

ICS 33. 600
M 60



中华人民共和国通信行业标准

YD/T 2502-2013

手机支付 移动终端安全技术要求

Mobile payment
security technical requirement for mobile terminal

2013-04-25 发布

2013-04-25 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 手机支付移动终端安全威胁	2
5 手机支付移动终端安全架构	3
6 硬件设备安全层技术要求	3
6.1 NFC-SWP 方式智能卡芯片安全要求	3
6.2 NFC 全移动终端方式内置安全模块芯片安全要求(可选)	3
6.3 对访问智能卡或内置模块的技术要求	4
6.4 射频安全要求	4
7 操作系统 OS 的安全层安全技术要求	4
7.1 操作系统存储安全要求	4
7.2 操作系统的启动和运行安全要求	4
7.3 软件应用管理安全要求	4
7.4 涉及通信连接类操作的管理安全要求	4
7.5 操作系统更新的安全要求	4
8 应用程序接口 API 安全层技术要求	5
9 业务应用安全层	5
9.1 手机支付客户端软件安全要求	5
9.2 对手机支付客户端软件提供安全保护的功能	5
9.3 通信安全要求	6
9.4 异常情况下的安全要求	6
10 运行环境的配置安全要求	7
附录 A (资料性附录) Android 安全架构	8
附录 B (资料性附录) Java API 安全策略	9
附录 C (资料性附录) Android API 访问策略	10

前 言

本标准按照 GB/T 1.1-2009给出的规则编写。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准主要依据手机支付系列相关标准制订，并结合国内外移动终端制造商的安全技术方案。

本标准是手机支付系列标准之一。该系列标准的名称预计如下：

——手机支付 术语和定义

——手机支付 总体技术要求

——手机支付 基于13.56MHz近场通信技术的移动终端技术要求

——手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块技术要求

——手机支付 基于2.45GHz射频技术的智能卡技术要求

——手机支付 基于13.56MHz近场通信技术的非接触式销售点终端技术要求

——手机支付 基于2.45GHz射频技术的非接触式销售点终端技术要求

——手机支付 基于13.56MHz和2.45GHz双频的非接触式销售点终端技术要求

——手机支付 基于13.56MHz近场通信技术的非接触射频接口技术要求

——手机支付 基于2.45GHz射频技术的非接触射频接口技术要求

——手机支付 智能卡和内置模块安全技术要求

——手机支付 移动终端安全技术要求

——手机支付 多应用管理技术要求

——手机支付 基于13.56MHz近场通信技术的移动终端测试方法

——手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块测试方法

——手机支付 基于2.45GHz射频技术的智能卡测试方法

——手机支付 基于13.56MHz近场通信技术的非接触式销售点终端测试方法

——手机支付 基于2.45GHz射频技术的非接触式销售点终端测试方法

——手机支付 基于13.56MHz和2.45GHz的双频非接触式销售点终端测试方法

——手机支付 基于13.56MHz的非接触射频接口测试方法

——手机支付 基于2.45GHz的非接触射频接口测试方法

——手机支付 智能卡和内置模块安全测试方法

——手机支付 移动终端安全测试方法

——手机支付 多应用管理测试方法

本标准由网络互联互通技术标准工作组提出。

本标准由中国通信标准化协会归口。

本标准起草单位：工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团公司。

本标准主要起草人：孙宇涛、潘 娟、袁 琦、任晓明、高庆华、张 强、戴军尧、任 鹏、宫 雪。

手机支付

移动终端安全技术要求

1 范围

本标准规定了手机支付移动终端安全技术要求,包括移动终端的安全架构、硬件设备安全层要求、操作系统安全层要求、应用程序接口API安全层要求、业务应用安全层要求、运行环境的配置安全要求等。

本标准适用于支持手机支付业务的移动终端设备。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅所注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

《智能终端信息安全 移动终端安全能力技术要求》

YD/T 2501-2013 《手机支付 智能卡和内置安全模块安全技术要求》

ISO/IEC 7816-4 信息技术.识别卡.带触点的集成电路卡.第4部分:用于交换的行业间命令

ISO/IEC DIS9798-2 信息技术.安全技术.实体鉴别.第2部分:采用对称加密算法的机制

全球平台(Global Platform)全球平台卡规范 V2.2(Global Platform Card Specification V2.2)

可信计算组织 TCG移动参考架构V1.0(TCG Mobile Reference Architecture v1.0)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

手机支付 Mobile Payment

基于NFC-SWP方式、NFC全终端方式的移动终端近场支付业务。

3.1.2

移动终端 Mobile Terminal

基于NFC-SWP方式、NFC全终端方式的移动终端。

3.1.3

可信计算 Trusted Computing

在移动终端系统中基于硬件安全模块支持下的可信计算平台,以提高系统整体的安全性。

3.1.4

操作系统 Operating System

管理移动终端硬件与软件资源的程序,同时也是移动终端系统的内核与基石,它是控制其他程序运行,管理系统资源并为用户提供操作界面的系统软件的集合。

3.1.5

应用程序接口 Application Programming Interface

一些预先定义的函数,目的是提供应用程序与开发人员基于某软件或硬件的以访问一组例程的能力,而又无需访问源码,或理解内部工作机制的细节。

3.2 缩略语

下列缩略语适用于本文件。

3DES	Triple DES	三重DES
AES	Advanced Encryption Standard	高级加密标准
APDU	Application Protocol Data Unit	应用协议数据单元
API	Application Protocol Interface	应用协议接口
CA	Certificate Authority	证书认证中心
CLDC	Connected Limited Device Configuration	有限连接设备配置
DES	Data Encryption Standard	数据加密标准
IMEI	International Mobile Equipment Identity	国际移动设备身份码
J2ME	Java 2 Platform, Micro Edition	Java 2平台, 微版本
JSR	Java Specification Request	Java规范请求
MDC	Modification Detection Code	修改检测码
MIDlet	Mobile Information Devices applet	移动信息设备小程序
MIDP	Mobile Information Device Profile	移动信息设备配置文件
OS	Operation System	操作系统
POS	Point Of Sale	销售终端
TCG	Trusted Computing Group	可信计算组织

4 手机支付移动终端安全威胁

支持手机支付的移动终端面临的安全威胁包括:

1) 对智能卡或者内置模块的非法攻击的安全威胁

攻击者通过使用非法软件访问智能卡和内置模块从而导致智能卡或者内置模块自动锁死,使手机支付无法进行。

攻击者获取访问智能卡或内置模块的认证信息后对智能卡或内置模块进行访问并获取有关信息,或者监听并获取智能卡或内置模块与移动终端的通信信息,从而使攻击者获得用户的账号、密码等机密信息,攻击者通过用户的账户进行转账、支付等给用户带来损失的非法操作。

2) 对手机支付客户端软件进行攻击的安全威胁

攻击者通过使用非法软件等方式修改客户端软件的配置参数和文件等使客户端软件无法正常启动或运行,使用户不能通过客户端软件进行手机支付业务的有关操作;窃取客户端软件的配置参数等信息,获取用户在客户端软件中输入的信息从而获得用户的密码及账号等机密信息。

3) 移动终端与外部实体进行通信时的信息窃取和攻击

在执行手机支付业务的有关操作时,移动终端通过移动通信网络或者无线局域网络等方式和远程服务器进行通信,攻击者获取有关通信信息并进行攻击等,造成业务信息泄露或者支付业务不能正常完成等安全威胁。

移动终端进行近距离支付时，攻击者通过专门的攻击设备干扰移动终端和POS之间的通信，使支付不能成功完成；或者攻击者通过专门的设备获取移动终端和POS及之间的通信信息，从而可能获得用户的账号、密码等机密信息；或者攻击者在用户不知情的情况下将POS机或者读卡器靠近用户的移动终端并进行盗刷等非法操作。

4) 移动终端的操作系统安全风险

攻击者通过恶意软件对移动终端操作系统进行攻击和破坏，使移动终端不能正常运行，从而造成用户不能使用移动终端正常的进行手机支付。

5) 访问恶意站点或钓鱼网站带来的安全威胁

用户在近场支付过程中，涉及到对网站的访问时，可能存在访问恶意网站，恶意网站可能会在用户不知情的情况下在移动终端中运行恶意软件或者盗取移动终端中的信息；攻击者创建模仿手机支付相关的钓鱼网站，用户在不知情的情况下通过移动终端访问钓鱼网站时可能会将与手机支付有关的账号与密码等机密信息泄漏给攻击者。

6) 移动终端被盗或丢失带来的安全威胁

移动终端被盗或丢失后，移动终端被别人用于支付，移动终端中存储的机密数据（例如与手机支付相关的账号、密码以及个人数据）发生泄漏。

5 手机支付移动终端安全架构

本标准作为移动终端信息安全的特殊应用，全面包含了移动终端信息安全的各个方面，具体包括硬件安全、操作系统安全、应用程序接口安全、应用软件安全等方面。

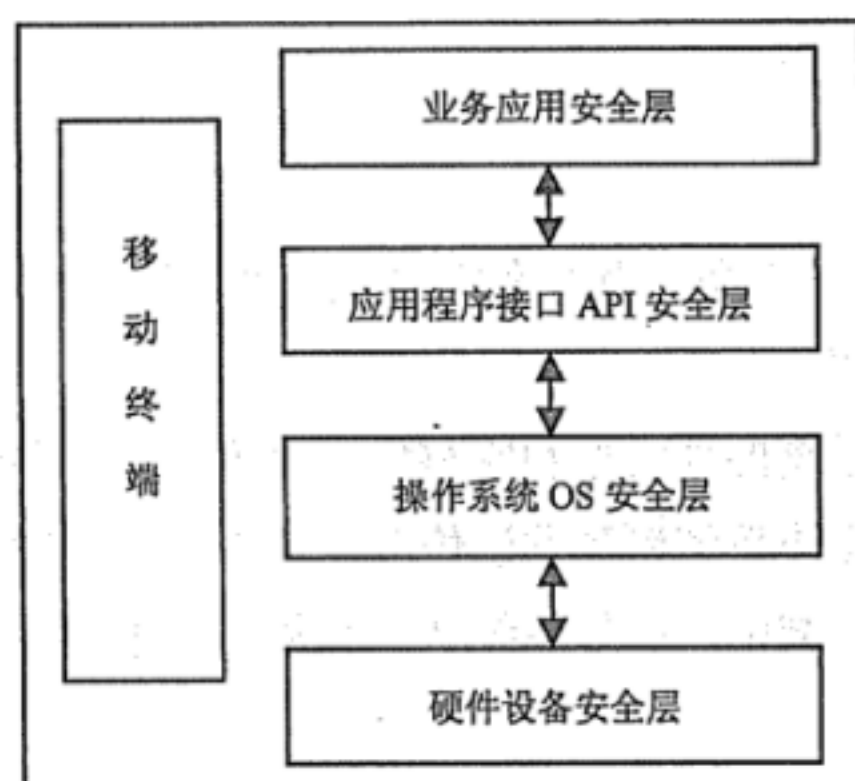


图1 手机支付移动终端安全架构

本标准的安全架构包括硬件设备安全层、操作系统OS安全层、应用程序接口API安全层、业务应用安全层等。终端安全架构见图1所示。

6 硬件设备安全层技术要求

6.1 NFC-SWP 方式智能卡芯片安全要求

相关内容见YD/T 2501-2013《手机支付 智能卡和内置模块安全技术要求》中第5章要求。

6.2 NFC 全移动终端方式内置安全模块芯片安全要求（可选）

相关内容见YD/T 2501-2013《手机支付 智能卡和内置模块安全技术要求》中第5章要求部分。

移动终端中内置芯片可采用可信计算的有关规范实现移动终端的系统安全,可采用的可信计算规范包括:

- TCG 移动参考架构 (TCG Mobile Reference Architecture v1.0);
- TCG 移动可信模块规范 (TCG Mobile Trusted Module Specification v1.0)。

采用移动终端中的内置模块存储手机支付应用时,可以将内置模块作为移动可信模块 (Mobile Trusted Module, MTM, 构建移动终端系统安全架构。

由智能卡存储手机支付应用时,移动终端中设置专门的安全模块作为移动可信模块,从而构建移动终端系统安全架构。

6.3 对访问智能卡或内置模块的技术要求

移动终端配置可以访问智能卡的软件,用户可以通过智能卡访问软件访问智能卡提供的访问内容及进行允许的手机支付业务操作。

为了避免移动终端的其他程序未经允许访问智能卡导致智能卡锁死等问题,移动终端可以对访问智能卡的权限进行管理和控制,只允许经过授权的智能卡访问软件可以访问智能卡中的相关文件。智能卡或者内置模块可以提供可以访问智能卡或者内置模块的软件的设置信息,移动终端只允许设置信息中的所允许的软件访问智能卡或者内置模块的相关文件。

6.4 射频安全要求

移动终端模拟为非接触卡和非接触读卡器之间进行通信实现非接触支付时,通信距离过大会导致恶意的非接触支付,从而影响非接触支付的安全,应设定移动终端和非接触读卡器之间进行非接触支付时的最大通信距离,最大通信距离应不超过10cm。

7 操作系统 OS 的安全层安全技术要求

7.1 操作系统存储安全要求

见《智能终端信息安全 移动终端安全能力技术要求》5.6节中的内容。

7.2 操作系统的启动和运行安全要求

操作系统启动时,应检查操作系统的真实性和完整性,检测到操作系统的某个组件出现非法修改时应进行报警并不加载该组件,避免操作系统受到非法修改和攻击下启动时所产生的安全威胁。

操作系统运行时,应保护运行区域中的操作系统文件和数据,不允许未经验证和许可对操作系统的文件进行修改。

7.3 软件应用管理安全要求

见《智能终端信息安全 移动终端安全能力技术要求》5.5.2节。

7.4 涉及通信连接类操作的管理安全要求

见《智能终端信息安全 移动终端安全能力技术要求》5.3.1.1节。

7.5 操作系统更新的安全要求

见《智能终端信息安全 移动终端安全能力技术要求》5.3.2节。

具体Android操作系统安全架构参见附录A。

8 应用程序接口 API 安全层技术要求

为保证移动终端中的软件应用符合移动终端的安全要求，移动终端在应用程序接口的管理方面应符合如下要求，应用程序接口API范围是指访问智能卡和内置模块的，实现手机支付功能的应用程序接口API：

- 移动终端应能够定义 API 的受保护安全级别以及移动终端中的各 API 所对应的受保护安全级别；
- 移动终端应定义移动终端中的应用的 API 访问权限的类别；对每类 API 访问权限，移动终端规定其对应的 API 访问控制策略，访问控制策略中包括该类 API 访问权限可以访问的 API；
- 移动终端能够根据应用的来源、是否为可信任应用等策略确定应用的类别，并为应用分配所对应的 API 访问权限；
- 移动终端中的应用在进行软件升级时，移动终端应检查是否需要调整该应用的 API 访问权限；删除移动终端中的某个应用后，移动终端应删除该应用的 API 访问权限的设置信息；
- 移动终端只允许应用执行其 API 访问权限内的 API 访问；
- 移动终端应对应用的 API 访问权限的设置信息进行保护，禁止应用修改自己或者其他应用的 API 访问权限。

移动终端将手机支付客户端软件作为一项应用进行管理，按照上述要求管理手机支付客户端软件的 API 访问权限，使手机支付客户端软件可以安全的调用移动终端提供的资源和能力。

具体Java API和android API安全策略参见附录B和附录C。

9 业务应用安全层

9.1 手机支付客户端软件安全要求

手机支付客户端软件应符合如下技术要求：

- 启动手机支付客户端软件时，应对用户进行身份验证，避免手机支付客户端软件被非法使用；
- 手机支付客户端软件应不涉及对敏感数据的存储和解密，只负责数据传输；
- 用户使用手机支付客户端软件进行在线支付时，应保证用户的输入信息的安全，避免用户输入的信息被移动终端中的其他软件或者恶意软件窃取；

应保证客户端软件本身的安全，避免客户端软件本身受到破坏和篡改；应提供客户端软件的安全管理规范，包括软件的下载、安装以及升级等环节的安全管理。

9.2 对手机支付客户端软件提供安全保护的功能

移动终端开机时，移动终端可以通过智能卡或者内置模块提供的信息识别出移动终端中安装的和手机支付相对应的手机支付客户端软件，然后对手机支付客户端软件提供安全保护。

采用的安全措施包括：

- 限制用户或其他软件对手机支付客户端软件进行修改、删除等操作；
 - 保护手机支付客户端软件的存储，不允许用户或其他软件对其文件和数据进行修改；
 - 手机支付客户端软件运行时，为该软件设置单独的运行区域，不允许其他程序访问客户端软件的运行区域，手机支付客户端软件运行结束后移动终端主动清除该手机支付客户端软件运行区域中的数据；
- 对手机支付客户端软件升级的保护：只允许从指定的远程服务器对手机支付客户端软件进行远程升级。

9.3 通信安全要求

9.3.1 与远程服务器通信安全要求

用户在移动终端上启动支付客户端软件，支付客户端软件和远程服务器之间建立通信，完成相关业务流程。支付客户端软件和远程服务器之间应进行身份验证并采取相应的安全措施，以保证通信数据的机密性和完整性。

9.3.2 近距离通信安全要求

移动终端模拟为非接触卡和非接触读卡器之间进行通信实现非接触支付时，通信距离过大可能会导致恶意的非接触支付，从而影响非接触支付的安全，应设定移动终端和非接触读卡器之间进行非接触支付时的最大通信距离，最大通信距离应不超过4cm。

9.4 异常情况下的安全要求

9.4.1 概述

支持手机支付的移动终端在进行支付应用下载、支付应用个人化、支付交易时，有可能遇到异常情况而影响正在进行的处理过程，从而造成处理过程不能正常完成和安全问题；潜在的异常情况包括设备断电、网络连接中断、多应用并发（例如，支付交易过程中接收到语音呼叫或短消息）、人为原因造成处理过程中断等。

9.4.2 支付应用下载过程中遇到异常情况时的安全技术要求

在手机支付应用下载过程中，由于网络连接中断、支付业务终端断电、移动终端断电及人为中断下载过程等异常情况，会导致手机支付应用下载中断。针对手机支付应用下载中断的处理应遵循以下安全要求：

- 在移动终端不保存手机支付应用下载中断状态信息的情况下，应能够重新启动手机支付应用的下载过程；
- 在移动终端保存手机支付应用下载中断状态信息的情况下，在重新启动手机支付应用下载过程时，移动终端根据保存的手机支付应用下载中断状态信息，从中断处恢复手机支付应用的下载过程，完成手机支付应用的下载。

移动终端在支付应用下载过程中遇到多应用并发情况时，应符合下面的要求：

- 在语音通话、短信或移动数据业务的过程中，需要进行支付应用下载时，应能够保证通话、短信或移动数据业务过程不影响支付应用下载过程的正常进行；
- 在进行支付应用下载过程中，有电话接入、接收短信或移动数据业务发生时，应能够保证通话、短信或移动数据业务过程不影响支付应用下载过程的正常进行。

9.4.3 支付应用个人化过程遇到异常情况时的安全技术要求

手机支付应用下载并完成安装后，需要进行个人化过程以获得手机支付应用相关的个人化数据。手机支付应用个人化过程中，由于网络连接中断、支付业务终端断电、移动终端断电或人为中断等原因，会导致个人化过程不能正常完成。手机支付应用个人化过程中断处理应当遵循以下要求：

- 由于网络连接中断、支付业务终端断电、移动终端断电或人为中断等原因导致手机支付应用个人化过程不能正常完成时，手机支付应用个人化过程应立即终止；
- 手机支付应用个人化过程中断后，移动终端在异常情况恢复正常时应能够重新启动手机支付应用个人化过程。

移动终端在支付应用个人化过程中遇到多应用并发情况时，应符合下面的要求：

- 在语音通话、短信或移动数据业务的过程中，需要进行支付应用个人化时，应能够保证通话、短信或移动数据业务过程不影响支付应用个人化过程的正常进行；
- 在进行支付应用个人化过程中，有电话接入、接收短信或移动数据业务发生时，应能够保证通话、短信或移动数据业务过程不影响支付应用个人化过程的正常进行。

9.4.4 在手机支付交易过程中遇到异常情况时的安全技术要求

在手机支付交易过程中，当移动终端由于低电或其他原因突然关机时，应能够保证手机支付应用的使用安全。包括如下情况：

- 在移动终端由于低电或其他原因异常关机，而造成本次手机支付交易中断的情况下，下一次手机支付交易应当能正常安全进行，而不受移动终端异常关机的影响；
- 支持关机状态下进行近距离支付的移动终端，在出现关机时应能够继续完成本次近距离支付。

移动终端在支付交易过程中遇到多应用并发情况时，应符合下面的要求：

- 在语音通话、短信或移动数据业务的过程中，需要进行手机支付交易时，应能够保证语音通话、短信或移动数据业务过程不影响手机支付交易过程的正常进行；
- 在进行手机支付交易的过程中，有电话接入、接收短信或移动数据业务发生时，应能够保证通话、短信或移动数据业务过程不影响手机支付交易过程的正常进行。

10 运行环境的配置安全要求

从移动终端系统安全考虑，移动终端应阻止外部网络对移动终端的非法访问和入侵，控制移动终端中的未经允许的数据输出，防止恶意软件通过移动终端对支付系统进行攻击以及移动终端中的信息的泄漏。另外，在移动终端中建议配置防病毒软件，防止移动终端受到病毒的攻击，维护移动终端系统的安全。

附录 A

(资料性附录)

Android 安全架构

A.1 概述

Android操作系统的安全措施包括沙箱(Sandbox)、许可(Permission)、应用程序签名(Application Signature)。支持手机支付的移动终端采用Android操作系统时应符合Android操作系统的上述安全措施的技术要求。

A.2 沙箱

Android 使用沙箱的概念来实现应用程序之间的分离和权限,以允许或拒绝一个应用程序访问设备的资源,比如说文件和目录、网络、传感器和 API。两个Android 应用程序,各自在其自己的基本沙箱或进程上。

A.3 许可

Android应用程序需要在自己的配置文件AndroidManifest.xml中声明需要的许可权限,包括申请访问的API和需要的系统资源。应用程序在Android系统中安装时,Android系统检查该应用程序申请的许可权限并将该应用程序申请的许可权限显示给用户,由用户判断是否授予该应用程序相应的权限。应用程序被授予其申请的许可权限后,Android系统只允许该应用程序访问其所申请的API和系统资源。

A.4 应用程序签名

Android对于应用程序签名的要求如下:

- Android 系统要求每一个安装在 Android 系统的应用程序都需要经过数字证书签名,数字证书的私钥由程序开发者安全保存。Android 将数字证书用来标识应用程序的作者和在应用程序之间建立信任关系。

- 使用相同数字签名签署的两个应用程序可以相互授予权限来访问基于签名的 API,如果它们共享用户 ID,那么也可以运行在同一进程中,从而允许访问对方的代码和数据。

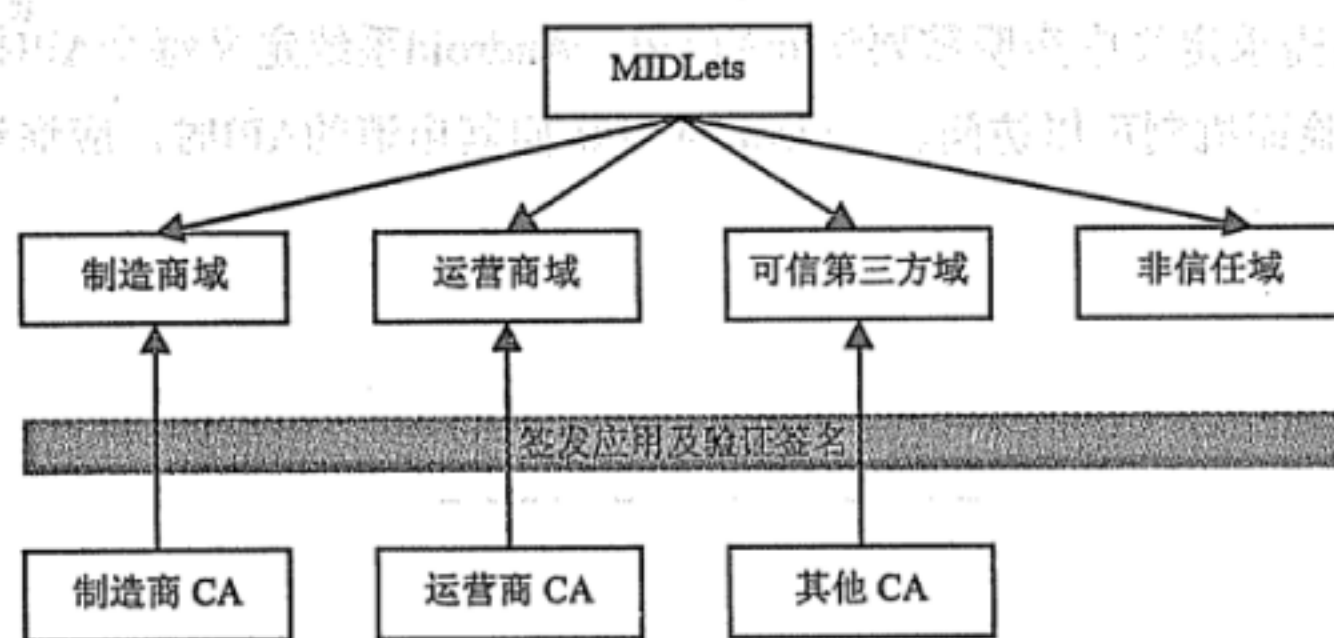
- 同一个开发者的多个程序尽可能使用同一个数字证书

- 数字证书的有效期:

数字证书的有效期需包含应用程序的预计生命周期,一旦数字证书失效,持有该数字证书的应用程序将不能正常升级。如果多个程序使用同一个数字证书,则该数字证书的有效期应包含所有程序的预计生命周期。Android Marke强制要求所有应用程序数字证书的有效期要持续到2033年10月22日以后。

附录 B
(资料性附录)
Java API 安全策略

移动终端支持Java 2平台Java ME时，应符合JSR-118 (MIDP 2.0规范)和JSR-139 (CLDC 1.1规范)规范，实现MIDP 2.0中定义的Java API。移动终端应支持的保护域包括：制造商域、运营商域、可信第三方域以及非信任域，每个保护域都与一系列的访问控制策略相对应，前三个保护域都通过代码签名验证机制确定应用的可信性，而非信任域则无须签名验证。具有合法签名的应用可以经过相应保护域的验证，相应的，对于敏感API可以定义为自动授予（也就是经过该保护域的验证就可以自动获得授权），也可以是用户批准（也就是经过用户许可才可以执行），没有合法签名的应用只能安装到非信任域，敏感API禁止访问或由用户批准。支持Java ME的移动终端提供的保护域如图B.1所示。



图B.1 支持Java ME的移动终端提供的保护域

对应用的签名验证可以采用基于PKI的代码签名机制，要求如下：

- 移动终端首先需要内置CA根证书（不同的保护域，根证书不同）；
- 开发者向CA申请证书，CA签发证书；
- 开发者开发应用后采用开发者证书签名，并发行应用；
- 手机用户下载/安装应用过程中，移动终端做签名验证。

在应用安装时，应用声明需要访问的API列表以及需要加入的保护域；每个保护域对应用的签名进行验证，并根据定义的API权限列表和对应的授权模式，在应用安装及运行过程中进行检查；通过检查后，应用才可以使用相应的API。

附录 C

(资料性附录)

Android API 访问策略

Android采用保护级别实现对受保护的API进行访问控制, 支持的保护级别包括:

- Normal: 无须授权即可拥有的权限, 主要针对用户影响小, 或用户不关注的 API 或资源;
- Dangerous: 权限在安装时需要用户确认才可以使用。像 WRITE_SETTINGS、SEND_SMS 这样的操作是危险的, 因为这会导致更改配置或引入费用。Android 会在安装时警告用户;
- Signature: 通过签名机制, 授权给与 API 或应用具有同样签名的其他应用;
- SignatureOrSystem: Signature 或者 System, 其中 Signature 与上面的签名机制相同, System 指对于系统内不同模块的访问无须授权。

Android应用在权限需求定义中声明需要访问的API, Android系统定义每个API接口的保护级别, 即需要通过什么样的权限验证机制可以访问。Android应用访问其申请的API时, 应通过相对应的保护级别的验证。

中华人民共和国
通信行业标准
手机支付
移动终端安全技术要求
YD/T 2502-2013

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061

宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2013年5月第1版
印张：1 2013年5月北京第1次印刷
字数：25千字

15115·171

定价：15元

本书如有印装质量问题，请与本社联系 电话：(010)67114922