国 际 电 信 联 盟

ITU-T X.1127

(09/2017)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务(1) – 移动安全

手机防盗措施的功能安全性要求和架构

ITU-T X.1127 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务(1)	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	**X.1120–X.1139**
网页安全	X.1140–X.1149
安全协议(1)	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统 (ITS) 安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1127 建议书

手机防盗措施的功能安全性要求和架构

摘要

ITU-T X.1127建议书以全球移动通信系统协会（GSMA）描述的一般要求为基础，主要讨论智能手机防盗机制功能安全性要求和功能架构。

智能手机迅速普及，并几乎成为人们生活中不可或缺的一部分。然而，很多智能手机使用者都有手机被盗的经历。在手机丢失或被盗的情况下，应当启用手机防盗措施（即死亡开关），以便能够：

– 远程删除智能手机上授权用户的数据；

– 使未授权用户无法对智能手机进行操作；

– 如果在技术上可行，防止出现未经授权用户的许可对手机进行再激活的行为；并且

– 如果授权用户对智能手机进行了恢复，应当允许该用户对手机进行操作，并在可行的范围内对智能手机上的用户数据进行存储。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1127	2017-09-06	17	11.1002/1000/13259

关键词

防盗措施、手机、安全性要求

* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，其次建议书的识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

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）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，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。

世界电信标准化大会（WTSA），每四年举行一次，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第一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）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“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和适应性等），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”等其它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

国际电联提醒注意：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它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，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，这可能并非最新消息，因此特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 X.1127 建议书

手机防盗措施的功能安全性要求和架构

1 范围

该建议书强调了智能手机防盗措施（例如死亡开关）的功能安全性要求和架构，这使用户能够远程删除其个人数据或将被盗的或丢失的智能设备进行禁用。

根据预测，本建议书中提及的功能安全性要求和功能架构适用于智能手机，针对智能手机用户、智能手机制造商以及移动服务运营商的需求提供防盗措施。

本建议书集中强调功能性要求、功能架构和防盗机制。该建议书使用了一个参考模型（包括设备所有者、授权服务器、备份服务器以及丢失或被盗的设备）。附录III中描述了防盗方面面临的具体威胁。本建议书没有对全球移动通信系统协会（GSMA）规定的智能手机防盗特点的一般要求进行修改[b-GSMA]。

2 参考文件

参考文献下列ITU-T建议书和其他参考文献的条款，通过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都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ITU-T X.1254] ITU-T X.1254 (2012)建议书，实体认证保证框架。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 数据的清理（data sanitization）[b-NIST SP 800-88]：数据的清理指通过采取普通和特殊方式，使媒体上书写的数据无法恢复。

3.1.2 实体认证保证（entity authentication assurance）（EAA）[ITU-TX.1254]：在证实实体符合其身份和对它的期望的认证过程中达到的信任度。（本定义是基于[b-ITU-T X.1252]中对‘认证保证’的定义）

注 – 信任是以实体和所称身份之间的绑定达到的信任度为依据的。

3.1.3 身份（identity）[b-ITU-T X.1250]：以一个或多个信息元素表示一实体，使实体足以在语境内得到区分。在IdM中，术语身份被理解为语境下的身份（属性子集）即，属性的多样性受限于实体存在和互动的边界条件（语境）框架。

注 – 各实体通过一个综合身份表示，它包括所有描述这类实体（属性）的可能信息元素。然而，这种综合身份是一个理论问题，不包括任何描述和实用情况，因为可能的属性数量是无限的。

3.1.4 死亡开关（kill switch）[b-GSMA]：“死亡开关”指一种用于对移动设备的关键功能进行禁用的方式。

注 – 死亡开关实质上是移动设备装置中的一种功能，因此，如果其接收到一些格式的信息，移动设备便会按照要求停止运行，且仅能在设备所有者对设备再次激活进行授权的情况下设备才能得以激活或再次使用。

3.1.5 移动电话（mobile phone）[b-ITU-T X-Sup.19]：用于通过无线电跨越大的地理区域接入公共移动网络来发起电话呼叫和传递文本信息、同时允许用户处于移动状态的电子设备。

3.1.6 智能电话（smartphone）[b-ITU-T X-Sup.19]：拥有强大计算能力、异质连接性和为第三方应用程序提供平台的先进操作系统的移动电话。

3.1.7 威胁（threat0）[b-ISO/IEC 27000]：可能对系统或机构造成伤害的有害事件的潜在起因。

3.1.8 隧道（tunnel）[b-ISO/IEC 27033-1]：隧道是建立在现有网络基础设施之上的连接网络设备的数据通道。

注 – 可以使用技术（例如协议封装、标签交换或虚拟电路）来建立隧道。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 硬件装置（device hardware）：组成一个正常运行的移动设备所需的物理部件包括：屏幕、按键、印刷电路板、码片、SIM卡、可移动存储等。

3.2.2 软件装置（device software）：“软件装置”指装置和SIM卡上的所有软件程序，包括应用程序、操作系统、引导加载器、引导ROM和固件等。

3.2.3 设备用户（device user）：移动设备的授权用户。

3.2.4 安全隧道（secure tunneling）：“安全隧道”指一项协议，该协议允许将数据或信息从一个网络选址安全地传送至另一个网络选址。

注 – 安全隧道通常支持实体认证、信息完整性和信息保密性。

4 缩写词和首字母缩略语

本建议书使用了下述缩写词和首字母缩略语：

ATM 自动柜员机

CRL 证书撤销列表

DER 唯一编码规则

DDoS 分布式拒绝服务

DM 设备管理

EAA 实体认证保证

GPS 全球定位系统

GSMA 全球移动通信系统协会

HTTP 超文本传输协议

LoA 保证水平

MAC 消息认证码

OCSP 在线证书状态协议

OMA 开放移动联盟

OTP 一次性密码

PII 个人验证信息

PKI 公钥基础设施

SIM 用户身份模块

SMS-SC 短消息服务 – 服务中心

SSL 安全套接层

TCP 传输控制协议

TFA 三因子认证

TLS 安全传输层协议

U 普遍

UICC 通用集成电路卡

USSD 非结构化补充数据业务

2FA 双重认证

5 惯例

本建议书适用于以下描述方式表达的规定：

a) “Shall”表示要求；

b) “Should”表示建议；

c) “May”表示允许；

d) “Can”表示可能性和能力。

6 防盗措施概述

6.1 防盗措施

智能手机迅速普及，并几乎成为人们生活中不可或缺的一部分。然而，很多智能手机使用者都有手机被盗的经历。在手机丢失或被盗的情况下，应当启用手机防盗措施（即死亡开关），以便能够：

– 在智能手机丢失或被盗的情况下，对智能手机上用户的个人数据进行远程删除；

– 使未授权用户无法对智能手机进行操作；

– 将用户的个人数据储存至备份服务器，如有必要，移动服务运营商或设备制造商会对其进行操作；

– 防止出现未经授权用户的许可对手机进行再激活的行为；并且

– 如果授权用户对智能手机进行了恢复，应当允许该用户对手机进行操作，并在可行的范围内对智能手机上的用户数据进行存储。

装在移动设备中的防盗软件，可以对被盗的或丢失的手机实行禁用。

当设备所有者发现移动设备已经丢失或被盗时，可通过以下两种方法对移动设备实施禁用：

1) 设备所有者可以联系其移动服务运营商，移动服务运营商可以对设备进行禁用；并且

2) 设备所有者可以使用一个应用程序或另一台移动设备，或使用一个禁用工具来对丢失的/被盗的移动设备进行禁用。

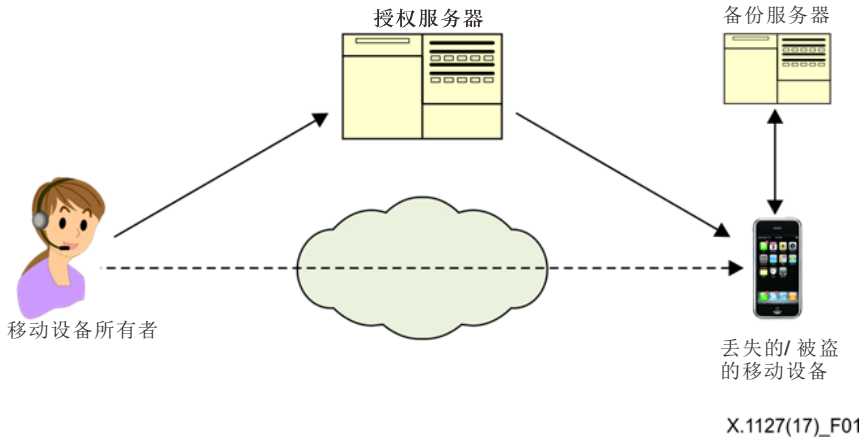


图1 – 防盗措施参考模型

图1描述了移动设备防盗措施参考模型。授权服务器支持对被盗的或丢失的移动设备实施禁用功能，该种操作由移动服务运营商或设备制造商来进行。授权服务器向被盗/丢失的移动设备发送禁用指令。备份服务器根据设备所有者的请求对移动设备个人数据进行储存。

应当使用安全隧道（例如安全套接层（SSL））对丢失的/被盗的移动设备和授权服务器之间的通讯进行保护。此外，应当使用安全隧道（例如SSL）对丢失的/被盗的移动设备和备份服务器之间的通讯进行保护。

本建议书以[ITU-T X.1254]中描述的用于管理EAA的实体认证保证（EAA）框架为基础。该EAA框架对实体认证保证水平（LoA）的四个等级进行了定义。每个LoA描述了对直至和包括认证程序本身的程序的置信度，从而保证使用一具体身份的实体实际是被赋予该身份的实体。

一些管辖区域可能要求防盗软件可供安装或下载。例如，在美国，加利福尼亚州强制要求在新手机上安装防盗软件，即使该软件会在默认的情况下启动，但用户有权利禁用该项功能。让防盗功能具备选择性退出而不是选择性接受的特征，更多的客户会采取防盗措施，因此，移动设备会得到更好的保护。

6.2 对防盗措施的高水平要求

从授权服务器向移动设备传递防盗信息时，防盗措施的高水平要求如下：

– 实体认证；

– 信息完整性；

– 重放检测和序列完整性；

– 收据证明与执行证明；
– 信息保密性；以及
– 对使用过的安全机制进行指示。

7 手机防盗措施功能架构

7.1 手机防盗措施面临的威胁

本节描述一组按照本建议书提出的某些要求或机制识别出的安全威胁。已按照下述ITU-T建议书提出了安全威胁模型和其他基本资料：

– [b-ITU-T X.800]规定与安全有关的总体架构组成要素，可酌情用于开放系统之间的通信需要保护的情况。
– [b-ITU-T X.805]规定用于提供端对端网络安全的网络安全架构。

[b-ITU-T X.800]和[b-ITU-T X.805]指出，网络面临着以下安全威胁：

– 信息和/或其他资源毁坏；
– 信息腐坏或修改；
– 信息和/或其他资源被盗取、移除或丢失；
– 信息泄露；
– 服务中断。

本建议书指出，移动电话防盗措施面临的具体威胁如下：

– 在请求未授权的情况下删除一个禁用手机上的数据；
– 在请求未授权的情况下对手机实行禁用；
– 在未经授权的情况下对手机上的敏感数据进行公开；
– 手机上的用户数据丢失；
– 在未经授权的情况下访问和/或修改禁用手机的功能或数据；
– 在未经授权的情况下对用于防盗措施的设备和网络运营商和/或禁用工具之间交换的用户数据和软件进行公开；

风险如下：

– 黑客可以找到一种方式劫持禁用指令并关闭移动设备；
– 储存在备用服务器中的个人数据或在移动设备和备用服务器之间传输的个人数据可能被泄露；

7.2 手机防盗措施的关键安全功能

对移动设备进行禁用的功能只能通过一个授权服务器或一个支持禁用功能的禁用工具来实行。为达成该项要求，措施需要具备以下五项功能：

1) 设备和服务器之间的安全通讯连接；
2) 设备服务器进行的实体认证；
3) 由服务器设备和经授权执行该项功能的服务器进行的实体认证；
4) 被盗移动设备的位置追踪；以及
5) 对禁用手机上的数据进行安全备份/删除。

应当通过个人网站提供一项机制允许设备所有者对要由设备所有者储存的个人验证信息（PII）进行管理。设备所有者可能会得到移动设备中安装的应用程序。防盗应用程序可能允许设备所有者选择用于防盗的数据（包括PII），并涉及对基于云的存储解决方案中的数据（包括PII）进行自动备份。该项管理流程由以下三步组成：

1) 在移动设备上安装应用程序；

2) 由移动服务提供商或设备制造商在网站上进行注册；

3) 通过个人网站对存储在备份服务器中的PII进行管理（即删除、下载、上传）。

7.3 移动设备防盗措施的功能架构

移动设备防盗措施的功能架构是以[b-3GPP TS 33.102]中描述的安全架构为基础。图2描述的安全架构包括以下五个安全组：

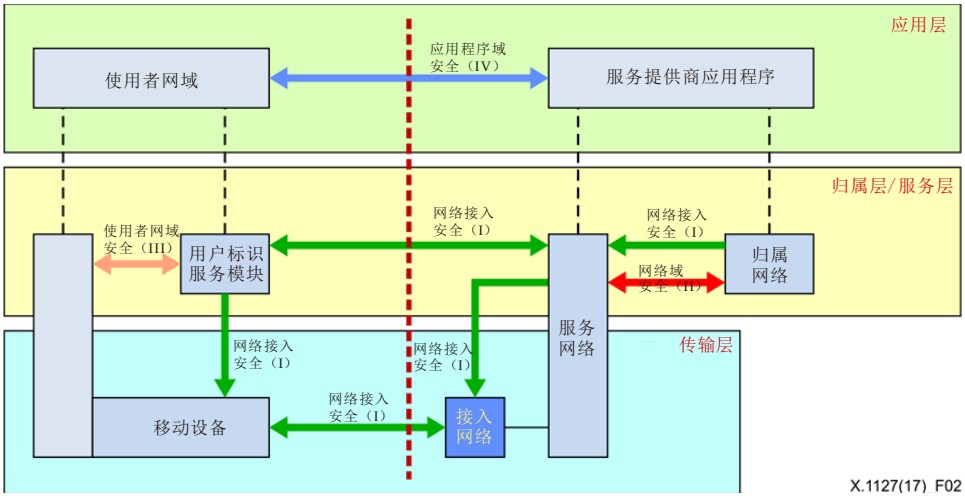
1) 网络接入安全（I）：“网络接入安全”指一套安全机制，使用户能够安全访问3G服务，特别是防止（无线电广播台）访问链接侵害；

2) 网络域安全（II）：“网络域安全”指一套安全机制，使域名提供商中的节点能够安全交换信令数据，并防止有线网络上的侵害；

3) 使用者网域安全（III）：“使用者网域安全”指一套安全机制，确保安全访问移动基站；

4) 应用程序域安全（IV）：“应用程序域安全”指一套安全机制，使用户域和提供商域内的应用程序能够安全地交换信息；

5) 安全特征可见性及可配置能力（V）：“安全特征可见性及可配置能力”指一套安全机制，使用户能够得知安全机制是否在运行以及服务的使用和提供是否应取决于安全机制。



注 – 图2选自[b-3GPP TS 33.102]

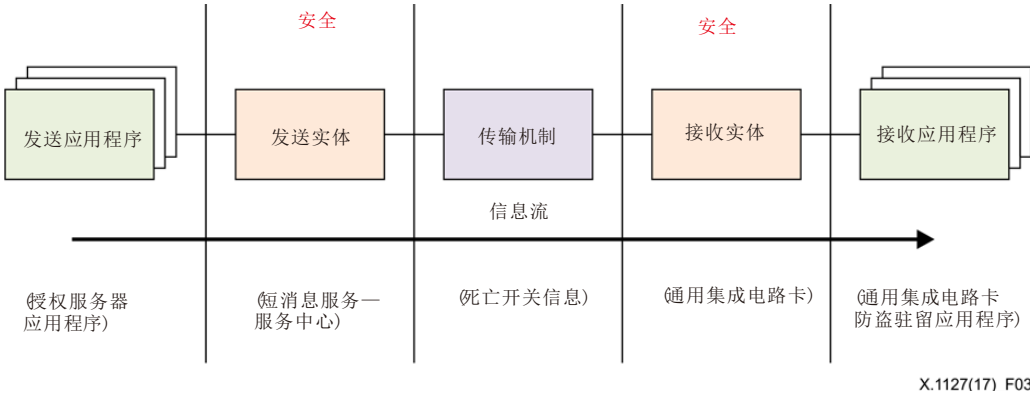
图2 – 安全架构

移动设备中的防盗措施应用程序是位于使用者网域中的一套应用程序的一部分，而服务提供商中的防盗功能是位于服务提供商应用程序中的一套应用程序的一部分。

用于防盗措施的安全参考模型是以[b-3GPP TS 22.048]中描述的一个模型为基础。发送应用程序是一个实体，该实体产生被发送的信息，而发送实体产生安全包（例如短消息服务—服务中心（SMS-SC）、通用集成电路卡（UICC）、非结构化补充数据业务（USSD）入口点、或专用通用（U）客户识别模块（SIM）工具包服务器），且我们可以从发送实体调

用安全机制。发送实体产生将被发送的安全包。我们通过传输层安全隧道或应用层安全隧道传递安

接收应用程序是一个实体，应用程序信息会用到该实体，而接收实体会接收安全包（例如SMS-SC、UICC、USSD入口点、或专用（U）SIM工具包）。



注 – 图3选自[b-3GPP TS 22.048]

图3 – 安全参考模型

在本建议书中，安全架构是以图1中的参考模型、图2中的安全架构和图3中的安全参考模型为基础。

7.4 手机防盗措施机制

7.4.1 安全通信机制

丢失的或被盗的移动设备应当作为一个验证服务器以及安全隧道的一个客户端。

客户端与服务器之间的通信信道应当满足以下六项安全方面的要求：

1) 保密性：安全隧道应确保数据不能被未授权的实体读取。这是通过加密数据（加密数据使用一个加密算法和一个秘密密钥） – 一个仅有交换数据的两个实体之间才知道的值来完成的。只有具备秘密密钥的实体才能对数据进行解密。

2) 完整性：安全隧道应确认数据是否在传输过程中被（有意或无意地）改变。应当通过产生一个消息认证码（MAC）（数据的键入密码校验和）来确保数据完整性。如果数据被修改且MAC被重新计算，新的MAC和旧的MAC就会有不同。

3) 对等认证：每个端点应当确认它要与之通信的另一个端点的身份，确保网络信息流通量以及数据是由预计的主机发送出来。安全隧道认证通常是单程运行，向客户端证实服务器；然而，一个安全隧道要求对两个端点都进行认证。

4) 重发保护：我们不应将同样的数据传递多次，且不应当以乱序的方式传递数据。可以在信息源使用一个序列号或计数器。信息源或信息会对其信息包添加一个序列号，序列号从0开始，且每次再发送另一条信息的时候，序列号会增加。

5) 网站流量分析保护：监控网络信息流通量的人不应决定网络信息流通量的内容或信息交换量的多少。安全隧道还可以隐藏几方的通讯，而SSL会使该种信息处于暴露状态。取决于安装启用的情况，通信频率可能得到保护。不过，可以数出正在交换的信息包的数目。

6) 访问控制：安全隧道的端点应当发挥过滤的作用，以确保只有经授权的用户才能访问特殊的网络资源。安全隧道的端点还可以允许或阻止一定类型的网络信息流通量，例如允许网络服务器访问文件，但抵制文件共享。

若要达到上述要求，我们推荐使用安全传输层协议（TLS）来确保移动设备和经授权的服务器之间的通信安全。TLS是一项协议，该协议在网络之间提供安全通信隧道。TLS允许客户端/服务器应用程序来阻止窃听、篡改或伪造信息的现象。TLS位于可靠传输协议（例如传输控制协议（TCP））的顶端，用于封装不同的更高级别的协议（例如超文本传输协议（HTTP））。

TLS包含三个基本阶段：

1) 对等协商支援的密钥算法；
2) 密钥交换与认证；
3) 对称密码加密与消息认证。

附录V中有关于TLS的详细介绍。

此外，本建议书推荐使用开放移动联盟（OMA）协议基础上的安全通信信道。

7.4.2 双向认证机制

认证用于证实通讯实体的身份。认证因素分为三类：

1) 知识因素：（“某一个使用者知道的东西”），例如密码；
2) 持有因素（“某一个使用者持有的东西”），例如自动柜员机（ATM）卡；以及
3) 与生拥有因素（“某一个使用者本身就是某种因素”），例如生物识别。

[b-ITU-T X.1158]介绍了三种识别方法：

1) 单因素认证（SFA）是传统的认证方法，在向用户授予访问权之前仅要求用户名和密码；
2) 双因素认证（2FA）是以将两种不同认证因素结合使用为基础。这些因素可能是一个用户知道的、持有的东西，或用户本身就是某种因素。日常生活中的一个典例就是，如果一位用户想从自动提款机取钱，他（她）只需要正确地提供银行卡（某一个使用者持有的东西）和PIN（个人识别号码，即某一个使用者知道的东西），交易即可完成。
3) 三因素认证（TFA）是基于将三种不同的独立的因素进行组合使用：某一个使用者知道的东西（密码）、某一个使用者持有的东西（安全令牌）以及某一个使用者本身就是的某种因素（生物识别）。

多因素认证是基于将两种或多种不同的独立的因素进行组合使用。双因素认证和三因素认证是多因素认证的一部分。

7.4.3 数据安全删除机制

“清除”指一种进程，该进程为访问媒体上的目标数据（该等目标数据在一定程度上不可用）提供通路[b-NIST SP 800-88]。[b-NIST SP 800-88]提供了以下三种清除方法：

1) 清除操作：“清除操作”使用逻辑技术清除所有的用户可寻址存储位置中的数据，以便防止简易无创数据恢复技术；该操作通常是通过向存储设备发送标准读写命令（例如通过用新值或菜单选项改写来将设备重置到出厂默认状态（当不支持改写时））来得以应用；

2) 清理操作：使用物理或逻辑技术，提供目标数据恢复（当使用最先进的实验室技术不可行时）；

3) 破坏操作：提供目标数据恢复（当使用最先进的实验室技术不可行时），随后导致无法使用媒体存储数据。

清除操作通过组织批准的软件覆盖媒体，并对被覆盖的数据进行验证。清除模式应至少为一个带有固定数据值（例如全部零点）的单写入通道。可以选择性地使用多个写入通道或更复杂的值。

8 功能安全性要求

8.1 概述

– 需要在[ITU-T X.1254]中描述的EAA（实体认证保证）框架上建立功能架构；

– 功能架构必须提供一个安全通道（例如，[b-IETF RFC 6460]中描述的TLS（安全传输层协议）或以用于组件之间通信的OMA（开放移动联盟）协议为基础建立的安全通信信道；

– 功能架构必须提供一个安全的密钥管理（例如，以[b-ITU-T X.509]中描述的公共密钥基础设施（PKI）为基础），用于支持安全隧道；

– 功能架构至少需要支持[ITU-T X.1254]中描述的LoA（保证水平）2实体认证机制；

– 功能架构至少需要支持[ITU-T X.1254]中描述的LoA（保证水平）2实体登记；

– 功能架构至少需要支持[ITU-T X.1254]中描述的LoA（保证水平）2实体证书管理；

– 功能架构需要支持用于消息传递的消息认证；

– 功能架构需要支持用于已传递的消息的抗重放攻击；

– 功能架构需要支持将设备数据备份至安全网络服务器的能力；

– 功能架构需要提供强大的授权（访问控制）；

– 功能架构需要支持[b-3GPP TS 22.048]中描述的安全机制]；

– 功能架构需要为移动设备所有者、授权服务器和被盗的移动设备提供身份管理。

8.2 移动设备所有者功能安全性要求

– 移动设备所有者需要经认证来访问授权服务器，该等授权服务器至少基于二因素认证（例如，[ITU-T X.1254]中描述的ID /密码和一次性密码（OTP））；

– 必须至少使用[ITU-T X.1254]中描述的LoA（保证水平）2实体登记程序对移动设备所有者进行认证；
– 设备所有者的功能架构至少需要使用[ITU-T X.1254]中描述的LoA（保证水平）2认证机制对授权服务器进行认证；
– 设备所有者的功能架构需要支持安全隧道（例如，[b-IETF RFC 6460]中描述的TLS（安全传输层协议）或基于OMA（开放移动联盟）协议的安全通信信道），以便传送的信息与授权服务器之间的通信。

8.3 授权服务器功能安全性要求

– 授权服务器的功能架构需要至少使用双因素认证机制（例如，[ITU-T X.1254]中描述的LoA（保证水平）3认证）对设备所有者进行验证；
– 授权服务器的功能架构需要经被盗的移动设备认证，至少需要使用双因素认证机制（例如，[ITU-T X.1254]中描述的LoA（保证水平）3认证）；
– 授权服务器的功能架构需要支持安全隧道（例如，[b-IETF RFC 6460]中描述的TLS（安全传输层协议）或基于OMA（开放移动联盟）协议的安全通信信道），以便信息与移动设备所有者之间的通信。
– 授权服务器的功能架构需要支持安全隧道，以便传输的消息与被盗的移动设备之间的通信。

8.4 被盗移动设备功能安全性要求

– 被盗的移动设备的功能架构需要支持安全隧道（例如，[b-IETF RFC 6460]中描述的TLS（安全传输层协议）或基于OMA（开放移动联盟）协议的安全通信信道），以便传送的信息与授权服务器之间的通信；
– 被盗的移动设备的功能架构需要经认证来访问授权服务器，至少使用双因素认证机制（例如，[ITU-T X.1254]中描述的LoA（保证水平）3认证）；
– 被盗的移动设备的功能架构需要认证授权服务器，至少使用双因素认证机制（例如，[ITU-T X.1254]中描述的LoA（保证水平）3认证）；
– 被盗移动设备的功能架构需要借助一个功能，将属于所有者的所有设备数据备份至一个安全的网络服务器；
– 被盗移动设备的功能架构需要执行访问控制机制，以便发送从授权服务器接收的指令；
– 被盗移动设备的功能架构需要保护数据或功能，防止未经授权的实体对数据或功能进行访问和使用；
– 一旦从授权服务器接收到将移动设备中的数据删除的指令，被盗移动设备的功能架构需要支持清除操作（用于第7.4.3节的安全数据删除）。

8.5 备份服务器功能安全性要求

– 备份服务器的功能架构需要支持一个安全隧道，以便使用移动设备传输消息；
– 备份服务器的功能架构需要使用一个健全的身份验证机制来验证移动设备，目的是备份设备数据（如有必要）；
– 移动设备需要使用一个健全的身份验证机制对备份服务器的功能架构进行验证；

– 备份服务器的功能架构需要支持从移动设备进行适当的设备数据备份的能力；
– 备份服务器的功能架构需要为移动设备提供足够的资源（即存储）。

附录 I

防盗措施的一般要求

（本附录不构成本建议书的一部分）

[b-GSMA]提供防盗措施信息的一般要求。本附录描述了这些要求。

I.1 设备所有者

– 为确认已永久丢失或被盗（例如，全球定位系统（GPS）坐标显示设备在所有者不知道的地点），所有者需要启动程序来禁用服务，步骤如下：
  - 向该设备发送信号，使设备长时间（30秒至3分钟）发出大的声响，让所有者确认设备的位置，假设它是在附近，
  - 在设备锁/主屏幕上显示设备返回的消息，
  - 使用GPS（或任何其他定位技术（如果设备支持该项功能））找到设备的位置，并在地图上显示位置；
– 所有者必须明确地‘选择退出’的设备禁用功能，但需要将‘选择加入’作为默认；
– 关于移动设备的初始启动和设置，我们为所有者推荐一个简短的教程，以帮助所有者安全地使用和存储新设备。在激活服务之前务必完成教程；
– 我们推荐所有者通过使用自助服务功能访问和调用设备禁用功能，而无须涉及网络运营商；
– 如果设备被运营商禁用，则设备所有者无法重新启用设备；
– 所有者可以调用一个功能，将属于所有者（个人数据）的所有设备数据备份到安全的网络服务器；
– 所有者必须具有远程呈现所有设备数据不可访问的能力；
– 所有者要具备远程删除设备上的用户数据（例如图片、视频、电话簿、电子邮件）的能力。如果用户数据被强加密，那么从设备中清除加密密钥就可以；
– 对于丢失或被盗设备（该等设备在已访问网络（漫游）上注册），在试图调用备份数据、禁用设备或恢复设备的功能时，可以通知所有者缴纳任何额外费用；
– 未授权的用户无法启用禁用设备的功能，也无法访问禁用设备的数据；
– 所有者应当能够启用一项功能，即当该设备不属于所有者时，在设备的主/锁屏幕上显示一个自定义的信息。

I.2 服务器

– 网络运营商需要对设备所有者的关于禁用设备的请求进行验证；
– 有关所有者禁用设备的要求需要经过验证，并且仅需对由该所有者注册的设备进行控制；
– 需要确保用户能够安全地定位和访问支持禁用功能的服务器；

– 仅允许经过充分培训的授权人员访问和调用禁用功能；
– 服务器需要生成和保留所有禁用请求的日志；
– 当恢复对先前禁用的重新启用的设备的服务时，需要将所有者的备份数据和应用程序恢复到设备上；
– 必须对已备份的所有者数据进行安全存储，并保证数据的保密性和完整性；
– 一旦业主要求对他们的设备进行禁用，如果设备可以成功通过认证，禁用功能可在15分钟内得以启动；
– 恢复出厂设置不能作为绕过防盗措施的手段。

I.3 移动设备

– 在要禁用设备之前，需证明禁用设备的请求属实；
– 必须由支持禁用功能的授权服务器执行禁用移动设备的机制。为满足这一要求，要做到以下几点：
  • 设备与服务器之间的安全连接；
  • 由设备的服务器进行身份验证；
  • 由服务器的设备和被授权执行该功能的服务器进行身份验证；
– 对于移动设备的初始启动和安装，我们需要通过设置防盗功能和任何其他相关的安全功能（例如设备访问控制机制）对所有者进行详细指导；
– 该设备应当具备一项功能，即被禁用后，允许合法所有者对其服务进行重新启动。且任何人如果不是合法所有者，均无法对服务进行重新启动；
– 当设备没有连接到公共陆地移动网络但连接到互联网时，应当允许使用设备禁用功能；
– 对于丢失或被盗设备（该等设备在已访问网络（漫游）上注册），我们要求所有功能（备份数据、禁用设备和恢复设备）成功发挥作用。

I.4 设备制造

– 我们建议，设备制造商继续实施和发展措施，以防止对丢失或被盗设备进行未经授权的重新初始化，使得除了所有者以外的人无法使用设备。

附录 II

防盗措施的附加安全性要求

（本附录不构成本建议书的一部分）

II.1 备份服务器要求

– 该机制需要由支持存储被盗/丢失的移动设备的PII的备份服务器来执行。为满足这一要求，需要做到以下几点：

- 设备与备份服务器之间的安全连接；
- 由移动设备的备份服务器进行的身份验证；
- 由备份服务器的设备进行的身份验证。

附录 III

防盗具体威胁

（本附录不构成本建议书的一部分）

III.1 移动设备所有者与授权服务器之间的威胁

– 设备所有者的身份模拟，即攻击者扮演设备所有者把不当的禁用指令传递给授权服务器。利用这种威胁的攻击，可能会导致无辜的移动设备被禁用；

– 篡改/窃听/重放信息，即一个不正确的禁用指令被传递至授权服务器；指令消息的内容被透露给攻击者（该攻击者能够在通信中窃听）；或巨大的流量发送导致授权服务器受到分布式拒绝服务（DDoS）攻击；

– 授权服务器身份模拟，即把合法的设备所有者的认证凭证进行暴露或把合法设备所有者的禁用指令传递给假冒授权服务器。利用这种威胁的攻击，可能会导致无辜的移动设备被禁用。

III.2 授权服务器与防盗禁用代理之间的威胁

– 认证服务器的身份模拟，即把不正确的禁用指令发送到被盗的移动设备；

– 篡改/窃听/重放信息，即把一个不正确的禁用指令发送到防盗禁用代理；把指令消息的内容暴露给攻击者（该攻击者能够在通信中窃听）；或巨大的流量发送导致禁用代理受到DDoS攻击；

– 禁用代理的身份模拟，即把合法的设备所有者的认证凭证进行暴露或把合法设备所有者的禁用指令传递给假冒禁用代理服务器。

III.3 防盗禁用代理与备份服务器之间的威胁

– 防盗禁用代理服务器身份模拟，即把存储在备份服务器中的备份信息透露给假冒禁用代理；

– 篡改/窃听/重放信息，即篡改备份信息并把备份信息透露给攻击者（该攻击者能够在通信中窃听）；

– 备份服务器身份模拟，即把备份信息透露给假冒备份服务器。

附录 IV

防盗措施方案

（本附录不构成本建议书的一部分）

IV.1 移动设备禁用功能类型

禁用功能分为两类：

1) “硬”禁用功能，该功能使被盗移动设备永远无法使用；

2) “软”禁用功能，该功能只会使“未经授权的用户”无法使用移动设备。

IV.2 启用被盗/丢失移动设备

防盗功能需要移动设备所有者的积极参与。当一个设备所有者购买新的移动设备和从蜂窝提供商订货时，他们应设置启用移动设备的防盗功能。

IV.3 被盗/丢失移动设备的禁用方案

如果手机被盗或丢失，设备所有者联系他们的蜂窝服务提供商，或使用一个由移动运营商运行的网站（称为授权服务器）向移动设备发送一个“设备禁用“指令。该指令会锁定移动设备，并且如果设备所有者进行了选择，也可以从移动设备删除一些个人数据或允许备份服务器存储一些个人资料。

即使设备已关闭或已将数据存储介质删除，该设备禁用指令会使该设备在全球任何商业移动服务供应商的网络或商业移动数据服务中均无法使用。

恢复锁定设备的唯一方法是使用手机所有者提供的密码。

附录 V

防盗措施安全传输层协议（TLS）协议

（本附录不构成本建议书的一部分）

本附录提供了一个用于防盗措施的TLS简介。[b-IETF RFC 6460]和[b-ISO/IEC 20648]中给出了TLS简介的典例。

V.1 TLS协议要求

– 我们推荐，将作为服务器的防盗方案用于实施TLS协议；但是，客户可以选择用或不用。TLS 1.2版本（在[b-IETF RFC 5246]中有详述）或更新的版本将被实施。

V.2 互操作性TLS密码套件

– 防盗方案不得使用MD5或SHA-1作为默认的密钥散列消息认证码（HMAC）；

– 防盗方案不得使用RC4作为默认的加密算法；

注 – [b- IETF RFC 7465]禁止使用RC4。

– 防盗方案需要支持：使用TLS 1.2中支持的签名算法来选择和使用签名/哈希算法对，以及使用SHA-256或更大强度的哈希算法；

– 防盗方案需要使用具有至少112位安全强度的密码套件。此外，需要支持下列密码套件：

- TLS_RSA_WITH_AES_128_CBC_SHA256 {0x00, 0x3C}.

V.3 数字证书

防盗方案要求支持[b-ITU-T X.509]第3版的公共密钥证书（该等证书符合[b-IETF RFC 5280]第4部分中定义的证书与证书扩展配置文件）。

– 防盗方案中的TLS服务器需要支持服务器证书；

– 推荐使用防盗方案中的TLS客户端支持客户端证书；

– 防盗方案要求支持2048位或更大的密钥，以便用于[b-ITU-T X.509]证书中的RSA/DSA服务器；

– 防盗方案要求支持唯一编码规则（DER）编码的[b-ITU-T X.509]，Base64编码的[b-ITU-T X.509]和PKCS # 12 [b-IETF RFC 7292]证书格式；

– 该防盗方案需要支持证书验证，如[IETF RFC 5280]中的第6节所描述，该等证书为数字证书。此外，应使用下列方法之一来确定证书是否已被撤销：

- 方法1：使用证书撤销列表（CRL）：在DER编码的[b-ITU-T X.509]支持的CRL或用Base64编码的[b-ITU-T X.509]格式以及当地储存的有效的CRL（本标准范围以外的分布）或从外界资源恢复的CRL（例如CRL分发点（CRLDP）），
- 方法2：在以下方法当中，使用一个证书状态协议（如在线证书状态协议（OCSP））：直接使用[b-IETF RFC 6960]中描述的OCSP，并且通过[b-IETF RFC 6066]中第8部分描述的TLS证书状态请求扩展间接使用OCSP。

附录 VI

OMA设备管理概述

（本附录不构成本建议书的一部分）

本附录提供了由OMA定义的设备管理（DM）概述协议[b-OMA-DM]。

VI.1 OMA设备管理规范

OMA DM规范专门用于移动设备（如手机、PDA、平板电脑）管理。设备管理的目的是支持以下用途：

– 服务开通：设备的配置（包括第一次使用），启用和禁用功能；
– 设备配置：允许更改设备的设置和参数；
– 软件升级：加载在设备上提供新的软件和/或错误修复，包括应用程序和系统软件；
– 故障管理：从设备中报告错误，查询设备状态。

以上所有功能都是由OMA DM规范来支持，且一个设备可以选择实现所有这些功能或这些功能中的一部分。由于OMA DM规范是针对移动设备，它的设计在以下方面比较敏感：

– 微内核设备，在微内核设备中记忆和存储空间可能会受到限制；
– 对通信带宽的限制（如在无线连接中）；
– 严密的安全性（因为设备很容易受到软件攻击），身份验证和挑战也为规范中的一部分。

参考资料

[b-ITU-T X.509] ITU-T X.509建议书（2012年），信息技术 – 开放式系统互联 – 目录：公钥和属性证书框架。

[b-ITU-T X.800] ITU-T X.800建议书（1991年），CCITT应用的开放系统互连安全体系结构。

[b-ITU-T X.805] ITU-T X.805建议书（2003年），提供端到端通信的系统的安全架构。

[b-ITU-T X.1158] ITU-T X.1158建议书（2014年），使用移动设备的多因素身份验证。

[b-ITU-T X.1250] ITU-T X.1250建议书（2009年），增强全球身份管理和互操作性的基本能力。

[b-ITU-T X.1252] ITU-T X.1252建议书（2010年），基线身份管理的术语和定义。

[b-ITU-T X-Sup.19] ITU-T X-系列建议书 – 补充19（2013），智能手机安全方面的补充。

[b-ISO/IEC 20648] ISO/IEC 20648：2016年，信息技术 – 存储系统的TLS规范。

[b-ISO/IEC 27000] ISO/IEC 27000：2016年，信息技术 – 安全技术 – 信息安全管理系统—概述和词汇。

[b-ISO/IEC 27033-1] ISO/IEC 27033-1：2009年，信息技术 – 安全技术 – 网络安全 – 第1部分：概述和概念。

[b-3GPP TS 22.048] 3GPP TS 22.048（2003年），(U)SIM应用工具包的安全机制，2003年6月。

[b-3GPP TS 33.102] 3GPP TS 33.102（2009年），3G安全；安全架构（发布9），2009年12月。

[b-IETF RFC 5246] IETF RFC 5246（2008年），传输层安全（TLS）协议1.2版。

[b-IETF RFC 5280] IETF RFC 5280（2008年），互联网X.509公开密钥基础设施证书及证书撤消清单（CRL）配置文件。

[b-IETF RFC 6066] IETF RFC 6066（2011年），传输层安全（TLS）扩展：扩展定义。

[b-IETF RFC 6460] IETF RFC（2012年），传输层安全（TLS）的B套配置文件。

[b-IETF RFC 6960] IETF RFC 6960（2013年），X.509互联网公开密钥基础设施在线证书状态协议 - OCSP。

[b-IETF RFC 7292] IETF RFC 7292（2015年），PKCS #12个人信息交换句法v1.1。

[b-IETF RFC 7465] IETF RFC 7465（2015年），禁止RC4密码套件。

[b-GSMA] GSMA, SG.24防盗功能要求v3.0，2016年5月17日。

[b-OMA-DM] Open Mobile Alliance，OMA设备管理V1.2，2013年4月。

[b-NIST SP 800-88] NIST，NIST特刊800-88修订1，媒体净化导则，2014年12月。

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、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备其他组件的建设、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	电话传输质量、电话设施及本地线路网络
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、互联网协议问题、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦