channels;
4. The MPS operator receives the client's response;
5. Authentication of the client;
6. The required financial operation (remittance/payment) is performed using the client's payment instrument details;
7. The operation result is sent to the client;
8. The response is transmitted via the NGN operator channels;
9. The client receives the result of the financial operation.



NOTE – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F04

Figure 4 – Performing payments initiated by merchant

6.4.1.4 Disconnecting the payment instrument from the MPS

Aim: To enable the client to remove the data about payment instrument from the MPS.

The basic roles: their goals and objectives

Client: to disconnect the payment instrument from the MPS.

Mobile operator: to transmit the message via communications channels.

MPS operator: to enable the client to disconnect the payment instrument.

The maximum guarantees

The client disconnects the payment instrument from the MPS.

The minimum guarantees

The client cannot disconnect the payment instrument.

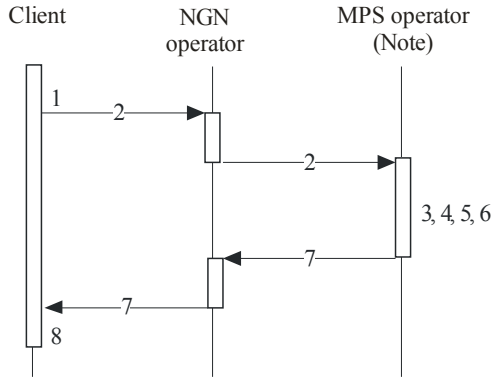
Initial data of the scenario

The client is enroled in the MPS and has the connected payment instrument.

Basic steps of the scenario

1. By means of his/her mobile device, the client generates the request to disconnect a certain payment instrument;
2. The request is transmitted via the NGN operator channels;
3. The MPS operator receives the request;

4. The MPS authenticates the client;
5. The payment instrument is removed from the IS DB;
6. The result of the payment instrument disconnection is sent to the client;
7. The response is transmitted via the NGN operator channels;
8. The client receives the operation result.



NOTE – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F05

Figure 5 – Disconnecting the payment instrument from the MPS

Alternative steps of the scenario

7. Disconnecting the payment instrument from the MPS is denied

a) The MPS operator IS informs the client of the impossibility to disconnect the payment instrument.

6.4.1.5 Disconnecting the client from the MPS

Aim: To disconnect the client from MPS services.

The basic roles: their goals and objectives

Client: to abandon the use of the MPS services.

MPS operator: to make the services inaccessible to the client.

The maximum guarantees

The client's cancellation of MPS services is registered.

The MPS services become inaccessible to the client.

The minimum guarantees

The disconnection from the services is denied to the client; the reason is specified.

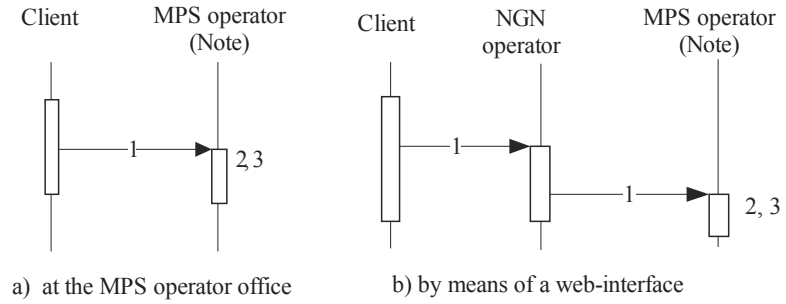
The client cancels the disconnection from the MPS services.

Initial data of the scenario

The client is enroled in the MPS.

Basic steps of the scenario

1. The client initiates the disconnection from the services:
   - at the office of the MPS operator;
   - through the web-interface: the client is authorized through the MPS operator's website and orders the disconnection from the service.
2. The client is authenticated in the MPS.
3. The MPS operator IS feeds the client status changes into the DB (the profile is blocked).
4. The client cannot use the MPS services without a re-enrolment.



NOTE – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F06

Figure 6 – Disconnecting the client from the MPS

Alternative steps of the scenario

1. A payment application is used in the MPS

The client initiates the disconnection from the MPS in the application.

3. The client cannot be disconnected from the MPS services

The MPS operator IS informs the client that the service cannot be disconnected at the moment.

6.4.2 Usage scenario with payment application

6.4.2.1 Receiving the payment application

Aim: To provide the client with the possibility to use the application in the MPS.

The basic roles: their goals and objectives

Client: to receive the payment application to be used in the mobile device.

Client applications distributor: to provide the client with the application.

The maximum guarantees

The client receives the application.

The minimum guarantees

The application is denied to the client.

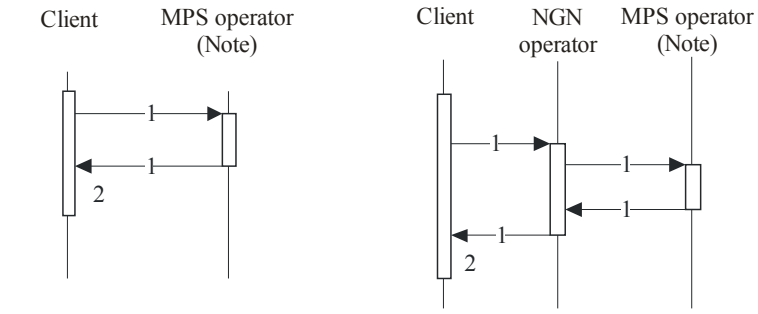
The client has no possibility to use the received application because of some technical characteristics of the mobile device.

Initial data of the scenario

The client is enroled in the MPS and possesses a technical possibility to use the application.

Basic steps of the scenario:

1. The client receives the application from the client applications distributor:
   - at the client applications distributor office;
   - through the web-interface (at the client applications distributor website).
2. The client is enabled to use the application on the mobile device.



a) at the MPS operator office b) by means of a web-interface

NOTE – Client applications distributor.

ITU-T Y.2741(11)_F07

Figure 7 – Receiving the payment application

Alternative steps of the scenario

1. a. The client receives the updated version of the application

The client has received the application before.

1. b. The client does not receive the application

The client requests help from the support service of the client applications distributor.

6.4.2.2 Activating the payment application

Aim: To activate the client's payment application.

The basic role: their goals and objectives

Client: to get the possibility to use the MPS services by means of the application.

MPS operator: to validate the use of the given payment application in the MPS by the given client.

Mobile operator: to transmit the message via communications channels.

The maximum guarantees

The client activates the application.

The client keys are loaded into the application.

The client keys are fed into the MPS operator IS DB.

The minimum guarantees

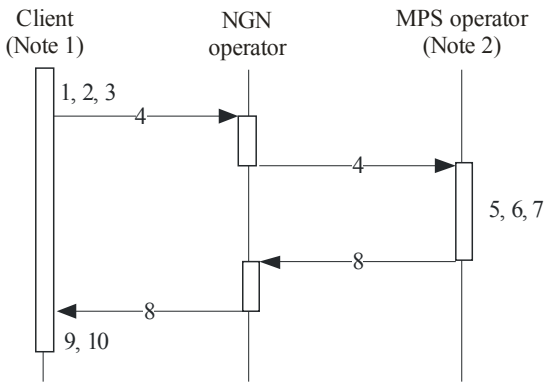
The activation of the application is denied to the client; the cause of denial is specified.

Initial data of the scenario

The client is enroled in the MPS, has the activation code and the application in the mobile device.

Basic steps of the scenario

1. The client selects "activation" in the application menu;
2. The client presents the activation code received during the enrolment procedure, to the application;
3. The application generates and sends a request to the MPS;
4. The request is transmitted via the NGN operator channels;
5. The MPS operator receives the enquiry. The activation code is verified;
6. The client keys are generated and stored in the MPS provider IS DB;
7. The keys and the activation result are sent to the client;
8. The response is transmitted via the NGN operator channels;
9. The client application receives the message, stores the client keys, and the activation result is displayed to the client;
10. The client receives the access to the MPS services in the application.



NOTE 1 – Client, payment instrument, payment application.

NOTE 2 – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F08

Figure 8 – Activating the payment application

Alternative steps of the scenario

5. Error in the activation code validation:

a) The MPS operator IS informs the client that the activation code is entered incorrectly;

b) The client's account is blocked if the limit of attempts to enter the activation code is exceeded.

6.4.3 Intersystem interaction usage scenarios

This Recommendation deals with general issues and offers basic scenarios of the interaction.

6.4.3.1 Performing financial transactions when the client is in the roaming

Aim: To make it possible for the client to use the enabled MPS service when outside the operator coverage area (home zone).

The basic roles: their goals and objectives

Client: to get the possibility to pay for the services using the MPS when abroad the home zone.

Mobile operator: to transmit the message over communications channels.

MPS operator: to enable the client to pay for the goods and services by means of the MPS.

Merchant: to render remote services to the client.

Issuer: to provide authorization for and initiate settlement of the client's payment operation.

Acquirer: to transfer authorization response for the operation of the merchant.

The maximum guarantees

The client pays for the service of the merchant.

The merchant renders the service.

The minimum guarantees

The client is denied to pay for the goods and services of the MPS operator.

Initial data of the scenario

The client is registered for MPS; the client is in the roaming area (outside the home zone) and has a connected payment instrument.

Basic steps of the scenario

The basic scenario steps are similar to the ones described in the scenario of the financial transaction within the home zone. The client request and the transaction result from the roaming zone and back to the home zone are performed under the roaming rules and are not covered in this Recommendation.

6.4.3.2 Performing financial operations by the client in another MPS

Aim: To enable the client to use the services of a different MPS which the client is not enroled to.

The basic roles: their goals and objectives

Client: to obtain the possibility to pay for the services provided by the merchant located in the coverage zone of a different MPS.

Mobile operator: to transmit the message over communications channels.

MPS operator: to enable the client to pay for the goods and services by means of another MPS.

Merchant: to render remote services to the client.

Issuer: to provide authorization for and initiate settlement of the client's payment operation.

Acquirer: to transfer authorization response for the operation of the merchant.

The maximum guarantees

The client pays for the service of the merchant.

The merchant renders the service.

The minimum guarantees

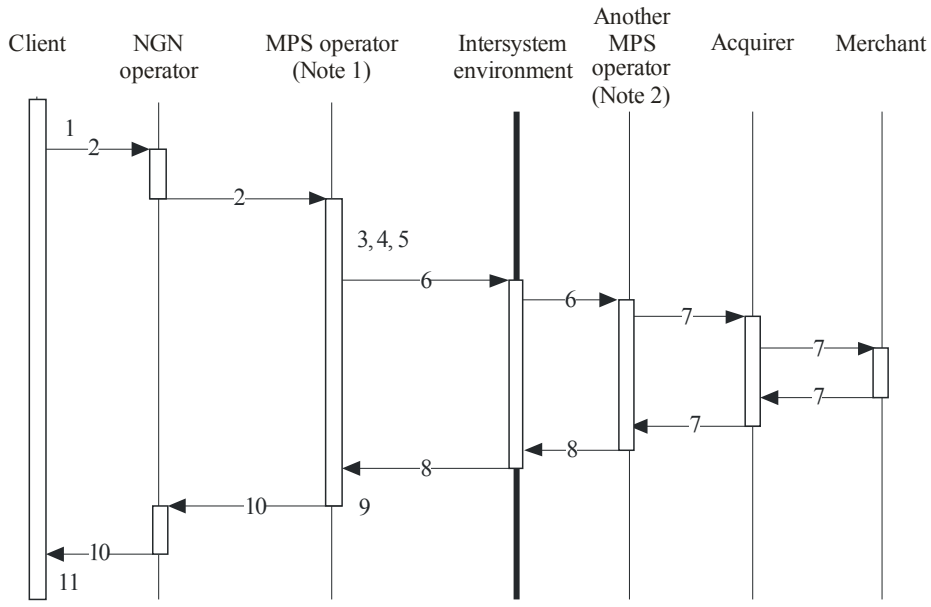
The client is denied to pay for the goods and services of the MPS operator.

Initial data of the scenario

The client is registered for MPS, has a connected payment instrument and is aware of the merchant details necessary for the payment transaction.

Basic steps of the scenario

1. The client generates a request by means of his/her mobile phone. The request contains the financial transaction parameters including payment ID and the parameters of the payment instrument;
2. The request is transmitted over the operator communications channels;
3. The MPS operator receives the request;
4. The client is authenticated;
5. The MPS operator is identified by payment ID;
6. The request is transmitted to the addressee (the operator of a different MPS) over the intersystem secure channels;
7. The required financial transaction using the client payment instrument details is performed;
8. The transaction result is sent to the client's home MPS;
9. MPS generated the response to the client;
10. The response is transmitted over the operator communications channels;
11. The client receives the transaction result.



NOTE 1 – Security provider, client authentication provider, service provider.
NOTE 2 – Security provider, service provider.

ITU-T Y.2741(11)_F09

Figure 9 – Performing financial operations by the client in another MPS

Alternative steps of the scenario

4. The client is not authenticated.

5. MPS cannot be identified.

7. The financial operation is not possible:

a) Transaction rollback is executed;

b) The operation performance result is returned to the client.

7 Transition from the token payment systems

Some operators have introduced services that enable the transfer of monetary and non-monetary tokens as payment for goods and services, within (and sometimes between) the NGN operators' billing systems.

Although these services are often represented as conducive for the development of immature economies with large proportions of non-banked population, in the long term these services can be disruptive to the fiscal and monetary systems of these economies.

Developing countries face a wide range of issues associated with cash-related crime. Development of electronic banking systems in such countries reduces the amount of cash in circulation, and thus leads to the reduction of cash-related crime.

The NGN operators offering token payment services should therefore develop roadmaps for the migration of these token payment systems to systems using financial transactions for the exchange of value.

Appendix I

Enrol a payment instrument in the system

(This appendix does not form an integral part of this Recommendation.)

Aim: To provide the client with the possibility to use his/her payment instrument in the MPS.

The basic roles: their goals and objectives

Client: to have an opportunity to take advantage of the MPS using a payment instrument.

Mobile operator: to transmit the message via communications channels.

MPS operator: to approve the use of the given payment application in the MPS by the given client.

Client authentication provider: to authenticate the client and his/her payment instrument.

The maximum guarantees

The client receives an opportunity to take advantage of the MPS to use the payment instrument.

The minimum guarantees

The given payment instrument is denied to be used by the client.

Initial data of the scenario

The client is enroled in the MPS and has a payment instrument.

Basic steps of the scenario

1. By means of his/her mobile device, the client transmits the payment instrument parameters to the MPS operator;
2. The request is transmitted via the NGN operator channels;
3. The MPS operator receives the request;
4. The MPS operator IS generates a random amount;
5. The MPS operator sends a request to reserve this amount at the given payment instrument to the acquirer system. Acquirer sends a request for authorization to the issuer of the payment instrument. The client shall contact the issuer and find out the amount to confirm that he/she is the legitimate owner of payment instrument;
6. The issuer of the payment instrument authenticates the client using its standard means of authentication;
7. After authentication, the issuer informs the client about the value of the reserved amount;
8. The client transmits the value to the MPS operator via the client application;
9. The request is transmitted via the NGN operator channels;
10. Upon receiving the value of the reserved amount from the client, the MPS operator compares it with the previously generated one;
11. Provided that both amounts coincide, the MPS operator stores the information on the payment instrument for further usage in the secure storage, and sends notification with the operation result to the client;
12. Simultaneously, the request is sent to the issuer (via the acquirer) to cancel the amount reservation at the payment instrument.

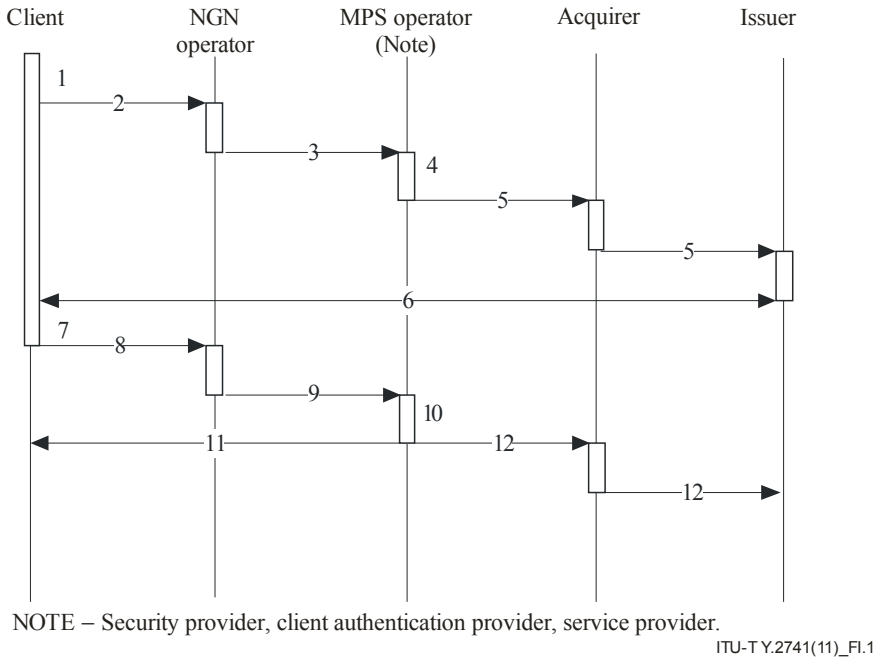


Figure I.1 – Enrol payment instrument in MPS

Alternative steps of the scenario

10. The value of the previously reserved amount does not coincide with the one entered by the client

The client receives an error notification. When the number of failed attempts exceeds three, the mobile device client's profile is blocked in the MPS system. The reserved amount is cancelled.

Appendix II

Mobile banking and mobile commerce systems implementation models

(This appendix does not form an integral part of this Recommendation.)

This appendix describes the examples of basic mobile banking and mobile commerce systems implementation models subject to the implemented security level.

The following terms are used in this appendix:

Message transmission channel: A means of transferring a client's request to perform a financial operation (money transfer) which requires a remote access to payment instruments. Examples of message transmission channels include SMS messages, USSD requests, batch communication (GPRS, EDGE, 3G data, HSDPA, etc.).

Payment instrument: A set of legal measures to perform a remittance, both cash and non-cash, for the purpose of making a payment. Examples of payment instruments include bank accounts, operator accounts and bank cards.

Available operations: A list of operations available in the system of a certain security level.

Restrictions: Limitations for using the system as provided by the accepted risk model that are legally stated or reserved in mutual contracts.

Predefined phone: A phone number previously indicated by the client in a special form of the service provider.

Ad hoc phone: A phone number indicated by the client directly when making a payment.

Predefined account: An account number previously indicated by the client in a special form of the service provider.

Ad hoc account: An account number indicated by the client directly when making a payment.

Predefined payment: A payment made under previously provided parameters where a payment recipient can be selected from the list defined by the MPS service provider (e.g., payment made by an individual person to a corporate entity for the provided services).

Ad hoc payment: A payment made by the client for the services that are not included in the list defined by the MPS service provider on condition that making such payment is technically realizable. Precondition: it is obligatory that either the service provider should have a channel to interoperate with the MPS provider or the service should be provided by another MPS provider and interoperation should be established between the two.

Automatic payment: A regular and automatic payment initiated by the MPS service provider with the prior client's consent.

Automatic payment with confirmation: A regular and automatic payment initiated by the MPS service provider with the client's consent.

Payment initiated by merchant: A payment whose parameters are determined and entered by the merchant. The client can either confirm or reject processing the offered payment.

Information service: A range of information services provided by the MPS system provider that are not associated with conducting financial operations (e.g., viewing a payment instrument balance, providing reference information).

Mobile banking and mobile commerce systems implementation models

Possible models of the mobile banking and mobile commerce systems subject to the implementation of the security levels are covered below. Each implementation model imposes certain requirements on payment instrument, available operations, restrictions and application used in the system.

II.1 The implementation of the system without the use of the client application

It corresponds to level 1 and level 2 of the system security (see [ITU-T Y.2740]).

Message transmission channel: Plain text SMS messages, USSD requests,

Payment instrument: Payments from bank accounts and operator accounts predefined in the service agreement.

Available operations: Payments are made only to recipients previously defined in the contract. A list of possible operations should be specified when signing a contract:

- Payment for a predefined phone;
- Payment into a predefined account;
- Making a predefined payment;
- Making automatic payments;
- Making automatic payments with confirmation;
- Information service.

Restrictions: Maximum payment limits which may include transaction amount limits, intraday transaction limits; restriction on available financial transactions which implies payments only for previously agreed services.

II.2 The implementation of the system with the use of the client application

It corresponds to level 3 and level 4 of the system security (see [ITU Y.2740]).

Message transmission channel: SMS messages, batch communication (GPRS, EDGE, 3G data, HSDPA, etc.). The message transmission channel and the message being transmitted must be encrypted using strong cryptography.

Payment instrument: Payments from bank and operator accounts predefined in the service agreement, payments using bank cards as well as the cards of international payment systems (payments include the transmission of critical data over the communications channels).

Available operations: Remote connection to the system is possible; a wide range of payments for various services connected to the system; the possibility to considerably increase the number of operations implemented within the MPS (introducing new payments and services; connecting new merchants); the list of available payments can be flexibly defined by both the service provider and the client; different MPS can interoperate in providing services. The following operations are possible to be implemented:

- Payment for a predefined phone;
- Payment into a predefined account;
- Making a predefined payment;
- Making automatic payments;
- Making automatic payments with confirmation;
- Information service;
- Payment for an ad hoc phone;

- Payments into an ad hoc account;
- Ad hoc payments;
- Payments initiated by a merchant.

Restrictions: Restrictions on payments are determined in the mutual contracts of the system participants.

Application: Using the application is obligatory to provide security (encryption of messages) as well as convenient system usage.

Bibliography

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011