

ICS 33.060

M 36

YD

中华人民共和国通信行业标准

YD/T 2408-2013

移动智能终端安全能力测试方法

Test methods for security capability of smart mobile terminal

2013-04-25 发布

2013-11-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
引 言	III
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 移动智能终端安全能力测试方法	2
4.1 概述	2
4.2 移动智能终端硬件安全能力	2
4.3 移动智能终端操作系统安全能力	3
4.4 移动智能终端外围接口安全能力	19
4.5 移动智能终端应用层安全	24
4.6 移动智能终端用户数据安全保护能力	29
5 移动智能终端功能限制性要求测试方法	34
参考文献	36

前 言

本标准按照 GB/T 1.1-2009给出的规则编写。

本标准移动智能终端安全系列标准之一，该系列标准的名称和结构预计如下：

- a) 《移动智能终端安全能力设计导则》；
- b) YD/T 2407-2013《移动智能终端安全能力技术要求》；
- c) YD/T 2408-2013《移动智能终端安全能力测试方法》；
- d) YD/T 1886-2009《移动终端芯片安全技术要求和测试方法》。

本标准在使用时与《移动智能终端安全能力技术要求》配套使用。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、北京展讯高科通信技术有限公司、大唐电信科技产业集团。

本标准主要起草人：潘 娟、匡晓烜、落红卫、汪 坤、李云帆、于 璐、袁广翔、何桂立、史德年、李 巍、虞华伟、李健巍、李 茜。

引 言

随着移动智能终端的广泛应用以及功能的不断扩展，其使用过程中的安全问题被越来越多的用户所关注。近年来，恶意吸费、窃听、窃录、位置信息泄露等安全事件频发，使用户对移动智能终端的安全性产生顾虑，进而影响到移动智能终端和移动互联网应用的发展。本标准的制定，旨在通过提高移动智能终端的自身的安全防护能力，防范移动智能终端上的各种安全威胁，避免用户的利益受到损害，同时防止移动智能终端对移动通信网络安全产生不利影响。

本标准是《移动智能终端安全能力技术要求》配套的测试方法。本标准针对技术要求提出的技术指标设计了相应的、科学的测试方法，用于验证移动智能终端是否满足技术要求规定的内容。本标准可用于对移动智能终端安全能力的管理。通过本标准可从测试方法角度保证移动智能终端安全能力要求的落地实施，切实地提高移动智能终端的安全能力。

移动智能终端安全能力测试方法

1 范围

本标准规定了移动智能终端安全能力的测试方法，包括移动智能终端硬件安全能力测试方法、移动智能终端操作系统安全能力测试方法、移动智能终端外围接口安全能力测试方法、移动智能终端应用层安全能力测试方法、移动智能终端用户数据保护安全能力测试方法等。

本标准适用于各种制式的移动智能终端，个别条款不适用于特殊行业、专业应用。其他终端参考使用。

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。

YD/T 1886 移动终端芯片安全技术要求和测试方法

YD/T 2407-2013 移动智能终端安全能力技术要求

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

移动智能终端 Smart Mobile Terminal

具有接入移动通信网能力，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

安全能力 Security Capability

在移动智能终端上可实现的，能够防范安全威胁的技术手段。

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

用户数据 User Data

移动智能终端上存储的用户个人信息，包括由用户在本地生成的数据、为用户在本地生成的数据、在用户许可后由外部进入用户数据区的数据等。

3.1.5

授权 Authorization

在用户身份经过认证后，根据预先设置的安全策略，授予用户相应权限的过程。

3.1.6

数字签名 Digital Signature

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者验证数据的来源和完整性，保护数据不被篡改、伪造，并保证数据的不可否认性。

3.1.7

代码签名 Code Signature

利用数字签名机制，由具有签名权限的实体对代码全部或部分功能进行签名的机制。

3.1.8

移动智能终端操作系统 Operator System of Smart Mobile Terminal

移动智能终端最基本的系统软件，它控制和管理移动智能终端各种硬件和软件资源，并提供应用程序开发的接口。

3.2 缩略语

下列缩略语适用于本文件。

CRL	Certificate Revocation List	证书撤销列表
LAWMO	Lock and Wipe Management Object	锁定/擦除管理对象
OCSP	Online Certificate Status Protocol	在线证书状态协议
WLAN	Wireless Local Area Network	无线局域网

4 移动智能终端安全能力测试方法

4.1 概述

本章描述了针对移动智能终端的各种安全能力进行评测的方法。评测结果有以下两种：

- 未见异常：通过评测方法没有发现存在安全风险或安全事件；
- 不符合要求：直接发现安全事件或不符合安全能力要求。

本章中所提及的确认见 YD/T2407-2013《移动智能终端安全能力技术要求》中的要求。

4.2 移动智能终端硬件安全能力

待定。

4.3 移动智能终端操作系统安全能力

4.3.1 安全调用控制能力

4.3.1.1 通信类功能受控机制

4.3.1.1.1 拨打电话受控机制

测试编号: 4.3.1.1.1
测试项目: 拨打电话的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.1.1 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供拨打电话的开发功能; 步骤2: 如果移动智能终端操作系统提供拨打电话的开发功能, 使用该功能开发拨打电话应用程序; 步骤3: 运行该应用程序, 查看终端是否要求用户确认拨打电话
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供拨打电话的开发功能, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端要求用户确认, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端不要求用户确认, 并成功拨打电话, 则该项目评测结果为“不符合要求”, 评测结束

4.3.1.1.2 三方通话受控机制

测试编号: 4.3.1.1.2
测试项目: 三方通话的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.1.2 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供三方通话的开发功能; 步骤2: 如果移动智能终端操作系统提供三方通话的开发功能, 使用该功能开发三方通话应用程序; 步骤3: 运行该应用程序, 查看终端是否要求用户确认三方通话
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供三方通话的开发功能, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端要求用户确认, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端不要求用户确认, 并成功开启三方通话, 则该项目评测结果为“不符合要求”, 评测结束

4.3.1.1.3 发送短信受控机制

测试编号: 4.3.1.1.3
测试项目: 发送短信的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.1.3 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供发送短信的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供发送短信的开发功能, 使用该功能开发发送短信应用程序;</p> <p>步骤3: 运行该应用程序, 查看终端是否要求用户确认发送短信</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供发送短信的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端要求用户确认, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端不要求用户确认, 并成功发送短信, 则该项目评测结果为“不符合要求”, 评测结束</p>

4.3.1.1.4 发送彩信受控机制

测试编号: 4.3.1.1.4
测试项目: 发送彩信的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.1.4 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供发送彩信的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供发送彩信的开发功能, 使用该功能开发发送彩信应用程序;</p> <p>步骤3: 运行该应用程序, 查看终端是否要求用户确认发送彩信</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供发送彩信的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端要求用户确认, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端不要求用户确认, 并成功发送彩信, 则该项目评测结果为“不符合要求”, 评测结束</p>

4.3.1.1.5 发送邮件受控机制

测试编号: 4.3.1.1.5
测试项目: 发送邮件的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.1.5 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供发送邮件的开发功能; 步骤2: 如果移动智能终端操作系统提供发送邮件的开发功能, 使用该功能开发发送邮件应用程序; 步骤3: 运行该应用程序, 查看终端是否要求用户确认发送邮件
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供发送邮件的开发功能, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端要求用户确认, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端不要求用户确认, 并成功发送邮件, 则该项目评测结果为“不符合要求”, 评测结束

4.3.1.1.6 移动通信网络数据连接受控机制

测试编号: 4.3.1.1.6.1
测试项目: 移动通信网络数据连接开启/关闭的开关
项目要求: 见 YD/T2407-2013 第 5.3.1.1.6 节
预置条件: 被测移动智能终端移动通信网络数据连接处于关闭状态
测试步骤: 步骤1: 检查被测移动智能终端是否提供移动通信网络数据连接开启/关闭的开关; 步骤2: 如果移动智能终端提供开关, 则使用该开关开启移动通信网络数据连接; 步骤3: 使用开关关闭移动通信网络数据连接
预期结果: 在步骤1, 在移动智能终端上应能找到开启/关闭移动通信网络数据连接的开关; 在步骤2后, 被测移动智能终端的移动通信网络数据连接成功开启; 在步骤3后, 被测移动智能终端的移动通信网络数据连接成功关闭。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 4.3.1.1.6.2
测试项目: 移动通信网络数据连接开启/关闭的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.1.6 节
预置条件: 被测移动智能终端移动通信网络数据连接处于关闭状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供移动通信网络数据连接开启/关闭的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供移动通信网络数据连接开启/关闭的开发功能, 使用该功能开发移动通信网络数据连接开启/关闭的应用程序;</p> <p>步骤3: 运行应用程序开启移动通信网络数据连接, 查看终端是否要求用户确认移动通信网络数据连接的开启</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供移动通信网络数据连接开启的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端要求用户确认移动通信网络数据连接的开启, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端不要求用户确认, 并成功开启移动通信网络数据连接, 则该项目评测结果为“不符合要求”, 评测结束</p>

测试编号: 4.3.1.1.6.3
测试项目: 移动通信网络数据连接状态提示
项目要求: 见 YD/T2407-2013 第 5.3.1.1.6 节
预置条件: 被测移动智能终端移动通信网络连接处于关闭状态
<p>测试步骤:</p> <p>步骤1: 通过移动智能终端操作系统上的开关打开移动通信网络数据连接;</p> <p>步骤2: 通过移动智能终端操作系统上的开关关闭移动通信网络数据连接;</p> <p>步骤3: 如果移动智能终端操作系统提供移动通信网络数据连接开启的开发功能, 则运行4.3.1.1.6.2中开发的移动通信网络数据连接开启的应用程序;</p> <p>步骤4: 运行移动通信网络数据连接关闭的应用程序</p>
<p>预期结果:</p> <p>在步骤1前, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据连接关闭的状态提示;</p> <p>在步骤1后, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据连接开启的状态提示;</p> <p>在步骤2后, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据连接关闭的状态提示;</p> <p>在步骤3后, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据连接开启的状态提示;</p> <p>在步骤4后, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据连接关闭的状态提示。</p> <p>移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”</p>

测试编号: 4.3.1.1.6.4
测试项目: 移动通信网络数据传送状态提示
项目要求: 见 YD/T2407-2013 第 5.3.1.1.6 节
预置条件: 被测移动智能终端移动通信网络连接处于开启状态
测试步骤: 步骤1: 运行移动智能终端上预置的应用软件通过移动通信网络进行数据传送; 步骤2: 关闭所运行软件; 步骤3: 运行第三方应用软件通过移动通信网络进行数据传送
预期结果: 在步骤1前, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据连接开启的状态提示; 在步骤1后, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据传送的状态提示; 在步骤2后, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据连接开启的状态提示; 在步骤3后, 移动智能终端应在用户主界面上给用户呈现移动通信网络数据传送的状态提示。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.3.1.1.7 WLAN 网络连接受控机制

测试编号: 4.3.1.1.7.1
测试项目: WLAN 网络连接开启/关闭的开关
项目要求: 见 YD/T2407-2013 第 5.3.1.1.7 节
预置条件: 被测移动智能终端 WLAN 网络连接处于关闭状态
测试步骤: 步骤1: 检查被测移动智能终端是否提供WLAN网络连接开启/关闭的开关; 步骤2: 如果移动智能终端提供开关, 则使用该开关开启WLAN网络连接; 步骤3: 使用开关关闭WLAN网络连接
预期结果: 在步骤1, 在移动智能终端上应能找到开启/关闭WLAN网络连接的开关; 在步骤2后, 被测移动智能终端的WLAN网络连接成功开启; 在步骤3后, 被测移动智能终端的WLAN网络连接成功关闭。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 4.3.1.1.7.2
测试项目: WLAN 网络连接开启/关闭的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.1.7 节
预置条件: 被测移动智能终端 WLAN 网络连接处于关闭状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供WLAN网络连接开启/关闭的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供WLAN网络连接开启/关闭的开发功能, 使用该功能开发WLAN网络连接开启、关闭的应用程序;</p> <p>步骤3: 运行应用程序开启WLAN网络连接, 查看终端是否要求用户确认WLAN网络连接的开启</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供WLAN网络连接开启的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端要求用户确认WLAN网络连接的开启, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端不要求用户确认, 并成功开启WLAN网络连接, 则该项目评测结果为“不符合要求”, 评测结束</p>

测试编号: 4.3.1.1.7.3
测试项目: WLAN 网络连接状态提示
项目要求: 见 YD/T2407-2013 第 5.3.1.1.7 节
预置条件: 被测移动智能终端 WLAN 网络连接处于关闭状态
<p>测试步骤:</p> <p>步骤1: 通过移动智能终端操作系统上的开关打开WLAN网络连接;</p> <p>步骤2: 通过移动智能终端操作系统上的开关关闭WLAN网络连接;</p> <p>步骤3: 如果移动智能终端操作系统提供WLAN网络连接开启的开发功能, 则运行4.3.1.1.6.2中开发的WLAN网络连接开启的应用程序;</p> <p>步骤4: 运行WLAN网络连接关闭的应用程序</p>
<p>预期结果:</p> <p>在步骤1前, 移动智能终端应在用户主界面上给用户呈现WLAN网络连接关闭的状态提示;</p> <p>在步骤1后, 移动智能终端应在用户主界面上给用户呈现WLAN网络连接开启的状态提示;</p> <p>在步骤2后, 移动智能终端应在用户主界面上给用户呈现WLAN网络连接关闭的状态提示;</p> <p>在步骤3后, 移动智能终端应在用户主界面上给用户呈现WLAN网络连接开启的状态提示;</p> <p>在步骤4后, 移动智能终端应在用户主界面上给用户呈现WLAN网络连接关闭的状态提示。</p> <p>移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”</p>

测试编号: 4.3.1.1.7.4
测试项目: WLAN 网络数据传送状态提示
项目要求: 见 YD/T2407-2013 第 5.3.1.1.7 节
预置条件: 被测移动智能终端 WLAN 网络连接处于开启状态
测试步骤: 步骤1: 运行移动智能终端上预置的应用软件通过WLAN网络进行数据传送; 步骤2: 关闭所运行软件; 步骤3: 运行第三方应用软件通过WLAN网络进行数据传送
预期结果: 在步骤1前, 移动智能终端应在用户主界面上给用户呈现WLAN网络数据连接开启的状态提示; 在步骤1后, 移动智能终端应在用户主界面上给用户呈现WLAN网络数据传送的状态提示; 在步骤2后, 移动智能终端应在用户主界面上给用户呈现WLAN网络数据连接开启的状态提示; 在步骤3后, 移动智能终端应在用户主界面上给用户呈现WLAN网络数据传送的状态提示。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.3.1.2 本地敏感功能受控机制

4.3.1.2.1 定位功能受控机制

测试编号: 4.3.1.2.1
测试项目: 调用定位功能的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.1 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供调用定位功能的开发功能; 步骤2: 如果移动智能终端操作系统提供调用定位功能的开发功能, 使用该功能开发调用定位功能的应用程序; 步骤3: 运行应用程序调用定位功能, 查看终端是否要求用户确认
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供调用定位功能的开发功能, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端要求用户确认对定位功能的调用, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端不要求用户确认, 并成功调用定位功能, 则该项目评测结果为“不符合要求”, 评测结束

测试编号: 4.3.1.2.1.2
测试项目: 定位功能的状态显示
项目要求: 见 YD/T2407-2013 第 5.3.1.2.1 节
前置条件: 被测移动智能终端定位功能处于开启状态
测试步骤: 步骤1: 通过移动智能终端操作系统上的应用软件调用定位功能; 步骤2: 关闭调用定位功能的应用软件
预期结果: 在步骤1前, 在移动智能终端的用户主界面上应没有定位功能被调用的状态提示; 在步骤1后, 移动智能终端应在用户主界面上给用户呈现定位功能被调用的状态提示; 在步骤2后, 在移动智能终端的用户主界面上应没有定位功能被调用的状态提示。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.3.1.2.2 通话录音功能受控机制

测试编号: 4.3.1.2.2
测试项目: 通话录音功能启动的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.2 节
前置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供通话录音的开发功能; 步骤2: 如果移动智能终端操作系统提供通话录音的开发功能, 使用该功能开发进行通话录音的应用程序; 步骤3: 在通话中运行应用程序进行通话录音, 查看终端是否要求用户确认开始通话录音
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供通话录音的开发功能, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端要求用户确认开始通话录音, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端不要求用户确认, 并成功进行通话录音, 则该项目评测结果为“不符合要求”, 评测结束

4.3.1.2.3 本地录音功能受控机制

测试编号: 4.3.1.2.3
测试项目: 本地录音功能启动的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.3 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供本地录音的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供本地录音的开发功能, 使用该功能开发进行本地录音的应用程序;</p> <p>步骤3: 运行应用程序调用本地录音功能, 查看终端是否要求用户确认</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供本地录音的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端要求用户确认开始本地录音, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端不要求用户确认, 并成功进行本地录音, 则该项目评测结果为“不符合要求”, 评测结束</p>

4.3.1.2.4 拍照/摄像功能受控机制

测试编号: 4.3.1.2.4
测试项目: 拍照/摄像功能启动的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.4 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供调用摄像头的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供调用摄像头的开发功能, 使用该功能开发调用摄像头的应用程序;</p> <p>步骤3: 运行应用程序调用摄像头操作, 查看终端是否有相应的提示;</p> <p>步骤4: 运行应用程序进行拍照或摄像操作, 查看终端是否要求用户确认</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供调用摄像头的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端给用户相应的提示(图像预览、指示灯、声音或图标等), 则执行步骤4;</p> <p>在步骤4后, 如果移动智能终端要求用户确认拍照或摄像操作, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端没有给用户任何提示, 则该项目评测结果为“不符合要求”, 评测结束</p>

4.3.1.2.5 对用户数据的操作受控机制

测试编号：4.3.1.2.5.1
测试项目：电话本数据写和删除操作的受控机制
项目要求：见 YD/T2407-2013 第 5.3.1.2.5 节
预置条件：被测移动智能终端处于正常工作状态
<p>测试步骤：</p> <p>步骤1：检查被测移动智能终端的操作系统是否提供电话本数据写和删除操作的开发功能；</p> <p>步骤2：如果移动智能终端操作系统提供电话本数据写和删除操作的开发功能，使用该功能开发电话本数据写和删除操作的应用程序；</p> <p>步骤3：运行应用程序写电话本，查看终端是否要求用户确认对电话本的写操作；</p> <p>步骤4：运行应用程序删除电话本，查看终端是否要求用户确认对电话本的删除操作</p>
<p>预期结果：</p> <p>在步骤1后，如果移动智能终端操作系统不提供电话本数据写和删除操作的开发功能，则该项目评测结果为“未见异常”，评测结束；</p> <p>在步骤3后，如果移动智能终端要求用户确认对电话本的写操作，则该项目评测结果为“未见异常”，评测结束；</p> <p>在步骤3后，如果移动智能终端不要求用户确认，并成功执行了电话本的写操作，则该项目评测结果为“不符合要求”，评测结束；</p> <p>在步骤4后，如果移动智能终端要求用户确认对电话本的删除操作，则该项目评测结果为“未见异常”，评测结束；</p> <p>在步骤4后，如果移动智能终端不要求用户确认，并成功执行了电话本的删除操作，则该项目评测结果为“不符合要求”，评测结束</p>

测试编号: 4.3.1.2.5.2
测试项目: 通话记录写和删除操作的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.5 节
前置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供通话记录写和删除操作的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供通话记录写和删除操作的开发功能, 使用该功能开发通话记录写和删除操作的应用程序;</p> <p>步骤3: 运行应用程序写通话记录, 查看终端是否要求用户确认对通话记录的写操作;</p> <p>步骤4: 运行应用程序删除通话记录, 查看终端是否要求用户确认对通话记录的删除操作</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供通话记录写和删除操作的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端要求用户确认对通话记录的写操作, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端不要求用户确认, 并成功执行了通话记录的写操作, 则该项目评测结果为“不符合要求”, 评测结束;</p> <p>在步骤4后, 如果移动智能终端要求用户确认对通话记录的删除操作, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤4后, 如果移动智能终端不要求用户确认, 并成功执行了通话记录的删除操作, 则该项目评测结果为“不符合要求”, 评测结束</p>

测试编号：4.3.1.2.5.3
测试项目：短信数据写和删除操作的受控机制
项目要求：见 YD/T2407-2013 第 5.3.1.2.5 节
前置条件：被测移动智能终端处于正常工作状态
<p>测试步骤：</p> <p>步骤1：检查被测移动智能终端的操作系统是否提供短信数据写和删除操作的开发功能；</p> <p>步骤2：如果移动智能终端操作系统提供短信数据写和删除操作的开发功能，使用该功能开发短信数据写和删除操作的应用程序；</p> <p>步骤3：运行应用程序写短信，查看终端是否要求用户确认对短信的写操作；</p> <p>步骤4：运行应用程序删除短信，查看终端是否要求用户确认对短信的删除操作</p>
<p>预期结果：</p> <p>在步骤1后，如果移动智能终端操作系统不提供短信数据写和删除操作的开发功能，则该项目评测结果为“未见异常”，评测结束；</p> <p>在步骤3后，如果移动智能终端要求用户确认对短信的写操作，则该项目评测结果为“未见异常”，评测结束；</p> <p>在步骤3后，如果移动智能终端不要求用户确认，并成功执行了短信的写操作，则该项目评测结果为“不符合要求”，评测结束；</p> <p>在步骤4后，如果移动智能终端要求用户确认对短信的删除操作，则该项目评测结果为“未见异常”，评测结束；</p> <p>在步骤4后，如果移动智能终端不要求用户确认，并成功执行了短信的删除操作，则该项目评测结果为“不符合要求”，评测结束</p>

测试编号: 4.3.1.2.5.4
测试项目: 彩信数据写和删除操作的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.5 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供彩信数据写和删除操作的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供彩信数据写和删除操作的开发功能, 使用该功能开发彩信数据写和删除操作的应用程序;</p> <p>步骤3: 运行应用程序写彩信, 查看终端是否要求用户确认对彩信的写操作;</p> <p>步骤4: 运行应用程序删除彩信, 查看终端是否要求用户确认对彩信的删除操作</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供彩信数据写和删除操作的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端要求用户确认对彩信的写操作, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端不要求用户确认, 并成功执行了彩信的写操作, 则该项目评测结果为“不符合要求”, 评测结束;</p> <p>在步骤4后, 如果移动智能终端要求用户确认对彩信的删除操作, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤4后, 如果移动智能终端不要求用户确认, 并成功执行了彩信的删除操作, 则该项目评测结果为“不符合要求”, 评测结束</p>

测试编号: 4.3.1.2.5.5
测试项目: 电话本数据读操作的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.5 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供电话本数据读操作的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供电话本数据读操作的开发功能, 使用该功能开发电话本数据读操作的应用程序;</p> <p>步骤3: 安装、运行会读电话本数据的应用程序, 检查在程序安装或首次运行时是否给用户提示</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供电话本数据读操作的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端给用户提示该程序会访问用户电话本数据, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端没有给用户任何提示, 并且程序能够对用户电话本进行读操作, 则该项目评测结果为“不符合要求”, 评测结束</p>

测试编号: 4.3.1.2.5.6
测试项目: 通话记录读操作的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.5 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供通话记录读操作的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供通话记录读操作的开发功能, 使用该功能开发通话记录读操作的应用程序;</p> <p>步骤3: 安装、运行会读通话记录的应用程序, 检查在程序安装或首次运行时是否给用户提示</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供通话记录读操作的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端给用户提示该程序会访问用户通话记录, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端没有给用户任何提示, 并且程序能够对用户通话记录进行读操作, 则该项目评测结果为“不符合要求”, 评测结束</p>

测试编号: 4.3.1.2.5.7
测试项目: 短信数据读操作的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.5 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供短信数据读操作的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供短信数据读操作的开发功能, 使用该功能开发短信数据读操作的应用程序;</p> <p>步骤3: 安装、运行会读短信数据的应用程序, 检查在程序安装或首次运行时是否给用户提示</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供短信数据读操作的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端给用户提示该程序会访问用户短信数据, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端没有给用户任何提示, 并且程序能够对用户短信数据进行读操作, 则该项目评测结果为“不符合要求”, 评测结束</p>

测试编号: 4.3.1.2.5.8
测试项目: 彩信数据读操作的受控机制
项目要求: 见 YD/T2407-2013 第 5.3.1.2.5 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 检查被测移动智能终端的操作系统是否提供彩信数据读操作的开发功能;</p> <p>步骤2: 如果移动智能终端操作系统提供彩信数据读操作的开发功能, 使用该功能开发彩信数据读操作的应用程序;</p> <p>步骤3: 安装、运行会读彩信数据的应用程序, 检查在程序安装或首次运行时是否给用户提示</p>
<p>预期结果:</p> <p>在步骤1后, 如果移动智能终端操作系统不提供彩信数据读操作的开发功能, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端给用户提示该程序会访问用户彩信数据, 则该项目评测结果为“未见异常”, 评测结束;</p> <p>在步骤3后, 如果移动智能终端没有给用户任何提示, 并且程序能够对用户彩信数据进行读操作, 则该项目评测结果为“不符合要求”, 评测结束</p>

4.3.1.3 操作系统的更新

测试编号: 4.3.1.3.1
测试项目: 操作系统的更新——授权更新
项目要求: 见 YD/T2407-2013 第 5.3.2 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供操作系统更新的能力; 步骤2: 如果移动智能终端操作系统提供操作系统授权更新的能力, 则使用授权的操作系统进行系统更新; 步骤3: 再使用未授权的操作系统进行系统更新
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供操作系统更新的能力, 则该项目评测结果为“未见异常”, 评测结束; 在步骤2后, 移动智能终端成功执行操作系统的更新; 在步骤3后, 如果移动智能终端无法正常执行操作系统的更新, 则该项目评测结果为“未见异常”, 如果移动智能终端成功执行操作系统的更新, 则该项目评测结果为“不符合要求”

测试编号: 4.3.1.3.2
测试项目: 操作系统的更新——风险提示
项目要求: 见 YD/T2407-2013 第 5.3.2 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供操作系统更新的能力; 步骤2: 检查被测移动智能终端的操作系统是否可执行安全的操作系统更新; 步骤3: 如果移动智能终端操作系统不能提供安全的操作系统更新, 则检查移动智能终端说明书
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供操作系统更新的能力, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3, 如果移动智能终端说明书中明示用户相应的安全风险, 则该项目评估结果为“未见异常”。如未明示, 则该项目评测结果为“不符合要求”

4.4 移动智能终端外围接口安全能力

4.4.1 无线外围接口安全能力

4.4.1.1 无线外围接口开启/关闭受控机制

测试编号: 4.4.1.1.1
测试项目: 蓝牙接口开启/关闭的开关
项目要求: 见 YD/T2407-2013 第 5.4.1.1 节
预置条件: 被测移动智能终端蓝牙接口处于关闭状态
测试步骤: 步骤1: 检查被测移动智能终端是否提供蓝牙接口开启/关闭的开关; 步骤2: 如果移动智能终端提供开关, 则使用该开关开启蓝牙接口; 步骤3: 使用开关关闭蓝牙接口
预期结果: 在步骤1, 在移动智能终端上应能找到开启/关闭蓝牙接口的开关; 在步骤2后, 被测移动智能终端的蓝牙接口被成功开启; 在步骤3后, 被测移动智能终端的蓝牙接口被成功关闭。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 4.1.1.1.2
测试项目: 蓝牙接口开启的受控机制
项目要求: 见 YD/T2407-2013 第 5.4.1.1 节
预置条件: 被测移动智能终端蓝牙接口处于关闭状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供蓝牙接口开启的开发功能; 步骤2: 如果移动智能终端操作系统提供蓝牙接口开启的开发功能, 使用该功能开发蓝牙接口开启的应用程序; 步骤3: 运行应用程序开启蓝牙接口, 查看终端是否要求用户确认蓝牙接口的开启
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供蓝牙接口开启的开发功能, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端要求用户确认蓝牙接口的开启, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端不要求用户确认, 并成功开启蓝牙接口, 则该项目评测结果为“不符合要求”, 评测结束

测试编号: 4.4.1.1.3
测试项目: NFC 接口开启/关闭的开关
项目要求: 见 YD/T2407-2013 第 5.4.1.1 节
预置条件: 被测移动智能终端 NFC 接口处于关闭状态
测试步骤: 步骤1: 检查被测移动智能终端是否提供NFC接口开启/关闭的开关; 步骤2: 如果移动智能终端提供开关, 则使用该开关开启NFC接口; 步骤3: 使用开关关闭NFC接口
预期结果: 在步骤1, 在移动智能终端上应能找到开启/关闭NFC接口的开关; 在步骤2后, 被测移动智能终端的NFC接口被成功开启; 在步骤3后, 被测移动智能终端的NFC接口被成功关闭。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 4.1.1.1.4
测试项目: NFC 接口开启的受控机制
项目要求: 见 YD/T2407-2013 第 5.4.1.1 节
预置条件: 被测移动智能终端 NFC 接口处于关闭状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供NFC接口开启的开发功能; 步骤2: 如果移动智能终端操作系统提供NFC接口开启的开发功能, 使用该功能开发NFC接口开启的应用程序; 步骤3: 运行应用程序开启NFC接口, 查看终端是否要求用户确认NFC接口的开启
预期结果: 在步骤1后, 如果移动智能终端操作系统不提供NFC接口开启的开发功能, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端要求用户确认NFC接口的开启, 则该项目评测结果为“未见异常”, 评测结束; 在步骤3后, 如果移动智能终端不要求用户确认, 并成功开启NFC接口, 则该项目评测结果为“不符合要求”, 评测结束

4.4.1.2 无线外围接口连接建立的确认机制

测试编号: 4.4.1.2
测试项目: 蓝牙配对连接的受控机制
项目要求: 见 YD/T2407-2013 第 5.4.1.2 节
预置条件: 被测移动智能终端蓝牙接口处于开启状态, 但还未进行配对连接。 评测电脑从未与被测终端进行过蓝牙配对
测试步骤: 步骤1: 将被测智能终端靠近已开启蓝牙接口的评测用电脑; 步骤2: 查看终端是否要求用户确认蓝牙机型配对
预期结果: 在步骤2后, 如果终端未要求用户确认蓝牙机型配对, 并未与评测电脑建立蓝牙配对, 则该项目评测结果为“未见异常”; 在步骤2后, 如果终端要求用户确认蓝牙机型配对, 则该项目评测结果为“未见异常”; 在步骤2后, 如果终端未要求用户确认蓝牙机型配对, 并成功完成蓝牙配对, 则该项目评测结果为“不符合要求”

4.4.1.3 无线外围接口连接状态提示

测试编号: 4.4.1.3.1
测试项目: 蓝牙接口连接状态显示
项目要求: 见 YD/T2407-2013 第 5.4.1.3 节
预置条件: 被测移动智能终端蓝牙接口处于关闭状态
测试步骤: 步骤1: 将被测移动智能终端蓝牙接口打开; 步骤2: 操作被测移动智能终端与另一蓝牙设备建立连接, 并配对成功; 步骤3: 操作被测移动智能终端中断当前蓝牙连接; 步骤4: 将被测移动智能终端蓝牙接口关闭
预期结果: 在步骤1前, 移动智能终端用户主界面上应无蓝牙相关标识; 在步骤2后, 移动智能终端应在用户主界面上给用户呈现蓝牙接口已建立数据连接的状态提示; 在步骤4后, 移动智能终端用户主界面上应无蓝牙相关标识。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 4.4.1.3.2
测试项目: NFC 接口连接提示
项目要求: 见 YD/T2407-2013 第 5.4.1.3 节
预置条件: 被测移动智能终端 NFC 接口处于关闭状态
<p>测试步骤:</p> <p>步骤1: 将被测移动智能终端NFC接口打开;</p> <p>步骤2: 操作被测移动智能终端与另一NFC设备建立数据连接;</p> <p>步骤3: 操作被测移动智能终端中断当前NFC连接;</p> <p>步骤4: 将被测移动智能终端NFC接口关闭。</p>
<p>预期结果:</p> <p>在步骤1前, 移动智能终端用户主界面上应无NFC相关标识;</p> <p>在步骤2后, 移动智能终端应给用户相应的提示(图标、声音或振动等), 提示NFC接口已建立数据连接;</p> <p>在步骤4后, 移动智能终端用户主界面上应无NFC相关标识。</p> <p>移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”</p>

4.4.1.4 无线外围接口数据传输的受控机制

测试编号: 4.4.1.4.1
测试项目: 蓝牙接口数据传输受控机制
项目要求: 见 YD/T2407-2013 第 5.4.1.4 节
预置条件: 被测移动智能终端蓝牙接口处于开启状态, 移动智能终端与测试 PC 配对成功
<p>测试步骤:</p> <p>步骤1: 采取终端所提供的文件传输方式, 从被测移动智能终端向测试PC发送数据;</p> <p>步骤2: 采取终端所提供的文件传输方式, 从测试PC向被测终端发送数据</p>
<p>预期结果:</p> <p>在步骤1后, 移动智能终端向用户提示, 文件开始传送;</p> <p>在步骤2后, 移动智能终端向用户提示, 文件开始传送。</p> <p>移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”</p>

测试编号: 4.4.1.4.2
测试项目: NFC 接口数据传输受控机制
项目要求: 见 YD/T2407-2013 第 5.4.1.4 节
预置条件: 被测移动智能终端 NFC 接口处于开启状态, 移动智能终端与测试 PC 已建立数据连接
测试步骤: 步骤1: 采取终端所提供的文件传输方式, 从被测移动智能终端向测试PC发送数据; 步骤2: 采取终端所提供的文件传输方式, 从测试PC向被测终端发送数据
预期结果: 在步骤1后, 移动智能终端向用户提示, 文件开始传送; 在步骤2后, 移动智能终端向用户提示, 文件开始传送。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.4.2 有线外围接口安全能力

4.4.2.1 有线外围接口连接建立的确认机制

测试编号: 4.4.2.1
测试项目: 有线外围接口连接建立的确认机制
项目要求: 见 YD/T2407-2013 第 5.4.2.1 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查移动智能终端的有线外围接口个数; 步骤2: 对每一个有线外围接口执行以下测试; 步骤3: 确认该有线外围接口的用途: 仅用于充电、仅用于数据连接、既可充电又可进行数据连接 步骤4: 如果该有线外围接口仅用于充电, 将其连接至测试PC检查其提示和状态; 步骤5: 如果该有线外围接口仅用于数据连接, 将其连接至测试PC检查其提示和状态; 步骤6: 如果该有线外围接口既可用于充电又可进行数据连接, 将其连接至测试PC, 检查其提示和状态; 步骤7: 选择充电模式; 步骤8: 选择数据连接模式
预期结果: 在步骤4后, 移动智能终端应给用户提示: 正在充电; 在步骤5后, 移动智能终端应给用户提示: 已建立数据连接; 在步骤6后, 用户可以选择“充电模式”或“数据连接模式”或者移动智能终端提供对于用户数据的授权访问; 在步骤7, 当用户选择充电模式或者移动智能终端没有授权对用户数据的访问, 移动智能终端进入充电状态, 其数据不可被访问; 在步骤8, 当用户选择数据连接模式或提供授权访问后, 移动智能终端进入数据连接状态, 其数据可被访问。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.4.2.2 U 盘模式的安全机制

测试编号: 4.4.2.2
测试项目: U 盘模式的安全机制
项目要求: 见 YD/T2407-2013 第 5.4.2.2 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 针对支持内置式USB存储模式的移动智能终端, 在终端处于锁屏状态下将移动智能终端采用USB模式连接到测试PC; 步骤2: 在测试PC侧以U盘模式访问移动智能终端中数据
预期结果: 在步骤2后, 移动智能终端应采取访问控制策略, 仅当用户提供正确的访问控制要求后, 才可访问到移动智能终端中的数据。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.5 移动智能终端应用层安全

4.5.1 应用软件安全配置能力

测试编号: 4.5.1
测试项目: 应用软件安全配置能力
项目要求: 见 YD/T2407-2013 第 5.5.1 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端的操作系统是否提供拨打电话、发起三方通话、发送短信、发送彩信、调用移动通信网络数据连接、调用定位功能、进行通话录音、本地录音、拍照/摄像、访问电话本、访问通话记录、访问短信和访问彩信的开发功能; 步骤2: 对于提供开发功能的调用, 开发相应的应用程序; 步骤3: 运行该应用程序, 检查对应的调用是否具有可配置能力; 步骤4: 禁用所有的调用, 再次运行, 检查应用程序实际运行的状态; 步骤5: 逐个打开每一个调用, 并运行, 检查应用程序实际运行的状态
预期结果: 在步骤3后, 如果可以找到应用程序安全配置菜单, 菜单中包含具有开发功能的调用的配置选项, 配置至少包含“允许调用”和“禁止调用”两个选项, 则继续执行步骤4; 否则, 该项目评测结果为“不符合要求”, 评测结束; 在步骤4后, 如果应用程序无法调用所有的功能, 则继续执行步骤5; 如果应用程序可以调用某些功能, 则该项目评测结果为“不符合要求”, 评测结束; 在步骤5后, 如果每打开一个调用, 应用程序仅可调用被允许的调用, 无法执行其他调用, 则该项目评测结果为“未见异常”, 否则该项目评测结果为“不符合要求”, 评测结束

4.5.2 应用软件安全认证机制

4.5.2.1 非认证签名

测试编号: 4.5.2.1
测试项目: 非认证签名
项目要求: 见 YD/T2407-2013 第 5.5.2.1 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端是否提供应用软件非认证签名机制; 步骤2: 对于提供了应用软件非认证签名机制的移动智能终端, 开发一款无认证签名的应用程序; 步骤3: 检查被测移动智能终端在上述应用程序安装过程中, 是否提示该应用程序的签名状态
预期结果: 在步骤1后, 如果检查到被测移动智能终端提供了应用软件非认证签名机制, 则继续执行步骤2; 在步骤3后, 如果被测移动智能终端在无认证签名的应用程序安装过程中, 提示该应用程序的签名状态, 则该项目评测结果为“未见异常”, 否则该项目的评测结果为“不符合要求”

4.5.2.2 认证签名

测试编号: 4.5.2.2
测试项目: 认证签名——应用程序安装
项目要求: 见 YD/T2407-2013 第 5.5.2.2 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 检查被测移动智能终端是否提供应用软件认证签名机制; 步骤2: 对于提供了应用软件认证签名机制的移动智能终端, 检查移动智能终端是否支持OCSP或CRL协议在线检查代码签名证书的有效性; 步骤3: 开发一款应用程序, 该程序具有认证的代码签名, 签名没有被篡改过, 且其签名证书处于有效期内; 将该应用程序安装到被测智能终端上; 步骤4: 开发一款应用程序, 该程序具有认证的代码签名, 签名证书处于有效期内, 但其签名被篡改过; 将该应用程序安装到被测智能终端上; 步骤5: 开发一款应用程序, 该程序具有认证的代码签名, 签名没有被篡改过, 但其签名证书被吊销; 将该应用程序安装到被测智能终端上; 步骤6: 开发一款应用程序, 该程序不具有认证的代码签名。将该应用程序安装到被测智能终端上
预期结果: 在步骤1后, 如果检查到被测移动智能终端提供了应用软件认证签名机制, 则继续执行步骤2; 在步骤2中, 如果被测移动智能终端支持OCSP或CRL协议在线检查代码签名证书的有效性, 则继续执行步骤3; 否则, 该项目评测结果为“不符合要求”, 评测结束; 在步骤3中, 应用程序应能够成功安装到被测智能终端上; 在步骤4、5、6中, 如果被测移动智能终端禁止应用程序安装或提示用户安装的风险, 则该项目评估结果为“未见异常”, 否则该项目的评估结果为“不符合要求”

4.5.3 开机自启动程序监控能力

测试编号：4.5.3
测试项目：开机自启动程序监控能力
项目要求：见 YD/T2407-2013 第 5.5.3 节
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤1：查看移动智能终端开机自启动程序； 步骤2：安装一个会开机自启动的应用程序，查看其是否被标识为开机自启动程序； 步骤3：将步骤2中增加的应用程序配置为不能够开机自启动； 步骤4：重启移动智能终端，在移动智能终端进入正常工作状态后检查步骤3中配置为不能开机自启动的应用程序是否在运行
预期结果： 在步骤1后，记录会开机自启动的程序； 在步骤2后，检查被安装的应用程序是否被配置为开机自启动； 在步骤3后，应可成功配置应用程序为不能够开机自启动； 在步骤4后，移动智能终端应没有运行已配置为不能开机自启动的应用程序。 移动智能终端满足以上预期结果，则该项目评测结果为“未见异常”，反之该项目评测结果为“不符合要求”

4.5.4 预置应用软件安全

4.5.4.1 收集用户数据

测试编号：4.5.4.1
测试项目：预置应用软件收集用户数据行为
项目要求：见 YD/T2407-2013 第 5.5.4.1 节
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤1：使预置应用软件信息安全测试系统（包括服务器和客户端软件）处于正常工作状态； 步骤2：将预置应用软件信息安全测试系统客户端软件安装到被测移动智能终端上，并与服务器建立连接； 步骤3：使用基于特征码扫描、静态源代码分析、动态行为监测等检测方法，对被测移动智能终端预置应用软件未向用户明示并经用户同意，擅自收集用户数据的行为（包括在用户无确认情况下开启通话录音、本地录音、拍照/摄像和定位的行为）进行检测
预期结果： 如果预置应用软件信息安全测试系统显示被测移动智能终端预置应用软件无擅自收集用户数据的行为，则该项目评测结果为“未见异常”；否则，该项目评测结果为“不符合要求”

4.5.4.2 修改用户数据

测试编号: 4.5.4.2
测试项目: 预置应用软件修改用户数据行为
项目要求: 见 YD/T2407-2013 第 5.5.4.2 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 使预置应用软件信息安全测试系统(包括服务器和客户端软件)处于正常工作状态;</p> <p>步骤2: 将预置应用软件信息安全测试系统客户端软件安装到被测移动智能终端上, 并与服务器建立连接;</p> <p>步骤3: 使用基于特征码扫描、静态源代码分析、动态行为监测等检测方法, 对被测移动智能终端预置应用软件未向用户明示并经用户同意, 擅自修改用户数据的行为(包括在用户无确认情况下删除或修改用户电话本数据、通话记录、短信数据和彩信数据的行为)进行检测</p>
<p>预期结果:</p> <p>如果预置应用软件信息安全测试系统显示被测移动智能终端预置应用软件无擅自修改用户数据的行为, 则该项目评测结果为“未见异常”; 否则, 该项目评测结果为“不符合要求”</p>

4.5.4.3 调用终端通信功能

4.5.4.3.1 流量耗费

测试编号: 4.5.4.3.1
测试项目: 预置应用软件流量耗费行为
项目要求: 见 YD/T2407-2013 第 5.5.4.3.1 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 使预置应用软件信息安全测试系统(包括服务器和客户端软件)处于正常工作状态;</p> <p>步骤2: 将预置应用软件信息安全测试系统客户端软件安装到被测移动智能终端上, 并与服务器建立连接;</p> <p>步骤3: 使用基于特征码扫描、静态源代码分析和动态行为监测等检测方法, 对被测移动智能终端预置应用软件未向用户明示并经用户同意, 擅自调用终端通信功能, 造成用户流量消耗的行为(包括在用户无确认情况下通过移动通信网络数据连接、WLAN网络连接和无线外围接口传送数据的行为)进行检测</p>
<p>预期结果:</p> <p>如果预置应用软件信息安全测试系统显示被测移动智能终端预置应用软件无擅自调用终端通信功能, 造成用户流量消耗的行为, 则该项目评测结果为“未见异常”; 否则, 该项目评测结果为“不符合要求”</p>

4.5.4.3.2 费用损失

测试编号: 4.5.4.3.2
测试项目: 预置应用软件费用损失行为
项目要求: 见 YD/T2407-2013 第 5.5.4.3.2 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 使预置应用软件信息安全测试系统(包括服务器和客户端软件)处于正常工作状态;</p> <p>步骤2: 将预置应用软件信息安全测试系统客户端软件安装到被测移动智能终端上, 并与服务器建立连接;</p> <p>步骤3: 使用基于特征码扫描、静态源代码分析和动态行为监测等检测方法, 对被测移动智能终端预置应用软件未向用户明示并经用户同意, 擅自调用终端通信功能, 造成用户费用损失的行为(包括在用户无确认情况下拨打电话、发送短信、发送彩信和开启移动通信网络连接并收发数据的行为)进行检测</p>
<p>预期结果:</p> <p>如果预置应用软件信息安全测试系统显示被测移动智能终端预置应用软件无擅自调用终端通信功能, 造成用户费用损失的行为, 则该项目评测结果为“未见异常”; 否则, 该项目评测结果为“不符合要求”</p>

4.5.4.3.3 信息泄露

测试编号: 4.5.4.3.3
测试项目: 预置应用软件信息泄露行为
项目要求: 见 YD/T2407-2013 第 5.5.4.3.3 节
预置条件: 被测移动智能终端处于正常工作状态
<p>测试步骤:</p> <p>步骤1: 使预置应用软件信息安全测试系统(包括服务器和客户端软件)处于正常工作状态;</p> <p>步骤2: 将预置应用软件信息安全测试系统客户端软件安装到被测移动智能终端上, 并与服务器建立连接;</p> <p>步骤3: 使用基于特征码扫描、静态源代码分析和动态行为监测等检测方法, 对被测移动智能终端预置应用软件未向用户明示并经用户同意, 擅自调用终端通信功能, 造成用户信息泄露的行为(包括在用户无确认情况下读取并传送用户电话本数据、通话记录、短信数据、彩信数据、通话录音、本地录音、图片、视频、音频和定位信息的行为)进行检测</p>
<p>预期结果:</p> <p>如果预置应用软件信息安全测试系统显示被测移动智能终端预置应用软件无擅自调用终端通信功能, 造成用户信息泄露的行为, 则该项目评测结果为“未见异常”; 否则, 该项目评测结果为“不符合要求”</p>

4.6 移动智能终端用户数据安全保护能力

4.6.1 移动智能终端的密码保护

测试编号: 4.6.1.1
测试项目: 开机密码保护
项目要求: 见 YD/T2407-2013 第 5.6.1 节
预置条件: 被测移动智能终端关机, 移动智能终端开启了用户身份认证功能
<p>测试步骤:</p> <p>步骤1: 将移动智能终端开机, 移动智能终端提示输入用户登录口令;</p> <p>步骤2: 输入正确的用户口令;</p> <p>步骤3: 通过移动智能终端的人-机界面, 进入用户登录口令更改菜单;</p> <p>步骤4: 修改用户登录口令为3位数;</p> <p>步骤5: 修改用户登录口令为4位或4位以上数字;</p> <p>步骤6: 关机, 再开机;</p> <p>步骤7: 输入旧密码;</p> <p>步骤8: 输入新密码;</p> <p>步骤9: 通过移动智能终端的人-机界面, 进入用户登录口令菜单, 关闭用户身份认证功能;</p> <p>步骤10: 关机, 再开机;</p> <p>步骤11: 通过移动智能终端的人-机界面, 将用户登录口令修改为正常值;</p> <p>步骤12: 关机, 再开机;</p> <p>步骤13: 持续输入错误的用户口令</p>
<p>预期结果:</p> <p>在步骤2后, 移动智能终端应提示输入登录口令正确, 终端正常开机;</p> <p>在步骤4, 移动智能终端应提示用户登录口令长度过短, 请求用户重新输入或者移动智能终端无法修改为3位数密码;</p> <p>在步骤5, 用户登录口令成功修改;</p> <p>在步骤7, 移动智能终端应提示登录口令错误;</p> <p>在步骤8后, 移动智能终端应提示输入登录口令正确, 终端正常开机;</p> <p>在步骤9, 在关闭用户身份认证功能前, 终端应提示用户输入用户登录口令, 输入正确, 终端应提示用户身份认证功能成功关闭;</p> <p>在步骤10后, 移动智能终端开机过程应不提示用户输入用户登录口令, 移动智能终端正常开机;</p> <p>在步骤13, 多次输入错误的用户登录口令后 (根据厂商声称, 但不多于5次), 终端应自动采取适当措施以防止持续不断的非法攻击如关机和锁死等。</p> <p>移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”</p>

测试编号: 4.6.1.2
测试项目: 开机后锁定状态的密码保护
项目要求: 见 YD/T2407-2013 第 5.6.1 节
预置条件: 被测移动智能终端关机, 移动智能终端开启了用户身份认证功能
<p>测试步骤:</p> <p>步骤1: 将移动智能终端开机, 进入屏保菜单, 启用屏保激活身份认证;</p> <p>步骤2: 保持移动智能终端处于空闲状态;</p> <p>步骤3: 使用另一终端拨打被测终端, 被测终端按接听键;</p> <p>步骤4: 呼叫结束;</p> <p>步骤5: 通过手机键盘激活系统;</p> <p>步骤6: 输入错误的口令;</p> <p>步骤7: 输入正确的口令;</p> <p>步骤8: 通过菜单关闭屏保激活身份认证;</p> <p>步骤9: 输入正确的口令</p>
<p>预期结果:</p> <p>在步骤1, 移动智能终端应提示输入屏保激活身份认证的口令;</p> <p>在步骤2, 在超过等待时间后, 移动智能终端应进入屏保状态;</p> <p>在步骤3, 移动智能终端应可正常接听电话;</p> <p>在步骤4, 呼叫结束后, 移动智能终端应立即进入屏保状态;</p> <p>在步骤5, 移动智能终端应提示用户输入屏保激活身份认证口令;</p> <p>在步骤6, 移动智能终端应提示口令错误;</p> <p>在步骤7, 移动智能终端应提示口令正确, 移动智能终端被激活, 进入正常使用状态;</p> <p>在步骤8, 移动智能终端应提示输入口令;</p> <p>在步骤9, 移动智能终端应提示屏保激活身份认证被成功关闭。</p> <p>移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”</p>

4.6.2 文件类用户数据的授权访问

测试编号: 4.6.2
测试项目: 文件类用户数据的授权访问
项目要求: 见 YD/T2407-2013 第 5.6.2 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 将图片、视频、音频和文档通过移动智能终端的文件类用户数据的授权访问功能进行保护; 步骤2: 开发第三方应用程序尝试访问被保护的图片、视频、音频和文档
预期结果: 在步骤2: 在用户确认后第三方应用程序可访问被保护的图片、视频、音频和文档。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.6.3 用户数据的加密存储

测试编号: 4.6.3
测试项目: 用户数据的加密存储
项目要求: 见 YD/T2407-2013 第 5.6.3 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 将移动智能终端的电话本数据存储于加密存储区; 步骤2: 将加密后的电话本数据采用未授权方式导出到其他设备(如本地计算机)上, 用文本编辑软件打开并查看器是否以密文方式存储
预期结果: 在步骤2, 使用文本编辑软件应无法还原电话本文件。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.6.4 用户数据的彻底删除

测试编号: 4.6.4
测试项目: 用户数据的彻底删除
项目要求: 见 YD/T2407-2013 第 5.6.4 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 在移动智能终端中预先存入测试数据, 使用数据读取工具对用户存储介质进行原始数据的读取; 步骤2: 通过移动智能终端的彻底删除功能对用户数据执行彻底删除操作; 步骤3: 使用数据读取工具再次对用户存储介质进行原始数据的读取; 步骤4: 比较步骤3和步骤1中所读出的数据
预期结果: 在步骤2, 移动智能终端可执行用户数据的彻底删除操作; 在步骤4, 对两次读出的数据进行相似性比较, 比较结果为“不一致”。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.6.5 用户数据的远程保护

测试编号: 4.6.5.1
测试项目: 用户数据的远程锁定
项目要求: 见 YD/T2407-2013 第 5.6.5 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 使用被测移动智能终端远程锁定的触发条件对移动智能终端进行远程锁定操作
预期结果: 在步骤1后, 被测移动智能终端被远程锁定。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 4.6.5.2
测试项目: 用户数据的远程删除
项目要求: 见 YD/T2407-2013 第 5.6.5 节
前置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 使用被测移动智能终端远程删除的触发条件对移动智能终端进行远程删除操作, 检查被测移动智能终端的用户数据是否被删除
预期结果: 在步骤1后, 用户数据被远程删除。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

4.6.6 用户数据的转移备份

测试编号: 4.6.6.1
测试项目: 用户数据的本地备份
项目要求: 见 YD/T2407-2013 第 5.6.6 节
前置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 通过外围接口移动智能终端与测试PC建立数据连接; 步骤2: 使用用户数据备份功能执行用户数据的备份, 检查备份的内容是否包含电话本、短信、彩信、邮件和多媒体数据。检查备份时是否给了用户相应的提示
预期结果: 在步骤2, 移动智能终端可执行对电话本、短信、彩信、邮件和多媒体数据的本地备份; 在步骤2, 移动智能终端应给用户提示正在执行数据的备份; 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 4.6.6.2
测试项目: 用户数据的远程备份
项目要求: 见 YD/T2407-2013 第 5.6.6 节
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 通过数据网络(移动通信网络、WLAN网络), 移动智能终端已建立数据网络连接; 步骤2: 移动智能终端与远程服务器建立连接; 步骤3: 执行用户数据的远程备份
预期结果: 在步骤2, 移动智能终端可执行对电话本、短信、彩信、邮件和多媒体数据的远程备份。 在步骤2, 移动智能终端应给用户提示正在执行数据的备份。 移动智能终端满足以上预期结果, 则该项目评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

5 移动智能终端功能限制性要求测试方法

测试编号: 5.1
测试项目: 移动智能终端应当真实传送信息, 不得通过对传送信息的处理或传送虚假信息使信息接收者错误识别特定通信主体等, 不得预置可改变通信系统提示信号的应用软件
项目要求: 见 YD/T2407-2013 第 6 章
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 参考说明书, 检查是否存在将主叫语音改变为已知主体语音特征的功能; 检查是否存在传送虚假图像等信息故意导致被叫方产生错误识别的功能; 对被测移动智能终端的预置应用软件进行检查, 确认是否具有相关语音软件或视频软件, 并对相关软件的菜单项进行遍历检查, 确认其是否具备可改变通信系统提示信号的功能
预期结果: 在步骤1, 如通过检查未发现导致信息接收者错误识别特定通信主体的功能, 也未发现可改变系统提示信号的应用软件, 则评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 5.2
测试项目: 移动智能终端不得预置国家法律法规禁止的信息内容
项目要求: 见 YD/T2407-2013 第 6 章
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 参考说明书, 对被测移动智能终端的菜单进行遍历检查, 确认其是否包含国家法律法规禁止的内容
预期结果: 在步骤1, 如通过检查未发现国家法律法规禁止的内容, 则评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

测试编号: 5.3
测试项目: 移动智能终端不得预置为传播发布国家法律法规禁止信息内容提供服务的应用软件
项目要求: 见 YD/T2407-2013 第 6 章
预置条件: 被测移动智能终端处于正常工作状态
测试步骤: 步骤1: 参考说明书, 对被测移动智能终端的应用软件进行遍历检查; 步骤2: 确认其能否为传播发布国家法律法规禁止信息内容提供服务
预期结果: 在步骤2, 如通过检查未发现为传播发布国家法律法规禁止信息内容提供服务的软件, 则评测结果为“未见异常”, 反之该项目评测结果为“不符合要求”

参 考 文 献

- [1] ITU-T X.msec-6:2012 《手机安全总览》
-

中华人民共和国
通信行业标准
移动智能终端安全能力测试方法
YD/T 2408-2013

*

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：2.75 2013年5月北京第1次印刷
字数：73千字

15115·85

本书如有印装质量问题，请与本社联系 电话：(010)67114922