ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34977—2017

信息安全技术　移动智能终端数据存储安全技术要求与测试评价方法

Information security technology—Security technology requirements and testing and evaluation approaches for data storage of mobile intelligent terminals

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国移动通信有限公司研究院、北京邮电大学、中国信息安全认证中心、成都电子科技大学、北京智言金信信息技术有限公司。

本标准主要起草人:何申、张二鹏、彭华熹、刘颖卿、徐国爱、张淼、秦潇潇、王佳昊、陈彪。

信息安全技术　移动智能终端数据存储安全技术要求与测试评价方法

1　范围

本标准规定了移动智能终端数据存储的安全技术要求、测试评价方法及安全等级划分。

本标准适用于移动智能终端厂商、移动操作系统提供商以及应用开发商开展移动智能终端数据存储安全设计、开发与测试。本标准仅适用于连接互联网的移动智能终端，保护的数据包含有硬件信息、操作系统数据、应用软件数据和用户个人数据等存储在移动智能终端中的非涉密数据。

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。

GB/T 25069—2010　信息安全技术　术语

3　术语和定义、缩略语

3.1　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

移动智能终端　mobile intelligent terminal

具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行第三方应用软件的移动终端。

3.1.2

移动智能终端信息系统　information system of mobile intelligent terminal

由移动智能终端及其配套设备、设施(含网络)构成的，按照一定的应用目标和规则对数据进行采集、加工、存储、传输、检索等处理的信息系统。

3.1.3

用户　user

使用移动智能终端资源的对象，包括人或第三方应用程序。

3.1.4

授权用户　authorized user

经过系统的身份认证后，根据预先设置的安全策略，已被授予相应权限的用户。

3.1.5

销毁　destroy

从信息系统和载体上永久清除数据并不可恢复。

3.1.6

备份　backup

信息系统为了防止数据及应用等因移动智能终端故障而造成丢失及损坏，从而在原文件中独立出

来单独贮存的程序或文件副本。

3.2 缩略语

下列缩略语适用于本文件。

CPU	中央处理器	(Central Processing Unit)
IMEI	国际移动设备识别码	(International Mobile Equipment Identity)
UDID	设备的唯一设备识别符	(Unique Device Identifier)
IMSI	国际移动用户识别码	(International Mobile Subscriber) (Identification Number)
PIN	SIM 卡的个人识别密码	(Personal Identification Number)
RAM	随机存取存储器	(Random Access Memory)
ROM	只读存储器	(Read-Only Memory)
SIM	客户识别模块	(Subscriber Identity Module)

4 数据信息的分类

移动智能终端中的数据分为以下四大类:硬件信息、操作系统数据、应用软件数据和用户个人数据。

4.1 硬件信息

移动智能终端的硬件信息是指关于硬件设备的信息,细分为如下两类:

a) 硬件基本信息:移动智能终端硬件设备的基本信息,例如移动智能设备的型号、设备名称、系统版本、RAM 和 ROM 大小、CPU 类型以及存储器的型号等;

b) 硬件配置数据:移动智能终端硬件设备的程序代码及配置数据,例如启动加载代码及数据、指令代码集等。

4.2 操作系统数据

操作系统数据主要是指操作系统自身包含的数据,细分为如下四类:

a) 操作系统参数信息:操作系统自身包含的描述性数据,例如操作系统版本号和操作系统位数等;

b) 操作系统程序文件:操作系统的运行程序及支撑文件,例如操作系统内核程序文件、驱动程序文件和接口库文件等;

c) 操作系统配置信息:操作系统的配置信息,例如系统安全配置信息、系统权限配置信息、数字证书等;

d) 操作系统密钥:操作系统相关密钥。

4.3 应用软件数据

应用软件数据主要是指应用软件自身包含的数据,其可细分为以下三类:

a) 应用程序文件:应用软件的程序代码的存储文件,例如应用软件可执行程序文件等;

b) 配置数据:应用软件的资源文件及配置文件,例如图片、字符串、配置信息等;

c) 代码签名证书:软件开发商用于对软件进行签名的证书。

4.4 用户个人数据

用户个人数据是指用户在使用移动智能终端的过程中产生的数据,细分为以下七类:

a) 通信信息是指移动智能终端用户用于发起或接受通信以及在通信过程中所产生的数据信息，包括通讯录、短信、邮件等；

b) 使用记录数据是指用户在使用移动智能终端的过程中间接产生的、反映用户操作记录的数据缓存数据，包括日志数据、通话记录、浏览器记录数据等；

c) 账户信息是指移动智能终端应用程序在注册或登录时需要填写的信息，以及应用程序所存储的用户相关信息；

d) 金融支付信息是指移动智能终端用户借助终端参与金融交易或支付活动而产生的数据信息，包括交易验证码、动态口令等；

e) 传感采集信息是指利用移动智能终端传感器设备所采集到的、能反映移动智能终端设备使用者的周边环境和身份特征的数据信息，包括地理位置信息、指纹信息等；

f) 用户设备信息是指可标识移动智能终端唯一性的数据信息，包括 IMEI、UDID 等；

g) 文件信息是指存储在移动智能终端设备存储介质中的数据信息。包括照片、音频、视频、文本等各种类型文件数据。

5 移动智能终端数据存储安全框架和目标

5.1 安全框架

图 1 为移动智能终端数据存储安全框架，主要包含 4 个部分：最底层是硬件信息存储安全，中间层是操作系统数据存储安全，顶层是应用软件数据存储安全，用户个人数据存储安全涉及应用软件、操作系统及硬件 3 个层面。

图 1 移动智能终端数据存储安全框架

5.2 安全目标

本标准以硬件信息、操作系统数据、应用软件数据、用户个人数据的机密性、完整性和可用性为安全目标，并分别提出数据存储安全技术要求。

5.2.1 机密性

数据的机密性是指数据和数据状态信息只能被授权用户正当获取和使用，不能泄露给未授权用户，确保隐私信息、私有数据和重要数据的机密性。

5.2.2 完整性

数据的完整性是指数据不被不正当地篡改或销毁，并具有不可否认性和真实性。移动智能终端应该保证隐私信息、私有数据和重要数据的完整性。

5.2.3 可用性

数据的可用性是指数据可被授权用户访问并按需求使用，即保证授权用户对数据的使用不会被不

合理地拒绝。移动智能终端应该保证数据具有可用性。

6 移动智能终端数据存储安全等级划分

根据移动智能终端所支持的数据存储安全能力和程度，将移动智能终端的数据存储安全划分为两个等级：基本级和增强级。

基本级规定了移动智能终端数据存储安全的基本技术要求，其包含了基本级应支持的数据存储安全能力集合。

增强级规定了移动智能终端数据存储安全应满足基本级要求以外还应满足的增强的数据存储安全技术要求其包含了增强级应支持的数据存储安全能力集合。

7 移动智能终端数据存储安全技术要求

7.1 安全技术要求汇总表

移动智能终端的数据存储安全技术要求汇总表如表 1 所示，其中“—”表示对相应的终端数据不作安全技术要求，“*”表示相应的终端数据应遵循 7.2、7.3 的安全技术要求。

表 1 移动智能终端数据存储安全技术要求汇总表

数据存储安全等级	终端数据		安全技术要求						
			加解密	完整性检测	访问控制	安全隔离	备份/恢复	数据销毁	安全审计
基本级	硬件信息	硬件基本信息	—	—	*	*	—	—	—
		硬件配置数据	—	*	*	*	—	—	—
	操作系统数据	操作系统参数信息	—	—	*	*	—	—	—
		操作系统程序文件	—	*	*	*	*	—	—
		操作系统配置信息	—	*	*	*	*	*	—
		操作系统密钥	*	*	*	*	*	*	—
	应用软件数据	应用程序文件	—	*	*	*	—	—	—
		资源文件	—	—	*	*	—	—	—
		代码签名证书	—	*	*	*	—	—	—
	用户个人数据	通信信息	—	*	*	*	*	*	—
		使用记录数据	—	—	*	*	—	—	—
		账户信息	*	*	*	*	—	*	—
		金融支付信息	*	*	*	*	—	*	—
		传感采集信息	*	*	*	*	—	*	—
		用户设备信息	—	—	*	*	—	—	—
		文件信息	—	—	*	*	—	—	—

表 1（续）

数据存储安全等级	终端数据		安全技术要求						
			加解密	完整性检测	访问控制	安全隔离	备份/恢复	数据销毁	安全审计
增强级	硬件信息	硬件基本信息	—	*	*	*	—	—	—
		硬件配置数据	—	*	*	*	—	—	—
	操作系统数据	操作系统参数信息	—	—	*	*	—	—	—
		操作系统程序文件	—	*	*	*	*	*	*
		操作系统配置信息	*	*	*	*	*	*	*
		操作系统密钥	*	*	*	*	*	*	*
	应用软件数据	应用程序文件	—	*	*	*	—	*	*
		资源文件	—	*	*	*	—	*	*
		代码签名证书	—	*	*	*	—	*	*
	用户个人数据	通信信息	*	*	*	*	*	*	*
		使用记录数据	*	*	*	*	*	*	*
		账户信息	*	*	*	*	*	*	*
		金融支付信息	*	*	*	*	*	*	*
		传感采集信息	*	*	*	*	*	*	*
		用户设备信息	*	*	*	*	—	—	*
		文件信息	*	*	*	*	*	*	*

7.2 基本级安全技术要求

7.2.1 加解密

应对移动智能终端数据进行加密存储，实现对数据的机密性和完整性进行保护，加解密操作应采用国家密码主管部门认可的密码算法。

对于加密的数据，未授权实体无法获得或操作明文，授权实体可通过合理的解密获得和操作明文，保证数据的可用性。

7.2.2 完整性检测

应对移动智能终端数据进行读取操作时的完整性检测，发现数据的完整性是否被破坏，防止未授权实体对数据进行篡改、删除和插入等操作。

数据完整性遭到破坏时，应提供授权用户可察觉的告警信息。

7.2.3 访问控制

当非授权实体访问移动智能终端数据时，系统应终止非授权实体的访问行为，并提供授权用户可察觉的告警信息。移动智能终端操作系统和应用软件访问或试图修改移动智能终端数据时，应确保授权用户知情并可控。

应用软件初装时应与授权用户约定其访问数据的权限。授权用户应可随时收回和授予实体访问移

动智能终端数据的权限。

7.2.4 安全隔离

应对移动智能终端数据进行安全隔离，为每个实体的数据分配独立的内存空间，以防止不同实体间数据的非法访问。

7.2.5 备份和恢复

为防止移动智能终端数据在系统硬件或存储介质出现故障时受到损坏而无法还原，系统应提供移动智能终端数据的备份和恢复功能。

数据备份包括本地备份和远程备份两种，本地备份是通过移动智能终端的外围接口实现的数据备份；远程备份是通过无线网络实现的数据在服务器侧的备份。移动智能终端应至少支持一种备份方式。

备份数据应与原数据具有相同的访问控制权限和安全存储要求。

远程备份存储设备、存储介质位置应在中华人民共和国境内，未经移动智能终端用户授权不得使用、处理备份的数据。

系统应提供授权用户恢复移动智能终端数据的功能。在移动智能终端数据受到损坏时，授权用户应可自主选择特定时间节点的备份文件对数据进行有效的恢复。

7.2.6 数据销毁

系统应提供销毁移动智能终端数据的功能，保证被销毁的移动智能终端数据无法恢复，确保移动智能终端数据的机密性。

系统应提供操作确认机制，以确保当且仅当在用户知情或控制下才能对移动智能终端数据执行销毁操作，避免误操作。

7.3 增强级安全技术要求

7.3.1 加解密

移动智能终端数据加解密的增强级技术要求应满足其基本级的加解密技术要求，此外还应支持国家密码主管部门认可的高强度加密技术对移动智能终端数据进行加密存储，如采用硬件加密芯片等。

7.3.2 完整性检测

移动智能终端完整性检测的增强级技术要求应满足其基本级的完整性检测技术要求，此外还应支持发现数据的完整性遭到破坏时，系统应能利用已经备份的数据进行有效的恢复，从而保证数据的可用性。

7.3.3 访问控制

移动智能终端数据访问控制的增强级技术要求应满足其基本级的访问控制技术要求，此外还应支持授权用户可制定和更改移动智能终端数据的访问控制列表，设置数据的访问规则，未授权用户应无法访问和更改移动智能终端数据的访问控制列表。

7.3.4 安全隔离

移动智能终端数据安全隔离的增强级技术要求应满足其基本级的安全隔离技术要求，此外还应支持：

a） 移动智能终端系统中用于进行基础认证的信息和程序应存放于不可更改的存储空间；

b） 应支持安全隔离策略，以实现用户的身份认证、程序的访问权限控制、程序之间通信的安全可靠。

7.3.5 备份和恢复

移动智能终端数据备份和恢复的增强级技术要求应满足其基本级的数据备份和恢复技术要求，此外还应支持：

a） 系统应提供身份认证等安全措施，确保仅授权用户知情或控制下才能执行本地和远程备份和恢复数据的操作；

b） 备份数据应进行加密存储。

7.3.6 数据销毁

移动智能终端数据销毁的增强级技术要求应满足其基本级的数据销毁技术要求，此外还应包括：

a） 系统应提供远程销毁数据的功能，以保证在移动智能终端遗失等情况下，移动智能终端数据不被泄漏；

b） 系统应提供身份认证等安全措施，以确保当且仅当在授权用户知情或控制下才能执行远程销毁数据的操作。

7.3.7 安全审计

移动智能终端应提供安全审计功能，对移动智能终端数据的创建、更改、拷贝、移动和删除等事件进行审计。

a） 系统应提供设定审计事件类型和审计数据对象的功能。对于每一受审计的事件，其审计记录应至少包括：事件的时间、操作的数据、操作者及其权限、事件类型和事件是否成功等信息，以便系统对事件进行审核，并供授权用户查看。

b） 系统应对有安全风险的操作进行主动告警。

c） 应对审计记录进行访问控制，提供授权用户可查看审计记录的界面。

8 移动智能终端数据存储安全测试评价方法

8.1 基本级测试评价方法

8.1.1 加解密

对移动智能终端数据加解密的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 以授权用户的身份查看是否能对移动智能终端数据进行加密操作；

2） 使用正确的密钥对加密的移动智能终端数据进行解密，查看是否可获得正确明文；

3） 使用错误的密钥对加密的移动智能终端数据进行解密，查看是否可获得正确明文。

b） 预期结果：

1） 授权用户可成功对移动智能终端数据进行加密操作；

2） 使用正确的密钥可成功解密得到正确的明文；

3） 使用错误的密钥无法解密得到正确的明文。

8.1.2 完整性检测

对移动智能终端数据的完整性检测的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 对移动智能终端数据的完整性进行破坏，再以授权用户的身份查看是否可对完整性受到破坏的移动智能终端数据进行完整性检测；

2） 完整性遭到破坏，查看系统是否会提示告警信息。

b） 预期结果：

1） 授权用户可对移动智能终端数据进行完整性检测；

2） 完整性遭到破坏，系统会提示用户告警信息。

8.1.3 访问控制

对移动智能终端数据访问控制的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 以非授权用户的身份访问移动智能终端数据，查看系统是否会阻止该访问操作，并查看系统是否会向用户告警；

2） 使用应用软件，在未获得权限的情况下对移动智能终端数据进行非法访问，查看系统是否告警授权用户；

3） 安装一个新的应用软件，查看系统是否提示用户与该应用软件约定其访问用户移动智能终端数据的权限；

4） 任选一个实体如应用软件，以授权用户的身份查看是否能随时收回和授予其访问移动智能终端数据的权限。

b） 预期结果：

1） 系统提示告警信息，并阻止非授权用户的访问操作；

2） 系统终止非法访问，并告警授权用户；

3） 系统提示用户与应用软件约定其访问数据的权限；

4） 授权用户能随时收回和授予实体访问移动智能终端数据的权限。

8.1.4 安全隔离

对移动智能终端数据安全隔离的测试评价方法和预期结果如下：

a） 测试评价方法：

查看不同的实体（如应用软件），是否可以互相访问数据，不同实体的数据是否进行了隔离存储。

b） 预期结果：

不同实体的数据进行了隔离存储，不能互相访问数据。

8.1.5 备份和恢复

对移动智能终端数据备份的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 以授权用户的身份查看是否支持数据的本地备份或远程备份；

2） 以非授权用户的身份查看是否具有备份数据的权限；

3） 查看备份数据是否满足原数据的安全存储要求。

b） 预期结果：

1） 系统支持数据的本地备份或远程备份；

2） 非授权用户没有数据备份的权限；

3） 备份数据与原数据具有相同的安全存储要求。

对移动智能终端数据恢复的测试评价方法与预期结果如下：

a） 测试评价方法：

分别以授权用户和非授权用户的身份检测是否可启动数据恢复功能，查看是否能选择不同时间节点的移动智能终端数据备份文件，并进行数据恢复，再检查是否正确恢复。

b） 预期结果：

授权用户可启动数据恢复功能，并可选择不同时间节点的备份文件对数据正确恢复，非授权用户无法启动数据恢复功能。

8.1.6 数据销毁

对移动智能终端数据销毁的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 分别以授权用户和非授权用户的身份检测是否能选择移动智能终端数据执行销毁操作，并查看系统是否提示用户确认操作；

2） 授权用户销毁数据后，检查是否销毁成功，尝试对数据进行恢复操作，查看能否恢复成功。

b） 预期结果：

1） 授权用户可对移动智能终端数据执行销毁操作，且系统会弹出消息框提示用户确认操作，非授权用户无法执行销毁移动智能终端数据的操作；

2） 授权用户销毁移动智能终端数据后，无法恢复已销毁的数据。

8.2 增强级测试评价方法

8.2.1 加解密

对移动智能终端数据加解密的增强级的测试评价方法包含其基本级的测试评价方法，此外还应包含：

a） 测试评价方法：

以授权用户的身份查看是否支持高强度的加密技术对移动智能终端数据进行加密存储，如采用硬件加密芯片等。

b） 预期结果：

采用了高强度的加密算法（如硬件加密芯片等）对移动智能终端数据进行加密存储。

8.2.2 完整性检测

对移动智能终端完整性检测的增强级的测试评价方法包含其基本级的测试评价方法，此外还应包含：

a） 测试评价方法：

1） 对移动智能终端数据的完整性进行破坏，再以授权用户的身份访问移动智能终端数据，并查看系统是否会对数据进行完整性检测；

2） 查看系统是否能利用备份数据对移动智能终端数据进行有效的恢复。

b） 预期结果：

1） 系统支持对移动智能终端数据进行完整性检测；

2） 如果有备份数据，系统能利用备份数据对移动智能终端数据进行有效的恢复，若没有备份数据，则系统会告知用户无法恢复。

8.2.3 访问控制

对移动智能终端数据访问控制的增强级的测试评价方法包含其基本级的测试评价方法，此外还应

包含：

a） 测试评价方法：

1） 分别以授权用户和非授权用户的身份检测是否能对移动智能终端数据的访问控制列表进行读取和更改；

2） 以授权用户的身份查看是否可以对移动智能终端数据设置不同的访问权限。

b） 预期结果：

1） 授权用户可以读取和更改移动智能终端数据的访问控制列表，非授权用户无法读取和更改移动智能终端数据的访问控制列表；

2） 授权用户可以对移动智能终端数据设置不同的访问权限。

8.2.4 安全隔离

对移动智能终端数据安全隔离的增强级的测试评价方法应包含其基本级的测试评价方法，此外还应包括：

a） 测试评价方法：

1） 以授权用户的身份查看移动智能终端系统中用于进行基础认证的信息和程序是否存放于不可更改的存储空间；

2） 查看是否有安全隔离策略，安全隔离策略是否满足要求。

b） 预期结果：

1） 移动智能终端系统中用于进行基础认证的信息和程序存放于不可更改的存储空间；

2） 支持安全策略，安全策略满足要求。

8.2.5 备份和恢复

对移动智能终端数据备份的增强级的测试评价方法应包含其基本级的测试评价方法，此外还应包括：

a） 测试评价方法：

1） 尝试执行本地备份或远程备份移动智能终端数据操作，检查系统是否会验证用户身份信息；

2） 查看备份数据是否进行加密存储。

b） 预期结果：

1） 系统会验证用户身份信息，如要求用户提供正确的账号和密码等；

2） 备份数据采用加密存储。

对移动智能终端数据恢复的增强级的测试评价方法与预期结果包含其基本级的测试评价方法与预期结果，此外，还应包含：

a） 测试评价方法：

1） 尝试执行从本地备份或远程备份进行数据恢复操作，检查系统是否会验证用户身份信息；

2） 以授权用户的身份检测是否可启动数据恢复功能，并检测是否可使用本地备份或远程备份文件有效地恢复移动智能终端数据。

b） 预期结果：

1） 系统会验证用户身份信息，如要求用户提供正确的账号和密码等；

2） 授权用户可启动数据恢复功能，使用本地备份或远程备份文件可有效地恢复移动智能终端数据。

8.2.6 数据销毁

对移动智能终端数据销毁的增强级的测试评价方法包含其基本级的测试评价方法，此外，还应

包含：

a） 测试评价方法：

1） 尝试执行远程销毁移动智能终端数据操作，检查系统是否会验证用户身份信息；

2） 以授权用户的身份远程销毁移动智能终端数据后，检查原始数据是否还存在，尝试对数据进行恢复操作，查看能否恢复成功。

b） 预期结果：

1） 系统会验证用户身份信息，如要求用户提供正确的账号和密码；

2） 授权用户销毁移动智能终端数据后，原始数据已彻底删除，无法对原始数据进行有效的恢复。

8.2.7 安全审计

对移动智能终端数据安全审计的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 以非授权用户的身份对移动智能终端数据分别进行创建、读取、更改、拷贝、移动和删除等操作，操作完成后，退出系统，再以授权用户的身份查看系统是否已生成审计记录，查看审计记录中是否包括事件的时间、操作的数据、操作者及其权限、事件类型和事件是否成功等信息；

2） 分别以授权用户和非授权用户的身份检测是否能查看所生成的审计记录内容；

3） 以授权用户的身份查看审计记录是否存在非授权用户创建、读取、更改、拷贝、移动和删除移动智能终端数据的事件的详细信息；

4） 进行对移动智能终端安全构成威胁的操作，如删除系统文件等，查看系统是否进行主动告警；

5） 以非授权用户的身份访问审计记录，查看是否有权限访问。

b） 预期结果：

1） 对于非授权用户对移动智能终端数据执行的创建、读取、更改、拷贝、移动和删除等操作，系统已生成审计记录，审计记录内容包括事件类型、事件发生时间、操作的数据、操作者及其权限、事件是否成功以及事件性质等；

2） 授权用户能查看所生成的审计记录，非授权用户不能查看所生成的审计记录；

3） 审计记录中存有非授权用户创建、读取、更改、拷贝、移动和删除移动智能终端数据的事件；

4） 系统针对有安全风险的操作进行主动告警；

5） 非授权用户没有权限访问审计记录，授权用户可查看审计记录。

参 考 文 献

[1] GB/T 17859—1999 计算机信息系统 安全保护等级划分准则
[2] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[3] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[4] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[5] YD/T 1699—2007 移动终端信息安全技术要求
[6] YD/T 1886—2009 移动终端芯片安全技术要求和测试方法
[7] YD/T 2407—2013 移动智能终端安全能力技术要求
[8] YD/T 2408—2013 移动智能终端安全能力测试方法