国 际 电 信 联 盟

ITU-T Y.2740

(01/2011)

国际电信联盟
电信标准化部门

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

下一代网络中移动远程金融交易的安全要求

ITU-T Y.2740 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
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
未来的网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
运营商级开放环境	Y.2900–Y.2999

如果需要进一步了解细目，请查阅*ITU-T*建议书清单。

ITU-T Y.2740建议书

下一代网络中移动远程金融交易的安全要求

摘要

近年来，使用移动网络的、形式多样的远程支付网络已得到建立。虽然这些网络实施了不尽相同的方式，但往往缺乏安全性。与此同时，包括移动网络在内的通信网络在向下一代网络（NGN）过渡的过程中发生了极大变化。

ITU-T Y.2740建议书阐述了NGN环境中移动商务和移动银行系统安全的开发方式。本建议书根据四种具体的安全级别阐述了移动商务和移动银行系统的安全要求，概括了移动商务和移动银行系统可能遇到的风险，并规定了减弱风险的手段。

历史沿革

版本	建议书	批准日期	研究组
1.0	ITU-T Y.2740	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。

前言

国际电信联盟(ITU)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)是国际电信联盟的常设机构，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

本建议书为简要扼起见而使用的“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

ITU-T Y.2740建议书

下一代网络中移动远程金融交易的安全要求

1 范围

本建议书根据四种安全级别阐述了下一代网络（NGN）应用服务所支持的远程移动金融交易的相关安全风险、风险的缓解和应对措施。本建议书还规定了保护个体个人有关远程移动金融交易的数据隐私的最低要求。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，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。所有的建议书和其他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他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 X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*。

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*。

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[ITU-T Y.2741] Recommendation ITU-T Y.2741 (2011), *Architecture of secure mobile financial transactions in next generation networks*。

3 定义

3.1 国际电联其它建议书定义的术语

本建议书使用其它建议书定义的以下术语。

3.1.1 接入控制（access control）[ITU-T X.800]: 防止对资源的未经授权的使用，包括防止以未经授权方式使用资源。

3.1.2 应用（application）[ITU-T Y.2741]: 上载客户（用户）移动装置的特别移动银行或移动商务应用。

3.1.3 认证（authentication）[ITU-T X.800]: 见数据来源认证和对等实体认证。

注 – 在本建议书中，“认证”一词并非用于数据完整性，相反，会使用“数据完整性”一词。

3.1.4 可用性（availability）[ITU-T X.800]: 应经授权实体的要求可接入和可使用特性。

3.1.5 客户（client）[ITU-T Y.2741]: 就电信业务和移动商务系统使用签订合同的私人个人或公司实体。

3.1.6 保密性（confidentiality）[ITU-T X.800]: 不向未经授权的个人、实体或程序提供和披露信息的特性。

3.1.7 数据完整性（data integrity）[ITU-T X.800]: 数据不被以未经授权方式修改或毁坏的特性。

3.1.8 数据来源认证（data origin authentication）[ITU-T X.800]: 证实所收数据源为声称源。

3.1.9 移动支持系统（mobile payment system）[ITU-T Y.2741]: 移动银行和/或移动商务系统。

3.1.10 下一代网络**（next generation network (NGN)）**[b-ITU-T Y.2001]: 能够提供电信业务并能够使用多种宽带、QoS使能传输技术的分组网络，其中与业务相关的功能独立于底层的传输技术。它使用户不受干扰地接入网络和相关竞争的服务提供商，并选择其所需的业务。该网络支持有助于连惯无所不在地向用户提供业务的一般移动性。

3.1.11 隐私（privacy）[ITU-T X.800]: 个人控制或影响与其相关的何种信息可由谁收集和存储，以及向谁披露的权利。

注 – 由于该术语关系到个人权利，因此不可能十分确切，且除作为安全性要求外，应避免该术语的使用。

3.1.12 否认（repudiation）[ITU-T X.800]: 参与通信的一个实体否认已参加过全部或部分通信。

3.1.13 安全维（security dimension）[ITU-T X.805]: 旨在解决特定方面网络安全的一套安全措施。

3.1.14 安全层（security layer）[ITU-T X.805]: 分层的网络设备和设施群。

3.1.15 安全平面（security planes）[ITU-T X.805]: 由安全维保护的某一类型网络活动。

3.2 本建议书定义的术语

本建议书使用权下列术语：

3.2.1 安全级别（security level）：确定风险防护有效性的系统安全规范。

4 缩写词和首字母缩略语

本建议书使用下列编写词和首字母缩略语：

GSM 全球移动通信系统

MPS 移动支付系统

MSISDN 移动站国际 ISDN 号码

NGN 下一代网络

PA-DSS 支付应用数据安全标准

PCI DSS 支付卡行业数据安全标准

5 惯例

无。

6 下一代网络中移动银行和移动商务系统的安全考虑

下一代网络（NGN）中移动支付系统的安全将以MPS架构和“[ITU-T Y.2741]下一代网络的安全移动金融交易架构”规定的MPS参与方角色以及下述MPS参与方风险分析为基础。

6.1 移动远程金融交易的基本风险

本节未考虑参与方在落实MPS时遇到的新的、影响到全球和行业风险的因素，其中包括系统、战略、国家和主权、市场、利率、流动性、法律、名誉风险等。该节涉及在进行远程移动支付时可能直接产生的信息风险，因此需要确定安全问题以降低风险：

- 保密性损失风险意味着未经授权获取保密信息；
- 破坏数据完整性风险是在传送或处理数据时造成信息畸变；
- 电子文件造假风险（权威性风险）系指非授权参与方生成电子文件；
- 否认风险指拒绝承认编制了电子文件；
- 有意或因疏忽造成的信息损坏风险；
- 交易风险涉及因不良传输质量无法完成交易。

6.2 安全目标

为改善移动支付的安全性，并在最大程度上降低参与方的风险，有关解决方案必需确保实现以下目标：

- 减少交易时个人或财务信息被截获的可能性；
- 减少从数据库中检索个人或财务信息的可能性；
- 减少交易时替换或扭曲个人或财务信息的可能性；
- 通过实施独一无二的认证减少非授权人员和试图进行假冒的人员使用解决方案的可能性；
- 减少在解决方案中使用“盗窃”信息的可能性；
- 为使交易启动者或参与者在行动后无法否定行动提供条件；
- 确保所有运作参与者遵守合法权利，履行职责；
- 确保交易的完成。

6.3 安全级别的支持手段

本建议书以MPS参与方风险分析为基础，描述四种MPS安全级别。

系统安全级别由一套安全维实施措施所确定（见表1）。因此，第四级安全级别必须具有最强的安全维实施措施。尽管如此，安全维要求已统一到了所有安全级别中。

使用MPS的各方应了解系统安全级别和系统风险。

任何系统元件某些风险的可接受的安全级别是由承担此项风险的一方决定的。

各方还可通过包括限制个人交易频次或金额、向高忠诚度用户提供的服务可用性在内的操作措施进一步缓解使用MPS的风险。

通过使用NGN网络公众标识符（如GSM网的MSISDN）可在系统中确认客户。

6.3.1 各安全级别安全维的实施措施

系统安全已委托给每个系统参与者，由安全保证物理和管理设施在数据传送、处理和存储中加以实现。系统参与者须确保实施信息安全保证行业标准（如[b-PCI DSS]和[b-PA-DSS]等）。

以下列出了确定MPS安全级别的八个安全维[ITU-T X.805]。所有系统参与者必须根据数据交换中所涉及的信息实施安全维。

1) 接入控制：对各MPS部分的接入只能按照系统人员或最终用户接入级别加以提供。该要求对所有安全级别均有效。

2) 认证：参加各方所称身份的真实性必须得到保证。这是缓解否认编制风险的关键因素之一。由于存在多种组织和技术实施可能性，各安全级别确定起码的认证机制要求。

认证的三个因素包括：

- 客户使用别人无法了解的一些信息，如接入密码（你所知道的）；
- 客户拥有他人没有的东西并采取了某些与众不同的行动，如生成了一个电子签名或信息认证代码（你所拥有的）；
- 客户使用其生物数据（你所具备的）。

3) 不可否认性：为防止个人或实体否认已完成的某个行动（如发送、转发或接收信息）提供手段。为此，所有系统人员和最终用户的行动必须经过强制性注册。事件记录不得修改，必须包含所有用户的所有行动。遵守要求的方式是通过法律规定或相互合同预定和已接受的认证机制。该要求对所有安全级别有效。

4) 数据保密性：系统中使用的数据受到保护，免受非授权披露和篡改。保密性要求由系统数据重要性所确定。各安全级别规定一些确保保密性的手段并对系统数据重要性级别施加限制。

5) 通信安全：保证双向（去往和来自收信方）按顺序交付信息，包括完成交易（使用确保完成交易的协议），保护信息在通过通信信道传送时免遭非授权披露。该要求对所有安全级别有效。

6) 数据完整性：数据的正确性、准确性和完整性是通过防止非授权修改、删除、创建和复制以及指出这些非授权行动得到保证的。在满足一些条件时确保交易在应用层面顺理成章加以完成。各安全级别定义一定的完整性保证机制。完整性保证可通过数据保密性和接入控制实现。

7) 可用性：保证保护对MPS数据和服务授权接入。该要求对所有安全级别有效，服务提供商应尽力予以满足。

8) 隐私：确保数据交换和系统参与者所存储的信息的安全。解决方案必须使用系统得以运作所必须的最低数据量。系统参与者须缓解非授权数据捕获和传送。系统须保证符合金融行业标准。

应在所有安全级别同等落实的安全维包括：

– 接入控制；
– 不可否认性；
– 通信安全；
– 可用性。

以下安全维在不同安全级别中具有不同的实施方式：

– 认证；
– 数据保密性；
– 数据完整性；
– 隐私。

6.3.2 安全级别 1

MPS可依赖于NGN运营商提供的客户认证。

数据保密性和安全性是通过数据传送环境（通信安全）保证的，而数据存储和处理中的数据安全性和完整性是通过数据存储机制以及数据接入控制设施保证的。

所传送的信息中没有敏感数据并实施数据存储所需要的机制和系统接入控制设施使隐私得到保障。系统组件不得存在非授权数据捕获和传送的潜在可能性。

6.3.3 安全级别 2

使用系统服务的认证可通过仅使用一个认证因素加以实现，无需使用加密协议。

认证使用一次性密码。一次性密码是通过各种令牌方式生成的（单因数一次性密码装置、单因数加密装置等）。

数据保密性、完整性和隐私的保证与级别1类似。

6.3.4 安全级别 3

获得系统服务必须使用多因数客户认证。

系统须使用一个以上的认证因数对客户进行认证。

传送信息时，必须与数据传送协议同时使用更多的信息加密，确保数据的保密性、完整性和隐私，从而，保证互操作参与方传送的数据安全（包括数据完整性核实）。在数据存储和处理中，数据的保密性、完整性和隐私通过在按照优先和许可情况分配接入的同时，采用附加的加密和隐蔽手段加以实现。

为保证该级别的安全要求，系统须使用上载到客户移动装置中的特殊软件应用。这些应用须实施双因数认证，确保所传数据的加密和解密。

各项认证均须要求输入密码和其它激活数据，以便激活认证密钥，每次认证后未加密的认证密钥副本须清除（多因数软件加密令牌）。

所有MPS互操作参与方均须使用防止系统被入侵的安全设施。在级别3解决方案中，通过通信信道传送的数据安全须通过采用严格的加密手段予以保证。加密方法的强度取决于所使用的加密密钥。有效的密钥规模须符合起码的密钥规模选择建议书，以确保其相关强度。

6.3.5 安全级别 4

这是最高的系统安全级别。为满足这一级别的安全要求，系统须使用安装在客户移动装置中的硬件安全模块。该硬件模块须实施双因数认证，确保所传数据的加密和解密。每次认证均须要求输入密码或其它用来激活认证密钥的激活数据，未加密的认证密钥副本须在每次认证后清除（多因数硬件加密令牌）。信息加密既使用对称加密算法，也使用非对称加密算法。

其它安全维的实施须完全与级别3相符。

表1 - 不同安全级别的安全维实施的相互关联

<table>
<tr><th rowspan="2">安全维</th><th colspan="4">安全级别</th></tr>
<tr><th>级别1</th><th>级别2</th><th>级别3</th><th>级别4</th></tr>
<tr><td>接入控制</td><td colspan="4">反应自经授权的系统人员提供对各系统部分的接入。反应允许经授权的客户激活上载到移动终端的特殊应用</td></tr>
<tr><td>认证</td><td>系统中的认证是通过NGN数据传送环境保证的</td><td>系统服务的使用中采用单因数认证</td><td>系统服务的使用中采用多因数认证</td><td>本人订购服务，其中使用必须识别的个人数据。使用系统服务时，采用多因数认证。必须使用硬件加密模块。</td></tr>
<tr><td>不可否认性</td><td colspan="4">交易启动方或参与方不能否定其所完成的行动，这一点通过法律规定的明确及暗含的法律合同或合约手段预定或可接受的认证机制加以保证。所有系统人员和最终用户的行动均须记录。事件日志不得修改并保存所有用户的所有行动。</td></tr>
<tr><td>数据保密性</td><td colspan="2" rowspan="2">传送数据过程中，数据保密性是通过数据传送环境（通行安全）保证的，而存储和处理数据时，其保密性是通过数据存储机制与系统接入控制实现的。</td><td rowspan="3">在数据传送过程中，数据保密性是通过与数据传送协议共同使用的额外信息加密实现的，从而确保互操作参与方所传数据的安全（包括数据完整性核实）。在数据存储和处理中，数据的保密性、完整性和隐私是通过按照特权和许可情况分配接入的同时采用更多加密机制实现的。</td><td rowspan="3">实施级别3要求必须在用户侧使用硬件加密和数据安全设施（硬件加密模块）。</td></tr>
<tr><td>数据完整性</td></tr>
<tr><td>隐私</td><td colspan="2">不在传送的信息中放入敏感数据以及实施规定的数据存储机制和系统接入控制设施可保证隐私。
系统组件不得存在非授权数据捕获和传送的潜在可能性。</td></tr>
<tr><td>通信安全</td><td colspan="4">向收件方传送信息是通过在通信信道上传送时防止非授权披露实现的。这是由NGN提供方保证的。</td></tr>
<tr><td>可用性</td><td colspan="4">可用性确保不对授权的系统数据和服务接入予以拒绝。可用性是通过NGN提供商以及MPS服务提供商保证的。</td></tr>
</table>

参考资料

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

[b-PA-DSS] Payment Card Industry (PCI), *Payment Application Data Security Standard. Requirements and Security Assessment Procedures*, Version 2.0, October 2010.

[b-PCI DSS] Payment Card Industry (PCI), *Data Security Standard. Requirements and Security Assessment Procedures*, Version 2.0, October 2010.

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