

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

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/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Page

1	Scope	1
2	References.....	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Roles, risks, participants, and scenarios of mobile payments in NGN.....	2
6.1	Roles within the mobile commerce and mobile banking systems.....	2
6.2	Risks in the MPS and MPS security levels	3
6.3	Participants and the system architecture of mobile commerce and mobile banking	3
6.4	The mobile payment system usage scenarios	5
7	Transition from the token payment systems.....	16
	Appendix I – Enrol a payment instrument in the system.....	17
	Appendix II – Mobile banking and mobile commerce systems implementation models	19
II.1	The implementation of the system without the use of the client application	20
II.2	The implementation of the system with the use of the client application	20
	Bibliography.....	22

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.

Document Sharing Hub