ICS 35.240
A.90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

信息安全技术　移动智能终端用户数据存储安全技术要求和测试评价方法

Information security technology　Security technical requirements and testing and evaluation methods for user data storage of mobile intelligent terminal

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　　发布

目　　次

1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 总体说明 1
4.1 安全技术要求分级 2
4.2 安全技术要求分类 2
5 安全技术要求 2
5.1 数据存储 2
5.2 数据访问控制 2
5.3 数据备份与恢复 3
5.4 数据销毁 3
5.5 安全审计 3
6 测试评价方法 3
6.1 数据存储 4
6.2 数据访问控制 5
6.3 数据备份与恢复 6
6.4 数据销毁 6
6.5 安全审计 7
7 不同安全等级的要求 7

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部网络安全保卫局。

本标准主要起草人：邹春明、唐迪、俞优、沈亮、张艳、宋好好、顾健。

信息安全技术 移动智能终端用户数据存储安全技术要求和测试评价方法

1 范围

本标准规定了移动智能终端的用户数据存储安全技术要求、测试评价方法和等级划分要求。

本标准适用于不同安全等级信息系统中移动智能终端操作系统及应用程序在用户数据存储安全方面的设计、开发及检测。

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 18336.2－2015 信息技术 安全技术 信息技术安全评估准则 第2部分:安全功能组件

GB/T 25069－2010 信息安全技术 术语

GB/T 30284－2013 移动通信智能终端操作系统安全技术要求（EAL2级）

3 术语和定义

GB/T 18336.2－2015、GB/T 25069－2010和GB/T 30284－2013界定的以及下列术语和定义适用于本文件。

3.1

移动智能终端 mobile intelligent terminal

接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端设备。

3.2

用户数据 user data

由用户产生或为用户服务的重要数据。

3.3

主体 subject

实施操作的实体。

3.4

客体 object

由主体操作的实体对象。

4 总体说明

4.1 安全技术要求分级

移动智能终端用户数据存储安全技术要求的安全等级按照数据存储、数据访问控制、数据备份与恢复、数据销毁、安全审计的强度划分为基本级和增强级。

4.2 安全技术要求分类

本标准主要基于移动智能终端用户数据存储的生命周期提出各阶段的具体安全技术要求，包括数据存储、数据访问控制、数据备份与恢复、数据销毁及安全审计五个方面。

5 安全技术要求

5.1 数据存储

5.1.1 存储介质

对用户数据提供安全的存储介质及存储路径：

a） 用户数据应存储在掉电非易失存储介质中；

b） 对主体产生的用户数据，应存储在默认或者设定的路径下。

5.1.2 资源控制

应按以下要求设计和实现资源分配能力：

a） 能对应用程序所产生的用户数据所占存储资源进行限制；

b） 能在数据的存储空间达到阈值时，向移动智能终端操作系统用户进行告警。

5.1.3 定义数据属性

应支持以默认方式或授权配置方式定义数据属性：

a） 基本属性：生成时间、最后修改时间、最后访问时间等；

b） 安全属性：所有者、读/写权限、数据类别、授权主体及权限、使用范围等；

c） 数据的重要程度。

5.1.4 数据保密性

应采取措施保证移动智能终端上用户数据的保密性：

a） 采用密码技术保证用户数据在本地存储时的保密性；

b） 采用国家密码主管部门认可的密码算法对重要用户数据进行加解密。

5.1.5 数据完整性

对移动智能终端上用户数据的完整性进行保护和监测：

a） 采用校验技术或密码技术保证用户数据存储时的完整性；

b） 对用户数据完整性进行监测，当完整性被破坏时，具有明确的提示；

c） 采用密码技术保证重要用户数据存储时的完整性，并采用国家密码主管部门认可的密码算法；

d） 检测到完整性错误时应对用户数据采取必要的恢复措施。

5.2 数据访问控制

5.2.1 访问控制策略

应提供默认或者可定义的访问控制策略：

a) 访问控制策略应包括授权主体、访问方式（读、写、删除等）、客体等元素；
b) 访问控制策略应覆盖所有的主体、客体以及之间的操作；
c) 采用默认禁止原则的访问控制策略；
d) 遵循最小授权原则，为主体授予业务所必需的最小权限。

5.2.2 主体身份鉴别与识别

对用户数据执行任何操作之前，对主体的身份进行鉴别或识别：
a） 当操作主体为人时，应对其身份进行鉴别；
b） 当操作主体为应用软件等实体时，应对其身份进行识别。

5.2.3 基于安全属性的访问控制

应提供基于安全属性的访问控制，只有访问控制策略所允许的主体才能对用户数据进行相应的操作。

5.3 数据备份与恢复

应对用户数据提供数据备份与恢复功能，数据备份包括复制备份或者转移备份：
a） 支持对用户数据通过移动智能终端的外围接口进行本地备份，或通过无线网络方式进行远程备份；
b） 备份数据应保留原数据的基本属性及安全属性；
c） 对备份数据提供保密性及完整性保护；
d） 支持定期或周期性的增量或全量备份策略；
e） 保证备份数据的可用性，并在恢复时对数据的完整性进行检测。

5.4 数据销毁

5.4.1 数据清除

当移动智能终端进行恢复出厂设置、卸载应用程序或其他情况下需要清除用户数据时，应明确的告知用户。

5.4.2 数据自毁

在一定条件下（如连续鉴别失败、接收到相应指令等），自动清除用户数据。

5.4.3 残余信息保护

应确保非授权主体不能获取其他主体使用后返还系统的存储资源中的信息内容。

5.5 安全审计

为用户数据提供防护的实体（如操作系统、应用软件）应对用户数据的访问等提供安全审计功能：
a） 审计事件类型至少应包括：数据的属性定义操作、数据的授权操作、数据的访问行为（包括成功及失败）、数据的备份及恢复、数据销毁；
b） 审计事件内容至少包括：事件发生的日期时间、主体身份、操作类型、事件结果（成功或失败）；
c） 对具有潜在风险的行为进行告警，如存储空间即将耗尽、完整性校验失败、非授权的访问尝试等。

6 测试评价方法

6.1 数据存储

6.1.1 存储介质

存储介质的测试方法与预期结果如下：

a） 测试方法：

1） 通过操作系统及应用软件生成或导入用户数据；

2） 断电关闭移动智能终端，再开启移动智能终端，检查数据是否丢失；

3） 通过登录移动智能终端操作系统，检查数据存储路径。

b） 预期结果：

1） 操作系统或应用软件所产生或导入的用户数据，移动智能终端断电重启后，数据未丢失；

2） 用户数据存储在默认或设定的路径下。

6.1.2 资源控制

资源分配的测试方法与预期结果如下：

a） 测试方法：

1） 通过移动智能终端设置对某类型数据所占存储空间进行限制；

2） 尝试增加该类数据，直至超出设定限额；

3） 检查存储数据超过限值时，是否能够进行告警，并且不超过设定空间限值。

b） 预期结果：

1） 能够限制应用程序所占的存储空间限额；

2） 当应用程序存储空间，以及移动智能终端存储空间达到限值时，应产生告警。

6.1.3 定义数据属性

定义数据属性的测试方法与预期结果如下：

a） 测试方法：

1） 获取移动智能终端特权账户，并以该账户登录移动智能终端操作系统，查看用户数据属性；

2） 尝试对数据的安全属性等进行修改。

b） 预期结果：

1） 数据属性至少包括基本属性及安全属性的各项要求；

2） 授权用户应能对安全属性进行修改。

6.1.4 数据保密性

数据保密性的测试方法与预期结果如下：

a) 测试方法：

1） 在移动智能终端上新增相应的用户数据；

2） 通过二进制读取工具查看存储器上的数据，检查其是否为明文；

3） 开发者应提供文档说明，所采取的密码算法类型。

b) 预期结果：

1） 所读取的内容应为非明文；

2） 所采用的密码算法类型为国家密码主管部门认可的。

6.1.5 数据完整性

数据完整性的测试方法与预期结果如下：

a) 测试方法：
   1） 对存储的数据通过其他途径（如将存储卡接入计算机等）对其进行篡改后，再插入移动智能终端；
   2） 从移动智能终端访问被篡改的数据，检查是否有完整性被破坏的提示；
   3） 尝试对完整性被破坏的用户数据进行恢复；
   4） 开发者应提供文档说明，所采取的密码算法类型。
b) 预期结果：
   1） 用户数据完整性被破坏时，在适当的时机以明确的方式告知用户；
   2） 能够对完整性被破坏的用户数据进行恢复；
   3） 所采用的密码算法类型为国家密码主管部门认可的。

6.2 数据访问控制

6.2.1 访问控制策略

访问控制策略的测试方法与预期结果如下：

a） 测试方法：
   1） 检查访问控制策略配置，是否覆盖了主体、客体及其之间的操作类型；
   2） 尝试不同的主体与客体之间的访问操作，检查默认策略是否完全覆盖；
   3） 新安装各类应用软件，在默认的访问控制策略下，检查该软件是否可以访问其他数据，或者其他应用软件是否能够访问该应用软件的数据；
   4） 检查访问控制策略是否采用或者支持最小授权原则对主体进行授权。
b） 预期结果：
   1） 访问控制策略覆盖所有的主体、客体及其之间的各项操作；
   2） 采用默认禁止原则的访问控制策略；
   3） 问控制策略应采用或者支持最小授权原则对主体进行授权。

6.2.2 主体身份鉴别与识别

主体身份鉴别与识别的测试方法与预期结果如下：

a） 测试方法：
   1） 尝试以用户身份访问数据，检查是否需要对其进行身份鉴别；
   2） 设置各应用软件之间的访问策略，检查授权的应用软件是否能够访问，而其他应用软件无法访问。
b） 预期结果：
   1） 用户访问数据时，需通过身份鉴别；
   2） 能够对授权的应用软件进行身份识别。

6.2.3 基于安全属性的访问控制

数据访问控制的测试方法与预期结果如下：

a） 测试方法：
   1） 检查系统是否具有根据主体、数据安全属性的访问控制策略；
   2） 分别以不同的主体身份尝试访问具有不同安全属性的用户数据。
b） 预期结果：

1) 操作系统或应用程序具有或可设置根据主体、数据安全属性的访问控制策略；操作系统或应用程序具备或可根据主体、数据安全属性设置访问控制策略；
2) 只有安全策略允许的主体才能访问相应的用户数据。

6.3 数据备份与恢复

数据备份与恢复的测试方法与预期结果如下：

a) 测试方法：
1) 分别通过移动智能终端的外围接口，如USB数据线接口、存储卡接口等，或无线网络，如移动通信网络、Wifi网络等方式对数据进行备份；
2) 备份完成后，通过二进制读取工具查看备份文件；
3) 删除移动智能终端上用户数据后，尝试对数据进行恢复，并检查恢复后数据的访问权限；
4) 对备份文件内容进行一定的篡改，再次尝试对数据进行恢复；
5) 分别设置不同的备份策略，检查是否按照设定的策略进行备份。

b) 预期结果：
1) 能够支持本地备份或者远程备份；
2) 备份文件以加密方式存储；
3) 支持对备份数据进行恢复，恢复后数据属性保持备份前状态；
4) 备份文件完整性被破坏后，在恢复时能进行相应的提示；
5) 能够支持各种备份策略，并能安装设定的策略进行备份。

6.4 数据销毁

6.4.1 数据清除

数据清除的测试方法与预期结果如下：

a) 测试方法：
1) 尝试对移动智能终端进行恢复出厂设置，检查是否会明确告知用户，将清除用户数据；
2) 尝试卸载带有用户数据的应用程序，检查是否明确告知用户，是否需清除用户数据，选择确定清除数据时，检查是否能够删除由其生成的数据和信息。

b) 预期结果：当需清除用户数据时，应明确告知用户。

6.4.2 数据自毁

数据自毁的测试方法与预期结果如下：

a) 测试方法：
1) 检查移动智能终端是否具备用户数据自毁功能；
2) 设置数据自毁的条件，如鉴别失败次数、长时间未成功连接后台、通过后台设置指令等；
3) 触发数据自毁条件，通过工具读取存储器的数据，检查数据是否已经清除。

b) 预期结果：
1) 移动智能终端具有用户数据自毁功能；
2) 数据自毁具有严格的触发条件。

6.4.3 残余信息保护

残余信息保护的测试方法与预期结果如下：

a) 测试方法：

1） 通过主动删除、数据自毁等方式清除用户数据；
2） 通过数据恢复工具尝试恢复存储器的已删除的数据，检查数据是否已经清除。

b） 预期结果：主动删除及数据自毁等方式清除的用户数据，通过数据恢复工具无法恢复获取。

6.5 安全审计

安全审计的测试方法与预期结果如下：

a） 测试方法：
1） 分别尝试定义数据属性、对数据进行授权操作、授权及非授权的数据访问、数据备份及恢复、数据删除销毁、破坏数据完整性等操作；
2） 检查是否具有相应的审计记录以及审计记录内容正确性。

b） 预期结果：
1） 能够对针对用户数据的各主要操作行为进行审计；
2） 审计内容包括了事件发生的日期时间、主体身份、操作类型、事件结果（成功或失败）；
3） 对具有潜在风险的行为能够及时告警。

7 不同安全等级的要求

不同安全等级的移动智能终端用户数据存储安全技术要求如表1所示。

表1 不同安全等级的移动智能终端用户数据存储安全技术要求

安全技术要求		基本级	增强级
数据存储	存储介质	5.1.1	5.1.1
	资源控制	——	5.1.2
	定义数据属性	5.1.3 a）、b）	5.1.3
	数据保密性	5.1.4 a）	5.1.4
	数据完整性	5.1.5 a）、b）	5.1.5
数据访问控制	访问控制策略	5.2.1 a）～c）	5.2.1
	主体身份鉴别与识别	5.2.2	5.2.2
数据访问控制	基于安全属性的访问控制	5.2.3	5.2.3
数据备份与恢复		5.3 a）～c）	5.3
数据销毁	数据清除	5.4.1	5.4.1
	数据自毁	——	5.4.2
	残余信息保护	——	5.4.3
安全审计		5.5 a）、b）	5.5