国　际　电　信　联　盟

ITU-T

国际电联电信标准化部门

Y.2741

(01/2011)

Y系列：全球信息基础设施，互联网的协议问题和下一代网络

下一代网络 – 安全

下一代网络中的安全移动金融交易架构

ITU-T Y.2741建议书

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200-Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
运行于NGN的IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
智能泛在网络	
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
电信级开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3099

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2741建议书

下一代网络（NGN）中的安全移动金融交易架构

摘要

ITU-T Y.2741建议书对下一代网络（NGN）环境中移动商务和移动银行安全解决方案的总体架构做出规范，具体阐述架构的主要参与方、各方作用以及移动商务和移动银行系统的操作情形。本建议书还提供移动商务和移动银行系统实施模式示例。

历史纪录

版本	建议书	批准时间	研究组	
1.0	ITU-T Y.2741	2011-01-28	13	

关键词

移动银行、移动商务、移动支付、远程支付、安全和安全性

前言

国际电信联盟（国际电联）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电联的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会(WTSA)确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织(ISO)和国际电工委员会(IEC)合作制定的。

注

本建议书为简要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款(以确保例如互操作性或适用性等)，只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们通过下列网址查询电信标准化局(TSB)的专利数据库： http://www.itu.int/ITU-T/ipr/.

目录

页码

1 范围 1

2 参考文献 1

3 定义 1

3.1 其它文献规定的术语 1

3.2 本建议书规定的术语 1

4 缩写词和首字母缩略语 2

5 约定 2

6 NGN中移动支付（各方）的作用、风险、参与方和不同情形 2

6.1 移动商务和移动银行系统内（各方）的作用 2

6.2 移动支付系统（MPS）中的风险和MPS的安全等级 3

6.3 移动商务和移动银行的参与方及系统架构 3

6.4 移动支付系统的使用情形 5

7 从代币支付系统的过渡 16

附录I – 在系统中登记支付工具 17

附录II – 移动银行和移动商务系统的实施模式 19

II.1 在不使用客户应用的前提下实施系统 20

II.2 在使用客户应用的前提下实施系统 20

参考书目 22

ITU-T Y.2741建议书

下一代网络中的安全移动金融交易架构

1 范围

本建议书对下一代网络（NGN）中的远程移动金融交易安全架构做出定义，该范围不包括所有其它金融交易，以及使用货币或非货币代币进行资产转移的交易。

NGN 通过组织管理灵活和功能个性化的繁复多样的业务，能够提供方便的移动支付系统（MPS）服务接入。

2 参考文献

下列 ITU-T 建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的 ITU-T 建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T Y.2740] ITU-T Y.2740建议书(2011) –下一代网络中远程移动金融交易的安全要求

3 定义

3.1 其它文献规定的术语

本建议书采用其它文献规定的下列术语：

3.1.1 下一代网络（Next Generation Network，NGN）[b-ITU-T Y.2001]：能够利用宽带和具有QoS机制的传输技术的，可以提供电信业务的基于包交换的网络。该网络中提供的与业务相关的功能独立于底层与传输相关的技术。该网络允许用户不受限地接入网络，可以自由选择服务提供商和/或业务。该网络支持通用移动性，使得网络可以随时随地向用户提供业务。

3.2 本建议书规定的术语

本建议书定义了下列术语：

3.2.1 应用（application）：上传至客户（用户）移动装置的特殊移动银行或移动商务应用。

3.2.2 银行账户（bank account）：个人或企业实体在一国的国家货币主管当局（如中央银行）授权的银行或其它金融机构持有的电子资金账户，可用于货物和服务（费用）的支付。

3.2.3 客户（client）：针对电信业务和移动商务系统的使用签署合同协议的个人或企业实体。

3.2.4 金融交易（financial transaction）：买卖双方之间按照合同条件对资产交换进行支付的事件或条件。

3.2.5 系统间环境（intersystem environment）：方便多种不同移动银行和移动商务系统之间建立互动的一套规则或系统。

3.2.6 移动装置（mobile device）：在NGN无线网络上用于通信的电子装置。

3.2.7 移动金融交易（mobile financial transaction）：使用移动装置启动和/或授权的金融交易。

3.2.8 移动支付系统（mobile payment system, MPS）：移动银行和/或移动商务系统。

3.2.9 货币代币（monetary token）：以一国的国家货币单位代表和衡量的、用于支付的电子或物理人工制品，但它并不存储于银行账户，也不与该账户直接联系。

电子货币代币的示例之一是储存在自成一体的电子钱包之中、不由银行账户映射的电子现金。物理货币代币包括硬币、纸币、旅行支票等。

3.2.10 非货币代币（non-monetary token）：并非由国家货币单位代表的、用于支付的电子或物理人工制品。电子非货币代币示例包括NGN签约用户账户中的未使用“分钟数”或“短信（SMS）数”，NGN运营商允许将这些从一个签约用户账户转至另一个账户。

3.2.11 支付身份（payment ID）：明确确定付款接收方身份的必备请求参数。在实施系统间环境中必须有商家身份和移动支付系统（MSP）身份（移动支付系统的独特识别符）。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

DB 数据库

ID 身份

IS 信息系统

MPS 移动支付系统

NGN 下一代网络

5 约定

无。

6 NGN中移动支付（各方）的作用、风险、参与方和不同情形

6.1 移动商务和移动银行系统内（各方）的作用

MPS 参与方的基本作用和职责为：

- 客户是拥有进行支付操作的支付工具的移动签约用户。
- 客户应用是上传到客户移动装置（电话、SIM卡、通信机等）中的特殊软件，旨在进行安全的移动支付操作。

- 支付工具是用于支付货物和服务（费用）的金融工具。
- NGN运营商提供客户与MPS进行远程互动、数据路由和传送的移动通信网络。
- 客户应用分销商是将应用提供给客户的参与方。
- 安全提供商是通过通信渠道提供数据传送安全的参与方。
- MPS运营商（服务提供商、支付网关）是确保MPS之内的互动并为最终用户提供支付服务的参与方。
- 发行方是发行支付工具的金融机构。
- 客户认证提供商确认客户操作。
- 受让方是维护商家关系并从商家接收所有金融交易的金融机构。
- 支付系统是确保银行间支付交易的组织。

6.2 移动支付系统（MPS）中的风险和MPS的安全等级

本款阐述在进行远程移动支付时可能出现的信息安全风险。这些风险包括但不限于：

- 失密风险 – 未经授权第三方获取保密信息。
- 完整性被破坏的风险 – 信息在传送或处理过程中失真。
- 伪造电子文件的风险 – 由未得到授权的一方生成文件。
- 否认风险 – 否认是电子文件的原作者。
- 有意或无意销毁信息的风险。
- 交易风险 – 例如由于移动通信不稳定，无法完成交易。
- 根据所实施的基于风险的安全机制，存在具有四个安全等级的系统[ITU-T Y.2740]。

6.3 移动商务和移动银行的参与方及系统架构

MPS 架构应遵循金融、法律和商务机构的已有相互关系系统之中，并方便系统参与方进行基于预计风险水平的必要安全程度的移动支付交易。建议架构应支持系统参与方在进行支付交易时已经采用的方案设计和规范。

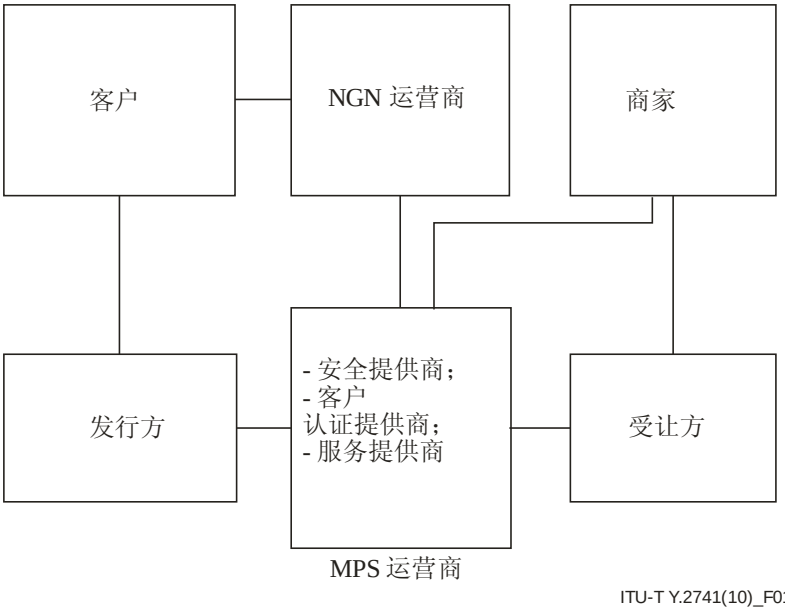


图1 – 移动商务和移动银行的参与方及系统架构

表1：移动支付系统的参与方

参与方	描述、关注（总体目标、具体目标、利益）	作用
客户	已就电信服务和移动商务系统的使用签订合同协议的个人或企业实体。 拥有移动装置和支付工具。 主要关注：增加服务数量，有可能进行安全的远程金融交易，扩大支付工具的范围。	客户
NGN运营商	为客户提供数字通信服务的机构。 主要关注：增加客户数量，扩大现有服务的范围，增加流量。	NGN运营商
MPS运营商	确保移动支付系统内金融机构、客户和NGN运营商之间进行安全远程互动的机构。 主要关注：创建广泛的移动商务网络，增加参与方以及远程交易的数量，确保实现最大操作安全性。	安全提供商、服务提供商、客户认证提供商
发行方	发行服务支付工具的金融和法律机构。 主要关注：扩大已发行的支付工具的使用，增加客户数量。	发行方
受让方	代表商家接收产品或服务支付的金融和法律机构。 主要关注：增加其服务的商家的交易数量。	受让方

表1：移动支付系统的参与方

参与方	描述、关注（总体目标、具体目标、利益）	作用
商家	提供货物或服务并接收客户支付的企业实体。 主要关注：宣传推广其货物和服务，增加客户数量，增加货物和服务（费用）支付的可能方法。	商家

根据架构实施情况，参与方可将不同作用相互合并。

为达到[ITU-T Y.2740]中要求的安全等级，可能需要介绍客户应用的作用、客户应用分销商的作用或两者的作用。前者上传到客户移动装置中；后者可由 NGN 运营商、移动支付运营商或第三方完成。

当使用国际支付系统卡作为支付工具时，支付系统的作用是必不可少的。

6.4 移动支付系统的使用情形

6.4.1 基本使用情形

6.4.1.1 客户在MPS中进行登记

目的：在MPS中对客户进行登记，使其使用服务。

基本角色：总体目标和具体目标

客户：获得使用MPS服务的机会。

MPS运营商：在MPS中登记新的客户。

最大保证

客户对使用MPS的条款和条件的同意得到注册

客户在MPS运营商的IS中得到注册

客户接收启动代码

最小保证

拒绝客户登记，指明拒绝原因

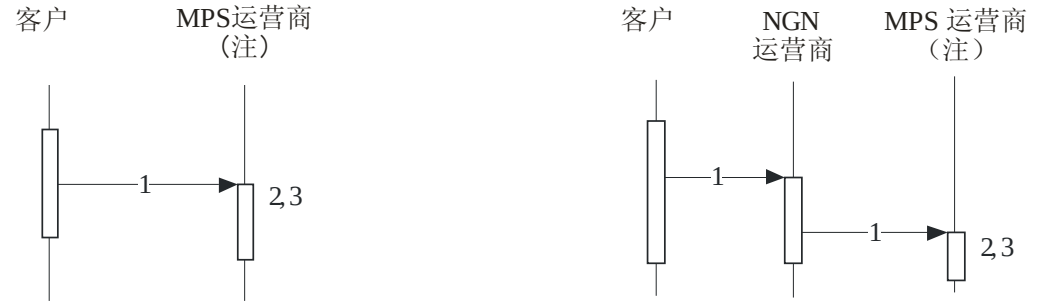
MPS运营商对客户登记取消予以记录

情形的初始数据

MPS中没有在用客户资料：客户尚未在MPS中登记或他/她的资料已被清除。

情形的基本步骤

1. 客户启动登记：
   a) 在MPS运营商办公室进行；
   b) 通过网络界面进行：客户在MPS运营商网站上得到授权并发出登记请求。
2. 客户在MPS内得到认证。
3. MPS运营商的IS在数据库中（DB）创建客户数据和资料。



a) 在MPS运营商办公室进行　　b) 通过网络界面进行

注 -安全提供商、客户认证提供商、服务提供商

ITU-T Y.2741(10)_F02

图2 – 客户在MPS中进行登记

情形的备选步骤

***3. a.*　客户已在MPS中登记（拥有在用资料）：**

MPS运营商的IS通知客户此前已登记过服务。

***3. b.*　客户在MPS内拥有账户，但已被封存：**

MPS运营商的IS激活客户账户。

***3. c.*　MPS运营商的IS拒绝注册：**

a) MPS运营商的IS对服务与客户连接的尝试予以记录；

b) MPS运营商的IS通知客户拒绝将其连接至服务，并说明具体理由。

6.4.1.2　应在MPS中使用的登记支付工具

客户须对其支付工具进行注册。在此过程中须满足下列条件：

– 客户须确认使用正在得到注册的支付工具的权利；

– 在注册支付工具过程中，须向MPS运营商数据库存入客户进行远程支付交易的、最少数量的必要参数；

– 支付工具参数须安全存储于MPS运营商一侧，须排除一切未得到授权的接入，并提供不可能进行客户未予授权的金融交易的可能性。

附录 I 具体说明连接支付工具的手段。

6.4.1.3　客户在其自身支付系统的归属区（home zone）内进行金融操作

目的：为客户提供使用MPS金融服务的可能性。

基本角色：总体目标和具体目标

客户：使用商家远程提供的服务。

移动运营商：通过通信渠道传送信息。

MPS运营商：方便客户通过MPS支付货物和服务费用。

商家：为客户提供远程服务。

发行方：为客户支付操作提供授权和初始结付。

受让方：传送商家操作的授权回复。

最大保证

客户支付商家提供服务的费用。

商家提供服务。

最小保证

拒绝客户支付MPS运营商的货物和服务费用。

情形的初始数据

客户在MPS中得到注册，并拥有已登记在MPS中的支付工具。

情形的基本步骤

1. 客户通过他/她的移动装置，生成包含金融操作参数和支付工具的请求；
2. 请求通过NGN运营商渠道传送；
3. MPS运营商接收请求；
4. 客户得到认证；
5. 使用客户支付工具细节进行所要求的金融操作（汇款/付款）；
6. 操作结果发至客户；
7. 通过NGN运营商渠道传送回复；
8. 客户接收金融操作结果。

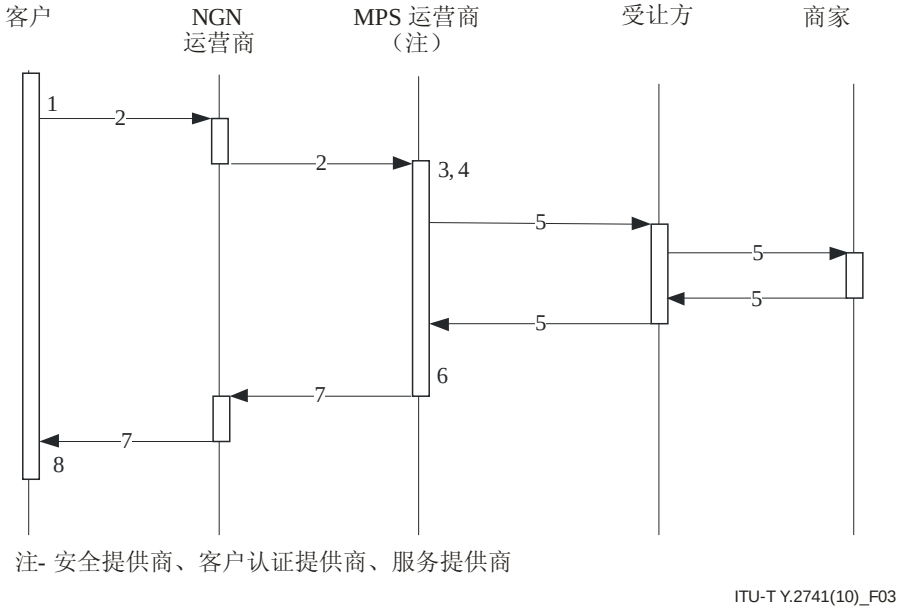


图3 – 客户进行金融操作

情形的备选步骤

6. **客户未得到认证**

7. **不可能进行金融操作**

a) 执行交易回滚；

b) 将操作处理结果返回客户。

备选情形：商家启动支付

情形的基本步骤如下

1. a) 商家提出支付要约（offer）并发至MPS运营商；

   b) MPS运营商确定客户以及向客户提供支付要约的方法；

   c) 通过NGN运营商渠道将请求发至客户。

2. 客户通过他/她的移动装置接收请求，并生成包含金融操作参数以及支付工具参数的回复；

3. 请求通过NGN运营商渠道传送；

4. MPS运营商接收客户的回复；

5. 对客户进行认证；

6. 使用客户支付工具细节进行所要求的金融操作（汇款/付款）；

7. 将操作结果发至客户；

8. 通过NGN运营商渠道传送回复；

9. 客户接收金融操作结果。

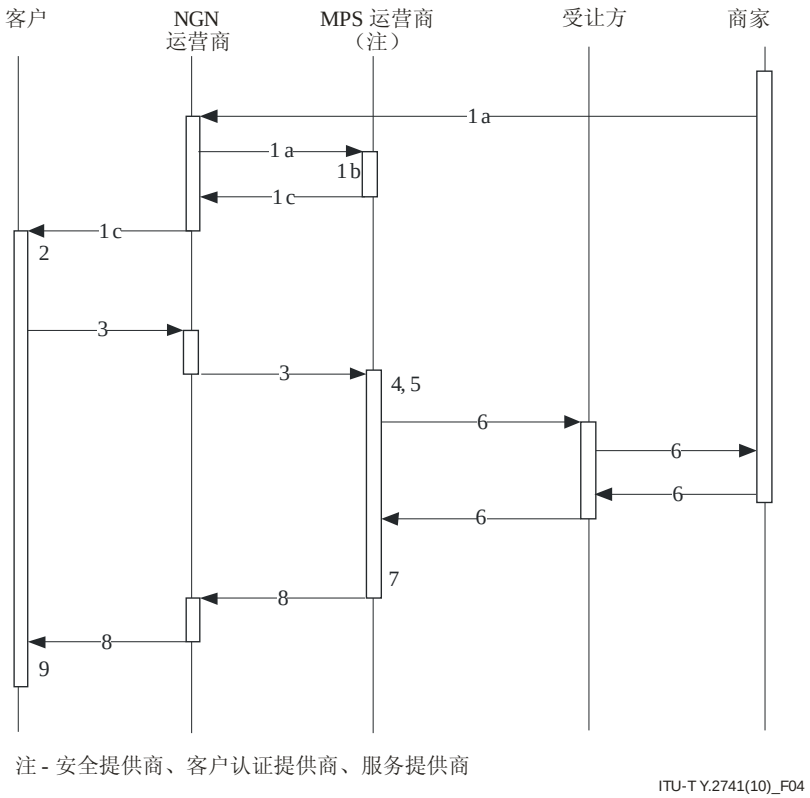


图4 – 进行商家启动的支付

6.4.1.4 将支付工具与MPS断开

目的：方便客户从MPS中去除有关支付工具的数据。

基本角色：总体目标和具体目标

客户：将支付工具与MPS断开；

移动运营商：通过通信渠道传送信息；

MPS运营商：方便用户断开支付工具。

最大保证

客户将支付工具与MPS断开。

最小保证

客户无法断开支付工具。

情形的初始数据

客户在MPS中登记并拥有得到连接的支付工具。

情形的基本步骤

1. 客户通过他/她的移动装置生成有关断开某个支付工具的请求；
2. 请求通过NGN运营商渠道传送；
3. MPS运营商接收请求；

4. MPS对客户进行认证；
5. 从IS数据库中去除支付工具；
6. 支付工具断开结果发至客户；
7. 通过NGN运营商渠道传送回复；
8. 客户接收操作结果。

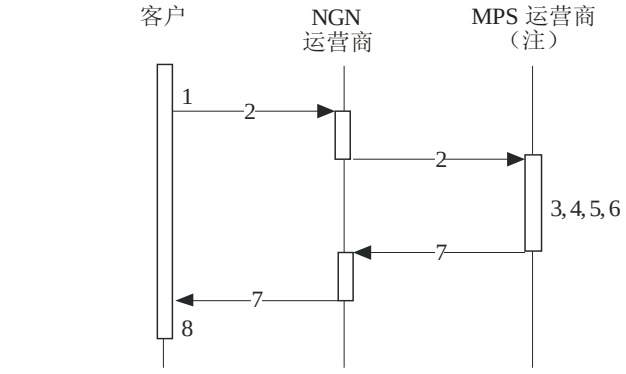


图5 – 将支付工具与MPS断开

情形的备选步骤：

7. 拒绝将支付工具与MPS断开

a) MPS运营商的IS通知客户不可能断开支付工具。

6.4.1.5 将客户与MPS断开

目的：将客户与MPS服务断开。

基本角色：总体目标和具体目标

客户：放弃使用MPS服务。

MPS运营商：使客户无法获得服务。

最大保证

客户取消MPS服务得到注册。

客户无法获得MPS服务。

最小保证

拒绝将客户与服务断开，并具体说明理由。

客户取消与MPS服务的断开。

情形的初始数据

客户在MPS中登记。

情形的基本步骤

1. 客户通过下列方式与服务断开：
   - 在MPS运营商办公室；
   - 通过网络界面进行：客户通过MPS运营商网站得到授权并发出与服务断开的指令。
2. 客户在MPS中得到认证。
3. MPS运营商的IS将客户状态变化输入数据库中（资料被封存）。
4. 客户不重新登记则不能使用MPS服务。

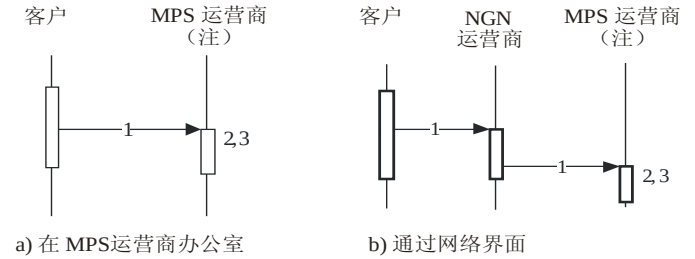


图6 – 将客户与MPS断开

情形的备选步骤

1. ***在MPS中使用支付应用***

客户在应用中启动与MPS的断开。

3. ***客户无法与MPS服务断开***

MPS运营商的IS通知客户目前无法断开服务。

6.4.2 支付应用的使用情形

6.4.2.1 接收支付应用

目的：为客户提供在MPS中使用应用的可能性。

基本角色：总体目标和具体目标

客户：接收将在移动装置中使用的支付应用。

客户应用分销商：为用户提供应用。

最大保证

客户接收应用。

最小保证

拒绝客户使用应用。

由于移动装置的某些技术特性，客户无法使用收到的应用。

情形的初始数据

客户在MPS中登记，并拥有使用应用的技术可能性。

情形的基本步骤

1. 客户从客户应用分销商处接收应用：
   - 在客户应用分销商办公室；
   - 通过网络界面（在客户应用分销商网站上）。
2. 客户能够在移动装置上使用该应用。

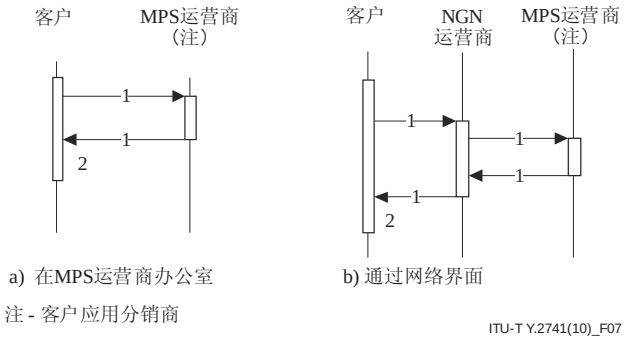


图7 – 接收支付应用

情形的备选步骤

1. a. **客户收到最新版本的应用**

客户此前收到过应用。

1. b. **客户不接收应用**

客户请求客户应用分销商提供支持服务。

6.4.2.2 激活支付应用

目的：激活客户的支付应用。

基本角色：总体目标和具体目标

客户：获得通过该应用使用MPS服务的可能性。

MPS运营商：确认特定客户在MPS中使用特定支付应用。

移动运营商：通过通信渠道传送信息。

最大保证

客户激活应用。

客户密钥载入应用。

客户密钥输入MPS运营商的IS数据库中。

最小保证

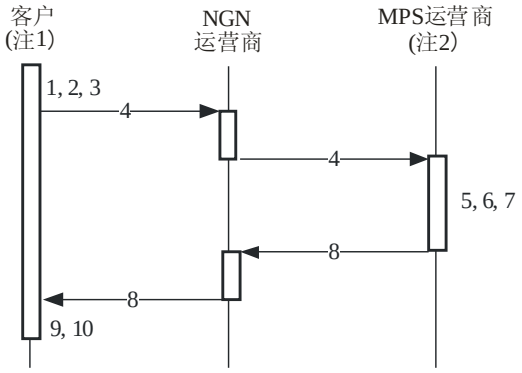
拒绝为客户激活应用；具体说明拒绝的理由。

情形的初始数据

客户在MPS中登记，并在移动装置中拥有激活代码和应用。

情形的基本步骤

1. 客户在应用菜单中选择“激活”；
2. 客户向应用介绍在登记过程中收到的激活代码；
3. 应用生成并向MPS发出请求；
4. 请求通过NGN运营商渠道传送；
5. MPS运营商接收查询，激活代码得到验证；
6. 生成客户密钥并在MPS提供商的IS数据库中加以存储；
7. 密钥和激活结果发至客户；
8. 通过NGN运营商渠道传送回复；
9. 客户应用接收信息、存储客户密钥并向客户显示激活结果；
10. 客户在应用中接收对MPS服务的接入。



注 1 - 客户、支付工具、支付应用
注 2 - 安全提供商、客户认证提供商、服务提供商

ITU-T Y.2741(10)_F08

图8 – 激活支付应用

情形的备选步骤

***5.* 激活代码确认错误：**

a) MPS运营商的IS通知客户激活代码输入错误；
b) 如果输入激活代码的尝试次数超过限制则封存客户账户。

6.4.3 系统间互动使用情形

本建议书阐述一般性问题，并提供互动的基本情形。

6.4.3.1 客户在漫游过程中进行金融交易

目的：使客户能够在运营商覆盖区（归属区）以外使用已使能的MPS服务。

基本角色：总体目标和具体目标

客户：具有在归属区以外对使用MPS的服务进行支付的可能性。

移动运营商：通过通信渠道传送信息。

MPS运营商：使客户能够通过MPS支付货物和服务费用。

商家：向客户提供远程服务。

发行方：为客户支付操作提供授权和初始结付。

受让方：传送商家操作的授权回复。

最大保证

客户支付商家服务的费用。

商家提供服务。

最小保证

拒绝客户支付MPS运营商货物和服务的费用。

情形的初始数据

客户在MPS中注册，并处在漫游区（归属区以外），同时拥有得到连接的支付工具。

情形的基本步骤

情形的基本步骤与归属区金融交易情形的步骤类似。客户请求和交易结果从漫游区返回到归属区的工作按照漫游规则进行，不属于本建议书的范围。

6.4.3.2 客户在另一个MPS中进行金融操作

目的：使客户能够使用客户未登记的一个不同MPS的服务。

基本角色：总体目标和具体目标

客户：获得支付位于不同一个MPS覆盖区的商家服务费用的可能性。

移动运营商：通过通信渠道传送信息。

MPS运营商：使客户能够通过另一个MPS支付货物和服务费用。

商家：为客户提供远程服务。

发行方：为客户支付操作提供授权和初始结付。

受让方：传送商家操作的授权回复。

最大保证

客户支付商家服务的费用。

商家提供服务。

最小保证

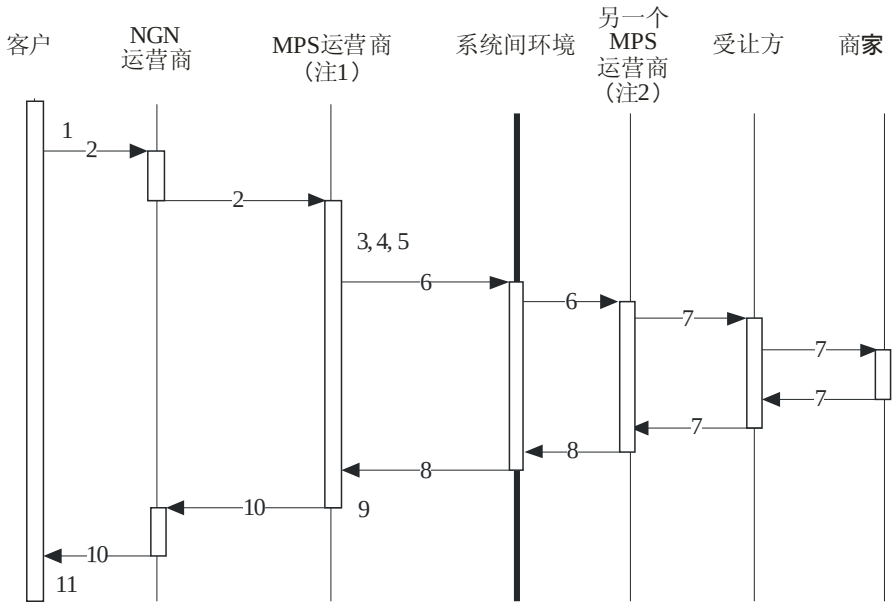
拒绝客户支付MPS运营商的货物和服务费用。

情形的初始数据

客户在MPS中注册，拥有得到连接的支付工具，并清楚进行支付交易所需的商家细节。

情形的基本步骤

1. 客户通过自己的移动电话发出请求，请求含有金融交易参数，包括（支付身份）和支付工具参数；
2. 通过运营商通信渠道传送请求；
3. MPS运营商接收请求；
4. 客户得到认证；
5. MPS运营商的身份通过支付身份得到明确；
6. 通过安全的系统间渠道将请求发至目的地（不同的MPS运营商）；
7. 利用客户支付工具细节进行所要求的金融交易；
8. 交易结果发至客户的归属MPS；
9. MPS向客户发出回复；
10. 通过运营商通信渠道传送回复；
11. 客户收到交易结果。



注 1 - 安全提供商、客户认证提供商、服务提供商
注 2 - 安全提供商、服务提供商

ITU-T Y.2741(10)_F09

图9 – 客户在另一个MPS中进行金融操作

情形的备选步骤

4. ***客户未得到认证。***

5. ***无法识别MPS。***

7. ***无法进行金融操作：***

a) 执行交易滚回；
b) 将操作性能结果能返回客户。

7 从代币支付系统的过渡

一些运营商已引入若干服务，方便人们在 NGN 运营商计费系统内（有时在计费系统之间）传送作为对货物和服务进行支付的货币和非货币代币。

虽然这些服务常常被介绍为有利于不成熟经济体（拥有大量不使用电子银行服务的人口）的发展，但从长远来讲，这些服务会干扰这些经济体的财政和货币系统。

发展中国家面临种类繁多的与现金犯罪有关的问题，在这些国家发展电子银行系统能够减少现金流通量，从而降低与现金有关的犯罪。

因此，提供代币支付服务的 NGN 运营商应制定路线图，将这些代币支付系统逐渐过渡发展为使用金融交易进行资产转让的系统。

附录I

在系统中登记支付工具

（本附录并非本建议书不可分割的部分。）

目的：为客户提供在MPS中使用其支付工具的可能性。

基本角色：总体目标和具体目标

客户：有机会通过支付工具充分利用MPS。

移动运营商：通过通信渠道传送信息。

MPS运营商：批准特定客户在MPS中使用特定支付应用。

客户认证提供商：认证客户及他/她的支付工具。

最大保证

客户拥有利用支付工具充分使用MPS的机会。

最小保证

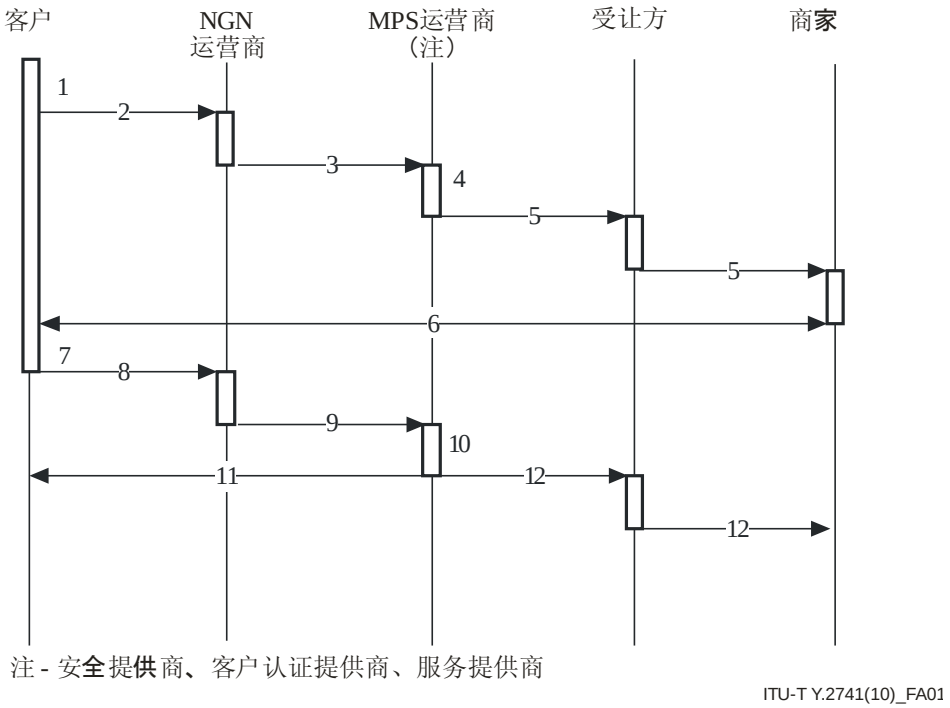
拒绝客户使用特定支付工具。

情形的初始数据

客户在MPS中登记，并拥有支付工具。

情形的基本步骤

1. 客户通过他/她的移动装置，将支付工具参数发至MPS运营商；
2. 通过NGN运营商渠道传送请求；
3. MPS运营商收到请求；
4. MPS运营商的IS生成随意数额；
5. MPS运营商向受让方系统发出在特定支付工具中预留这一数额的请求。受让方向支付工具发行方发出授权请求。客户须与发行方联系，以了解该数额，并确认他是支付工具的合法拥有人；
6. 支付工具发行方使用其标准认证手段对客户进行认证；
7. 认证之后，发行方将预留数额值通知客户；
8. 客户通过客户应用将数额值发至MPS运营商；
9. 通过NGN运营商渠道传送请求；
10. MPS运营商收到客户传来的预留数额值后，即将其与此前生成的数值进行比较；
11. 在两个数额值相符时，MPS运营商在安全存储装置上存储有关支付工具的信息，以备今后使用，同时将这一情况及操作结果通知客户；
12. 同时，将请求发至发行方（通过受让方），以取消支付工具中预留数额。



图I.1 – 在MPS中登记支付工具

情形的备选步骤

10. **此前预留的数额值与客户输入的值不符**

客户收到错误通知。如尝试失败次数超过三次，则MPS系统将移动装置的客户资料封存，并取消预留数额。

附录II

移动银行和移动商务系统的实施模式

（本附录不构成本建议书不可分割的部分。）

本附录以示例说明须遵守已实施安全等级的移动银行和移动商务系统的基本实施模式。

本附录使用了下列术语：

信息传送渠道：传送客户进行金融操作（转账）请求的手段，需远程接入支付工具。信息传送渠道示例包括短信、USSD请求、批通信（GPRS、EDGE、3G数据、HSDPA等）。

支付工具：一套进行现金和非现金汇款的法律措施，目的是进行支付。支付工具示例包括银行账户、运营商账户和银行卡。

可用操作：具有特定安全等级的系统的可用操作清单。

限制：使用系统的限制，在相互达成的合同中通过在法律上得到表明或保留的、已得到接受的风险模式加以规定。

预确定电话号码：客户通过服务提供商的专门表格在此前表明的电话号码。

临时电话：客户在进行支付时直接指明的电话号码。

预确定账户：客户通过服务提供商的专门表格在此前指明的账号。

临时账户：客户在进行支付时直接指明的账号。

预确定支付：按照此前提供参数进行的支付。付款接收方可从MPS服务提供商确定的名单中选出（如个人向企业实体支付已提供服务的费用）。

临时支付：客户为不包括在MPS服务提供商确定的清单中的服务进行的费用支付，前提是这种支付在技术上可行。前提条件：服务提供商须拥有与MPS进行互操作的渠道，或应由另一个MPS提供商提供服务，并在二者之间建立互操作。

自动支付：MPS服务提供商根据客户此前的同意启动的定期和自动支付。

带有确认的自动支付：MPS服务提供商按照客户的同意进行的定期和自动支付。

商家启动的支付：一种参数由商家确定和输入的支付。客户可以确认或拒绝处理这一主动提供的支付。

信息服务：MPS系统提供商提供的一系列信息服务，它与进行金融操作没有关系（如查看支付工具余额、提供参考信息）。

移动银行和移动商务系统的实施模式

以下探讨须符合得到实施的安全等级的移动银行和移动商务系统的可能模式。每一种实施模式都对支付工具、可用操作、限制和系统使用的应用提出了某些要求。

II.1 在不使用客户应用的前提下实施系统

它与 1 级和 2 级系统安全相对应（见[ITU-T Y.2740]）。

信息传送渠道：普通文字短信、USSD请求，

支付工具：通过在服务协议中预先确定的银行账户或运营商账户进行支付。

可用操作：仅向此前在合同中确定的接收方进行支付。在签订合同时应具体明确可能的操作清单：

- 支付预先确定的电话；
- 支付到预先确定的账户；
- 进行预先确定的支付；
- 进行自动支付；
- 进行带有确认的自动支付；
- 信息服务。

限制：最大支付额限制，可包括交易额限制、一天内的交易限制；对可用金融交易的限制，这意味着只能为此前同意的服务支付。

II.2 在使用客户应用的前提下实施系统

它与 3 级和 4 级系统安全相对应（见[ITU Y.2740]）。

信息传送渠道：短信、批通信（GPRS、EDGE、3G数据、HSDPA等）。信息传送渠道和正在传送的信息必须使用极强的加密方法进行加密。

支付工具：通过在服务协议中预先确定的银行或运营商账户支付；使用银行卡以及国际支付系统卡支付（支付包括经通信渠道的关键数据的传送）。

可用操作：可实现与系统的远程连接；为繁复多样的与系统连接的服务进行各种各样的支付；有可能大大增加MPS内实施的操作数量（引入新的支付和服务；连接新的商家）；服务提供商和客户之间可以灵活确定可用支付清单；不同MPS在提供服务时可实现互操作。可实施下列操作：

- 支付预先确定的电话；
- 支付到预先确定的账户；
- 进行预先确定的支付；
- 进行自动支付；
- 进行带有确认的自动支付；
- 信息服务；
- 支付临时电话号码；

- 支付到临时账户；
- 临时支付；
- 由商家启动的支付，

限制：系统参与方相互间的合同确定对支付的限制。

应用：使用应用是提供安全（信息加密）和方便系统使用必不可少的。

参考书目

[b-ITU-T Y.2001] ITU-T Y.2001建议书 (2004)，《下一代网络（NGN）概况》。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	终端和主观与客观评估方法
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网的协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2011年，日内瓦