ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34975—2017

信息安全技术　移动智能终端应用软件安全技术要求和测试评价方法

Information security technology—Security technical requirements and testing and evaluation approaches for application software of smart mobile 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:公安部第三研究所(公安部计算机信息系统安全产品质量监督检验中心)、杭州安恒信息技术有限公司、华东师范大学、中国电子技术标准化研究院、中国信息安全研究院有限公司、中国信息通信研究院、中国移动通信集团公司、华东理工大学、国家信息中心。

本标准主要起草人:俞优、张艳、陆臻、何道敬、唐迪、顾健、沈亮、杨元原、陈妍、杨晨、许玉娜、范渊、孙小平、林家骏、杨正军、潘娟、邱勤、袁捷、章恒。

信息安全技术　移动智能终端应用软件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应用软件的安全技术要求和测试评价方法。

本标准适用于移动智能终端应用软件的开发、运作与维护等生存周期过程的安全保护与测试评估，不适用于移动智能终端恶意软件的评估。

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 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 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　smart mobile 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产品。

3.2

移动智能终端操作系统　operating system of smart mobile terminal

移动智能终端最基本的系统软件，用于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接口。

3.3

移动智能终端应用软件　application software of smart mobile terminal

针对移动智能终端开发的应用软件，包括移动智能终端预置的第三方应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装和升级的应用软件。

4　安全技术要求

4.1　安全功能要求

4.1.1　安装及卸载安全

4.1.1.1　安装要求

终端应用软件的安装需得到明确授权，其安装过程只能运行在特定环境中且不能破坏其运行环境。具体技术要求如下：

a) 包含可有效表征供应者或开发者身份的签名信息、软件属性信息；
b) 正确安装到相关移动智能终端上，并生成相应的图标；
c) 安装时应提示终端操作系统用户对其使用的终端资源和终端数据进行确认；
d) 不应对终端操作系统和其他应用软件的正常运行造成影响。

4.1.1.2 卸载要求

终端应用软件卸载后，不影响移动智能终端的正常使用。具体技术要求如下：
a) 应能删除安装和使用过程中产生的资源文件、配置文件和用户数据；
b) 删除用户使用过程中生成的数据时应有提示；
c) 不应影响终端操作系统和其他应用软件的功能。

4.1.2 鉴别机制

4.1.2.1 身份认证

若终端应用软件涉及用户敏感数据，则应对访问用户提供有效的身份认证机制。具体技术要求如下：
a) 在用户访问应用业务前，终端应用软件对其身份进行鉴别，并提供鉴别失败处理措施；
b) 具备登录超时后的锁定或注销功能。

4.1.2.2 口令安全机制

若终端应用软件使用过程中涉及用户口令，则具体技术要求如下：
a) 在使用过程中不应以明文形式显示和存储；
b) 不应默认保存用户上次的账号及口令信息；
c) 具备口令强度检查机制；
d) 具备口令时效性检查机制；
e) 修改或找回口令时，具备验证机制；
f) 在使用过程中应具备防键盘劫持机制。

4.1.2.3 验证码安全机制

若终端应用软件使用过程中涉及验证码包括图形和手机短信验证码，则具体技术要求如下：
a) 验证码应在终端应用软件服务端生成；
b) 图形验证码应具备一定的抗机器识别能力；
c) 应具有短信验证码防重放攻击机制。

4.1.3 访问控制

4.1.3.1 基于用户的控制

若终端应用软件涉及用户敏感数据，则应对访问用户提供有效的授权机制。具体技术要求如下：
a) 授权用户访问的内容不能超出授权的范围；
b) 限制应用用户账号的多重并发会话。

4.1.3.2 对应用软件的限制

终端应用软件访问终端数据和终端资源应经过终端操作系统用户明确的许可。具体技术要求如下：

a） 未得到许可前不应访问终端数据和终端资源；
b） 未得到许可前不应修改和删除终端数据，不应修改终端资源的配置。

4.1.4 数据安全

4.1.4.1 数据存储安全

终端应用软件不应以明文形式存储用户敏感数据，以防止数据被未授权获取。

4.1.4.2 数据传输安全

终端应用软件不应以明文形式通过网络传输用户敏感数据，以防止数据被未授权获取。

4.1.4.3 数据删除

终端应用软件若具备数据删除功能，在删除数据前应明确提示用户，并由用户再次确认是否删除数据。

4.1.4.4 备份和恢复

终端应用软件若具备备份和恢复功能，具体技术要求如下：
a） 备份机制应完整有效，且应对备份数据进行保护；
b） 恢复数据在使用前应校验其可用性、完整性。

4.1.5 运行安全

4.1.5.1 实现安全

终端应用软件应保证程序自身的安全性：
a） 不应设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口；
b） 应具备安全机制防止程序被反编译、反调试；
c） 应不存在已公布的高危风险漏洞。

4.1.5.2 稳定性

终端应用软件应保证其稳定运行，避免出现功能失效等类似现象。具体要求如下：
a） 不应造成终端崩溃或异常的情况；
b） 避免出现失去响应、闪退等现象；
c） 允许随时停止、退出。

4.1.5.3 容错性

终端应用软件应能处理可预知的错误操作，不应影响程序的正常工作。

4.1.5.4 资源占用

终端应用软件的运行对终端资源，不应长时间固定或无限制占用，不应影响对终端合法的用户登录和资源访问。

4.1.5.5 升级

终端应用软件应支持软件的更新，具体技术要求如下：
a） 至少采取一种安全机制，保证升级的时效性和准确性；

b） 保证终端应用软件安全机制的有效性。

4.1.6 其他安全要求

终端应用软件服务端应至少满足如下要求：

a） 不应在数据库或文件系统中明文存储用户敏感信息；
b） 不应在 Cookie 中保存明文口令；
c） 应采取会话保护措施保障终端应用软件与服务端之间的会话不被窃听、篡改、伪造和重放；
d） 不应在服务器端日志中记录用户敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理；
e） 应确保服务器端日志数据的安全存储，并严格限制日志数据的访问权限；
f） 如使用开源第三方应用组件及代码，应对已公布的安全漏洞及时更新补丁；
g） 服务器端应不存在已公布的高危风险漏洞。

4.2 安全保障要求

4.2.1 开发

4.2.1.1 安全架构

开发者应提供终端应用软件安全功能的安全架构描述，安全架构描述应满足以下要求：

a） 与产品设计文档中对安全功能实施抽象描述的级别一致；
b） 描述与安全功能要求一致的终端应用软件安全功能的安全域；
c） 描述终端应用软件安全功能初始化过程为何是安全的；
d） 证实终端应用软件安全功能能够防止被破坏；
e） 证实终端应用软件安全功能能够防止安全特性被旁路。

4.2.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a） 完全描述终端应用软件的安全功能；
b） 描述所有安全功能接口的目的与使用方法；
c） 标识和描述每个安全功能接口相关的所有参数；
d） 描述安全功能接口相关的安全功能实施行为；
e） 描述由安全功能实施行为处理而引起的直接错误消息；
f） 证实安全功能要求到安全功能接口的追溯。

4.2.1.3 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a） 根据子系统描述终端应用软件结构；
b） 标识和描述终端应用软件安全功能的所有子系统；
c） 描述安全功能所有子系统间的相互作用；
d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口。

4.2.2 指导性文档

4.2.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一

致，对每一种用户角色的描述应满足以下要求：

a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；

b） 描述如何以安全的方式使用终端应用软件提供的可用接口；

c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；

d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；

e） 标识终端应用软件运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；

f） 充分实现安全目的所执行的安全策略。

4.2.2.2 准备程序

开发者应提供终端应用软件及其准备程序，准备程序描述应满足以下要求：

a） 描述与开发者交付程序相一致的安全接收所交付终端应用软件必需的所有步骤；

b） 描述安全安装终端应用软件及其运行环境必需的所有步骤。

4.2.3 生命周期支持

4.2.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a） 为终端应用软件的不同版本提供唯一的标识；

b） 使用配置管理系统对组成终端应用软件的所有配置项进行维护，并唯一标识配置项；

c） 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法。

4.2.3.2 配置管理范围

开发者应提供终端应用软件配置项列表，并说明配置项的开发者。配置项列表至少包含终端应用软件、安全保障要求的评估证据和终端应用软件的组成部分。

4.2.3.3 交付程序

开发者应使用一定的交付程序交付终端应用软件，并将交付过程文档化。在给用户方交付终端应用软件的各版本时，交付文档应描述为维护安全所必需的所有程序。

4.2.4 测试

4.2.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖描述应表明测试文档中所标识的测试与功能规范中所描述的终端应用软件的安全功能间的对应性。

4.2.4.2 功能测试

开发者应测试终端应用软件安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a） 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b） 预期的测试结果，表明测试成功后的预期输出；

c） 实际测试结果和预期的测试结果一致。

4.2.4.3 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

4.2.5 脆弱性评定

基于已标识的潜在脆弱性，终端应用软件能够抵抗具有基本攻击潜力攻击者的攻击。

5 测试评价方法

5.1 安全要求测试

5.1.1 安装及卸载安全

5.1.1.1 安装要求

安装要求的测试评价方法如下：

a) 测试方法：

1) 在移动智能终端上指定位置安装终端应用软件；
2) 检查应用软件是否包含供应者或开发者的签名信息、软件属性信息（如名称、版本信息和描述等）；
3) 检查终端应用软件是否提示操作系统用户对其使用的终端资源（如网络通信模块、摄像头、导航定位等）和终端数据（如相册、通讯录等）进行确认；
4) 运行终端应用软件，检查是否对终端操作系统、其他应用软件（包括预置应用软件）的使用造成影响。

b) 预期结果：

1) 能够安装到移动智能终端上，并生成相应图标；
2) 包含供应者或开发者的签名信息、软件属性信息；
3) 提示终端操作系统用户对其使用的终端资源和终端数据进行确认；
4) 终端应用软件安装后，终端操作系统和其他应用软件仍能正常使用。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.1.2 卸载要求

卸载要求的测试评价方法如下：

a) 测试方法：

1) 卸载终端应用软件，检查其安装及使用生成的文件和数据是否能完全删除；
2) 检查删除用户数据时（如业务数据）是否有提示；
3) 检查是否对终端操作系统、其他应用软件（包括预置应用软件）的使用造成影响。

b) 预期结果：

1) 卸载时能够将其安装及使用过程产生的数据全部删除；
2) 删除用户数据时能够提示用户；
3) 卸载后系统软件和其他应用软件仍能正常使用。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.2 鉴别机制

5.1.2.1 身份认证

身份认证的测试评价方法如下：

a) 测试方法：

1) 检查在用户访问应用业务前，终端应用软件是否对其身份进行鉴别；
2) 连续尝试登录失败时，检查终端应用软件是否具备鉴别失败处理措施（如锁定账号等）；
3) 用户登录后长时间不进行任何操作。

b) 预期结果：

1) 只有身份认证成功的应用用户才能使用终端应用软件；
2) 具备鉴别失败处理措施；
3) 具备登录超时后的锁定或注销功能。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.2.2 口令安全机制

口令安全机制的测试评价方法如下：

a) 测试方法：

1) 在终端应用软件中输入口令，检查口令是否以明文形式显示或存储；
2) 检查终端应用软件是否默认保存用户上次的账号及口令信息；
3) 检查终端应用软件是否具备口令强度检查机制（如口令长度、复杂度要求等）；
4) 检测终端应用软件是否具备口令时效性检查机制（如主动提示用户定期修改口令等）；
5) 检测终端应用软件在修改或找回口令时，是否具备验证机制（如验证手机号码等）；
6) 检查终端应用软件是否具备防键盘劫持机制。

b) 预期结果：

1) 口令在使用、存储过程中不出现明文；
2) 未保存用户上次的账号及口令信息；
3) 具备口令强度检查机制，初始化及修改用户口令时，能够根据策略检查输入口令的长度和复杂度，若输入的口令不符合口令强度要求，能够提示，并要求重新设置有效口令；
4) 具备口令时效性检查机制，能够主动提示用户修改口令；
5) 修改或找回口令时，具备验证机制，以防止口令的被非授权获取或篡改；
6) 口令在使用过程中具备防键盘劫持机制，无法劫持获取用户输入的口令。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.2.3 验证码安全机制

验证码安全机制的测试评价方法如下：

a) 测试方法：

1) 检查终端应用软件验证码是否在服务端生成而不是在客户端生产；
2) 检查终端应用软件图形验证码是否可以被机器识别出明文；
3) 检查终端应用软件手机短信验证码是否具备限制应用用户短信验证码的多重发送机制。

b) 预期结果：

1） 验证码在服务端生成；
2） 图片验证码在使用过程中具备一定的抗机器识别能力；
3） 终端应用软件手机短信验证码具有防重放攻击机制。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.3 访问控制

5.1.3.1 基于用户的控制

基于用户的控制的测试评价方法如下：

a） 测试方法：
1） 用户成功登录后，分别访问其授权和非授权的业务；
2） 使用同一用户账号在其他终端上同时登录。

b） 预期结果：
1） 应用用户仅能访问授权业务；
2） 对用户账号的多重并发会话进行限制。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.3.2 对应用软件的限制

对应用软件的限制的测试评价方法如下：

a） 测试方法：
1） 检查终端应用软件访问、修改和删除终端数据前是否明确经过终端操作系统用户的许可；
2） 检查终端应用软件访问、修改终端资源及其配置是否明确经过终端操作系统用户的许可。

b） 预期结果：
1） 未经过终端操作系统用户明确许可前，终端应用软件不能访问、修改和删除终端数据；
2） 未经过终端操作系统用户明确许可前，终端应用软件不能访问、修改终端资源及其配置。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.4 数据安全

5.1.4.1 数据存储安全

数据存储安全的测试评价方法如下：

a） 测试方法：
处理用户敏感数据（如金融账户、联系人信息、聊天信息等）时，检查应用软件是否以明文形式写入文件中。

b） 预期结果：
不以明文形式将用户敏感数据写到任何文件中。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.4.2 数据传输安全

数据传输安全的测试评价方法如下：

a） 测试方法：

截取数据包，检查应用软件是否以明文形式通过网络传输用户敏感数据。

b） 预期结果：

不以明文形式通过网络传输用户敏感数据。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.4.3 数据删除

数据删除的测试评价方法如下：

a） 测试方法：

1） 检查终端应用软件是否提供数据删除的功能；

2） 检查在数据删除前，终端应用软件是否明确提示用户，并由用户再次确认是否删除数据。

b） 预期结果：

1） 提供数据删除功能；

2） 在数据删除之前，终端应用软件能够明确通知用户，用户能够进一步确认或取消数据删除操作。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.4.4 备份和恢复

备份和恢复的测试评价方法如下：

a） 测试方法：

1） 检查终端应用软件是否提供数据备份和恢复机制；

2） 检查存储的备份数据是否为明文；

3） 数据恢复后，检查终端应用软件是否进行校验。

b） 预期结果：

1） 提供有效的数据备份和恢复机制；

2） 对备份数据进行保护；

3） 恢复数据在使用前校验其有效性、完整性。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.5 运行安全

5.1.5.1 实现安全

实现安全的测试评价方法如下：

a） 测试方法：

1） 检查终端应用软件（如分析源代码）是否存在有违反或绕过安全规则的任何类型的接口，以及文档中未说明的接口；

2） 检查终端应用软件是否具备安全机制防止程序被反编译、反调试；

3） 测试终端应用软件是否存在已公布的高危风险漏洞。

b） 预期结果：

1） 不留有任何违反或绕过安全规则的任何类型的接口；

2） 提供有效的机制（如混淆技术）防止程序被反编译、反调试；

3） 不存在已公布的高危风险漏洞。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.5.2 稳定性

稳定性的测试评价方法如下：

a） 测试方法：

1） 在测试过程中，检查终端应用软件是否出现失去响应、非正常退出、功能失效和造成系统崩溃等异常现象；

2） 检查终端应用软件是否提供停止、退出的功能。

b） 预期结果：

1） 测试过程中，终端应用软件稳定运行，未出现失去响应、非正常退出、功能失效和造成系统崩溃等现象；

2） 运行过程中，终端应用软件能够随时停止、退出。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.5.3 容错性

容错性的测试评价方法如下：

a） 测试方法：

尝试输入错误的操作（如输入数据类型、长度等），检查应用软件是否能够处理。

b） 预期结果：

支持处理可预知的用户错误操作，且不影响程序的正常工作。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.5.4 资源占用

资源占用的测试评价方法如下：

a） 测试方法：

在终端上测试终端应用的资源占用情况。

b） 预期结果：

未出现长时间、无限制占用终端系统资源的情况。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.5.5 升级

升级的测试评价方法如下：

a） 测试方法：

1） 检查终端应用软件是否提供软件的升级功能；

2） 检查终端应用软件是否提供安全机制，从而保证升级的时效性（如自动升级、更新通知等）和准确性（如完整性校验）。

b） 预期结果：

1） 具备升级功能；
2） 更新过程中，采用安全机制保证升级的时效性和准确性。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.1.6 其他安全要求

其他安全要求的测试评价方法如下：

a） 测试方法：
1） 检查终端应用软件服务端是否在数据库或文件系统中明文存储用户敏感信息；
2） 检查是否存在 Cookie 中保存明文口令的现象；
3） 检查是否提供措施保障终端应用软件与服务端之间的会话不被窃听、篡改、伪造和重放；
4） 检查终端应用软件服务端日志是否涉及用户敏感信息；
5） 检查终端应用软件服务端日志是否严格限制访问权限；
6） 测试开源第三方应用组件及代码是否及时更新补丁；
7） 检查应用软件服务端是否存在高危风险安全漏洞。

b） 预期结果：
1） 终端应用软件服务端未在数据库或文件系统中明文存储用户敏感信息；
2） 不存在 Cookie 中保存明文口令的现象；
3） 采取会话保护措施保障终端应用软件与服务端之间的会话不可被窃听、篡改、伪造和重放等；
4） 终端应用软件服务端日志中未涉及用户敏感信息，或对录敏感信息进行了模糊化处理；
5） 终端应用软件服务端安全存储日志数据，并严格限制日志数据的访问权限；
6） 开源第三方应用组件及代码及时更新补丁，不存在已公布的安全漏洞；
7） 应用软件服务端不存在已公布的高危风险漏洞。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2 安全保障要求测试

5.2.1 开发

5.2.1.1 安全架构

安全架构的测试评价方法如下：

a） 测试方法：
审查安全架构文档是否准确描述如下内容：
1） 与产品设计文档中对安全功能实施抽象描述的级别一致；
2） 描述与安全功能要求一致的终端应用软件安全功能的安全域；
3） 描述终端应用软件安全功能初始化过程为何是安全的；
4） 证实终端应用软件安全功能能够防止被破坏；
5） 证实终端应用软件安全功能能够防止安全特性被旁路。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.1.2 功能规范

功能规范的测试评价方法如下：

a) 测试方法：

审查功能规范文档是否准确描述如下内容：

1) 完全描述终端应用软件的安全功能；
2) 描述所有安全功能接口的目的与使用方法；
3) 标识和描述每个安全功能接口相关的所有参数；
4) 描述安全功能接口相关的安全功能实施行为；
5) 描述由安全功能实施行为处理而引起的直接错误消息；
6) 证实安全功能要求到安全功能接口的追溯。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.1.3 产品设计

产品设计的测试评价方法如下：

a) 测试方法：

审查产品设计文档是否准确描述如下内容：

1) 根据子系统描述终端应用软件结构；
2) 标识和描述终端应用软件安全功能的所有子系统；
3) 描述安全功能所有子系统间的相互作用；
4) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.2 指导性文档

5.2.2.1 操作用户指南

操作用户指南的测试评价方法如下：

a) 测试方法：

审查操作用户指南是否准确描述如下内容：

1) 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
2) 描述如何以安全的方式使用终端应用软件提供的可用接口；
3) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
4) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
5) 标识终端应用软件运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；
6) 充分实现安全目的所执行的安全策略。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.2.2 准备程序

准备程序的测试评价方法如下：

a） 测试方法：

审查准备程序文档是否准确描述如下内容：

1） 描述与开发者交付程序相一致的安全接收所交付终端应用软件必需的所有步骤；

2） 描述安全安装终端应用软件及其运行环境必需的所有步骤。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.3 生命周期支持

5.2.3.1 配置管理能力

配置管理能力的测试评价方法如下：

a） 测试方法：

1） 审查开发者是否为不同版本的终端应用软件提供唯一的标识；

2） 现场检查配置管理系统是否对所有的配置项作出唯一的标识，且配置管理系统是否对配置项进行了维护；

3） 审查开发者提供的配置管理文档，是否描述了对配置项进行唯一标识的方法。

b） 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.3.2 配置管理范围

配置管理范围的测试评价方法如下：

a） 测试方法：

1） 审查开发者提供的配置项列表；

2） 配置项列表是否描述了组成终端应用软件的全部配置项及相应的开发者。

b） 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.3.3 交付程序

交付程序的测试评价方法如下：

a） 测试方法：

1） 现场检查开发者是否使用一定的交付程序交付终端应用软件；
2） 审查开发者是否使用文档描述交付过程，文档中是否包含以下内容：在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

b） 预期结果：
开发者提供的文档和现场活动证据内容应满足上述要求。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.4 测试

5.2.4.1 覆盖

覆盖的测试评价方法如下：

a） 测试方法：
审查开发者提供的测试覆盖文档，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的终端应用软件的安全功能是对应的。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.4.2 功能测试

功能测试的测试评价方法如下：

a） 测试方法：
1） 审查开发者提供的测试文档，是否包括测试计划、预期的测试结果和实际测试结果；
2） 审查测试计划是否标识了要测试的安全功能，是否描述了每个安全功能的测试方案（包括对其他测试结果的顺序依赖性）；
3） 审查期望的测试结果是否表明测试成功后的预期输出；
4） 审查实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.4.3 独立测试

独立测试的测试评价方法如下：

a） 测试方法：
1） 评价者应审查开发者提供的测试资源；
2） 评价者应审查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

b） 预期结果：
开发者提供的资源应满足上述要求。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

5.2.5 脆弱性评定

脆弱性评定的测试评价方法如下：

a) 测试方法：

从用户可能破坏安全策略的明显途径出发，按照安全机制定义的安全强度级别，对终端应用软件进行脆弱性分析。

b) 预期结果：

渗透性测试结果应表明终端应用软件能够抵抗具有基本攻击潜力攻击者的攻击。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。