ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXX—20XX

信息安全技术 移动终端安全管理平台技术要求

Information security technology—Technology requirement of mobile security management platform

（征求意见稿）

（本稿完成日期：2017-4-25）

XXXX-XX-XX 发布　　XXXX-XX-XX 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

引　言

移动终端安全管理平台主要针对机构或组织移动终端以及移动终端上的移动应用、数据进行安全管理，保障企业移动终端的使用符合安全使用管理规范，防止非法移动终端访问破坏企业数据，防止他人窃取移动终端中的企业数据。部署方式上通常采用客户机/服务器架构，其客户端驻留在受管控的移动终端上，执行安全防护与监管一体化的安全管理，面向不同的移动操作系统分别有相对应的客户端软件；服务端则通常安装在独立的服务器上，用于制定和分发安全策略，对分布式部署的客户端进行集中远程监控。

本标准针对移动终端用户访问机构或组织应用中的安全身份鉴别、终端接入、访问控制、数据安全、安全审计等安全需求，从安全功能要求和安全保障要求两个方面，规范了移动终端安全管理平台的安全技术要求，按照移动终端安全管理平台安全功能的强度以及安全保障要求，将安全等级划分为基本级和增强级。其中，安全功能包括终端管理、应用管理、数据安全、接入控制、安全管理、客户端保护和安全审计等七个方面，安全保障要求则主要从开发、指导性文档、生命周期支持和测试等方面进行规范。

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/TC260）提出并归口。

本标准起草单位：中国信息安全研究院有限公司、公安部第三研究所、中国电子技术标准化研究院、工业和信息化部电子科学技术情报研究所、国家信息技术安全研究中心、中国信息安全测评中心、中国信息安全认证中心、国家信息中心、中国电信上海理想信息产业(集团)有限公司、北京北信源软件股份有限公司、华东师范大学、北京时代新威信息技术有限公司、西安电子科技大学、北京航空航天大学、北京传媒大学

本标准主要起草人：杨晨、张艳、王惠莅、左晓栋、张格、陆臻、顾键、刘贤刚、范科峰、梁露露、王嘉捷、王石、王新杰、肖荣、钟力、丁富强、贾雪飞、魏方方、周亚超、何道敬、张弛、陈晓峰、刘虹、伍前红、姜正涛

信息安全技术移动终端安全管理平台技术要求

1 范围

本标准规定了移动终端安全管理平台的安全功能要求和安全保障要求，适用于移动终端安全管理平台产品的设计、开发与检测，为组织机构、个人用户等实施移动互联应用的安全防护提供技术参考。

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/T25069－2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3-2015和GB/T25069－2010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

指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

移动终端安全管理平台 Mobile Terminal Security Management Platform

为增强移动智能终端的安全性、可控性和时效性，通过定制安全策略对移动智能终端设备、应用等进行统一管理和安全接入控制的产品。

4 基本级安全要求

4.1 安全功能要求

4.1.1 终端管理

4.1.1.1 终端注册

应提供对移动智能终端的注册功能，注册信息包括注册日期、硬件型号、设备序列号、系统软件版本、所属部门等。

4.1.1.2 远程管理

应提供以下远程管理功能：

a) 应能远程锁定移动智能终端；

b) 应能远程擦除移动智能终端存储的敏感业务数据；

c) 应能远程备份移动智能终端存储的敏感业务数据。

4.1.1.3 存储介质管理

应具备基于业务应用需求的外接存储介质管理、监测等功能，对违规使用进行告警和阻断。

4.1.1.4 系统环境安全检测

应具备对移动智能终端系统环境的恶意程序的检测、告警、杀除等功能。

4.1.1.5 远程监测

应能对移动智能终端位置信息、运行服务、设备性能、软件版本（至少应包括操作系统等）等信息进行监测。

4.1.1.6 口令或生物特征识别认证策略

应能远程设置终端口令策略，至少应包括口令长度、口令类型、复杂字符、定期更换策略、最多失败次数等。

应能监测是否设置用户口令，阻断未设置用户口令的终端接入。

应支持生物特征识别功能。

4.1.1.7 功能限制

应能远程设置功能限制策略，至少应包括禁用摄像头、禁止截屏、禁用WiFi、限制SD卡读写权限等。

4.1.2 应用管理

应支持设置白名单、黑名单的功能，并能够根据白名单、黑名单执行相应的应用程序管理策略。

4.1.3 数据安全

4.1.3.1 远程传输安全

应保障远程数据传输的安全：

a) 应采用加密、数据完整性保护等安全机制，保障远程数据传输的安全；

b) 应采用会话超时检测机制，保障远程数据传输的可用性。

4.1.3.2 数据安全存储

应对敏感数据加密存储。

应采用基于角色的数据访问控制机制。

4.1.3.3 数据防泄漏

应具备敏感数据防泄漏相关安全策略设置功能，并基于策略配置实现对终端敏感数据访问操作行为的安全监测。

4.1.3.4 数据安全监测

应支持对业务系统数据流向的实时监测，具备信息内容扫描、过滤和阻断等功能。

4.1.4 终端接入控制

4.1.4.1 终端用户管理

应具备以下终端用户管理功能：

a) 仅允许注册的移动智能终端接入系统；
b) 对终端用户进行管理的功能，可以创建、修改和删除用户；
c) 对终端用户组进行管理的功能，包括：创建、修改和删除用户组，以及修改用户所属的用户组。

4.1.4.2 终端接入认证

当终端用户请求远程接入系统时，应采用双向认证机制，并采用安全机制保障传输数据的保密性、完整性。

4.1.4.3 访问控制策略

应能够针对不同终端用户或用户组制定不同的应用资源远程访问控制策略。

应提供以下远程访问限制能力：

a) 终端用户限制：只有授权终端用户能够对应用资源进行远程访问；
b) 访问内容限制：授权终端用户对应用资源进行远程访问的内容不能超出预定义的范围；
c) 动作限制：授权终端用户对应用资源进行远程访问的动作（如对文件、文件夹进行读、写、复制、下载等操作）不能超出预定义的范围（有则适用）；
d) 时间限制：授权终端用户对应用资源进行远程访问的时间不能超出预定义的范围（有则适用）；
e) 序列号/地址限制：授权终端用户通过网络对应用资源进行远程访问时，该终端用户所使用的移动智能终端的序列号/地址不能超出预定义的范围（有则适用）；
f) 次数限制：授权终端用户对应用资源进行远程访问的次数不能超出预定义的范围（有则适用）。

4.1.5 安全管理

4.1.5.1 管理员属性初始化

应具备授权管理员属性的初始化功能。

4.1.5.2 管理员唯一性标识

应为授权管理员建立唯一的身份标识，同时将授权管理员的身份标识与其所有可审计事件进行关联。

4.1.5.3 管理员属性修改

应具备授权管理员的属性（至少包括管理员口令）修改功能。

4.1.5.4 管理员身份鉴别

应在执行任何与安全功能相关的操作之前，对声称履行授权管理员职责的人员进行身份鉴别。

当身份鉴别失败的次数达到指定阈值后，应能阻断鉴别请求。

4.1.5.5 配置管理能力

应具备授权管理员对产品进行安全配置和管理的功能，至少包括：

a) 增加、删除和修改远程接入控制等相关策略；
b) 查看当前远程接入控制策略配置；
c) 查看和管理审计日志。

4.1.5.6 管理角色

应采用基于角色的管理员授权机制，实现对系统管理、审计管理、安全管理等管理角色的划分。

4.1.5.7 终端集中管理

应具备终端集中管理功能，包括：

a) 移动智能终端客户端软件统一安装；
b) 移动智能终端应用程序白名单统一下发；
c) 移动智能终端操作系统、应用软件、客户端软件等的统一升级。

4.1.6 客户端保护

应具备对安装在移动智能终端上的客户端软件进行安全保护的功能，防止非授权用户进行以下操作：

a) 强行终止客户端软件运行；
b) 强制取消客户端软件在系统启动时自动加载；
c) 强行卸载、删除或修改客户端软件。

4.1.7 安全审计

4.1.7.1 审计数据生成

应能对下列事件生成审计记录：

a) 授权管理员鉴别的成功和失败；
b) 终端用户身份鉴别的成功和失败事件；
c) 授权管理员鉴别尝试不成功的次数超出了设定的限制导致会话连接终止；
d) 终端用户身份鉴别尝试不成功的次数超出了设定的限制导致会话连接终止；
e) 授权管理员的重要操作，如增加、删除管理员，终端用户管理，远程备份移动智能终端的业务数据，远程锁定移动智能终端，远程擦除移动智能终端的业务数据等；
f) 终端用户对应用资源远程接入的所有请求，包括成功和失败。

应在每一个审计记录中记录事件发生的日期和时间、事件主体身份、事件描述，成功或失败的标志。

4.1.7.2 审计日志存储

应提供以下功能对审计日志进行存储：

a) 存储在掉电非易失性存储介质中；
b) 当存储空间达到阈值时，应通知授权管理员。

4.1.7.3 审计日志管理

应对审计日志进行如下管理：

a) 仅允许授权管理员访问审计日志；
b) 具备按日期、时间、终端用户标识、网络资源标识等条件对审计日志进行组合查询的功能；
c) 具备对审计日志进行备份的功能。

4.2 安全保障要求

4.2.1 开发

4.2.1.1 安全架构

开发者应提供产品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产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品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) 完全描述产品的安全功能；
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) 根据子系统描述产品结构；
b) 标识和描述产品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、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产品提供的可用接口；
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) 标识产品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必须执行的安全策略。

4.2.2.2 准备程序

开发者应提供产品及其准备程序，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产品必需的所有步骤；
b) 描述安全安装产品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) 为产品的不同版本提供唯一的标识；

b) 使用配置管理系统对组成产品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

开发者应提供包含产品、安全保障要求评估证据和产品组成部分的产品配置项列表，并说明配置项的开发者。

4.2.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，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，表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性。

4.2.4.2 功能测试

开发者应测试产品安全功能，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它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。

4.2.4.4 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗具有基本攻击潜力的攻击者的攻击。

5 增强级安全要求

5.1 安全功能要求

5.1.1 终端管理

5.1.1.1 终端注册

应具备对移动智能终端的注册功能，注册信息包括注册日期、硬件型号、设备序列号、系统软件版本、所属部门等。

5.1.1.2 越狱检测

支持对移动终端系统权限的状态检测。

5.1.1.3 远程监测

应能对移动智能终端位置信息、运行服务、设备性能、软件版本（至少应包括操作系统、应用程序、杀毒工具等）等信息进行监测。

5.1.1.4 非授权外联监控

应能检测出移动智能终端的非授权外联行为，并能自动对非授权外联行为进行有效的阻止（如断网、远程锁定等）。

5.1.1.5 远程管理

应提供以下远程管理功能：

a) 应能远程锁定移动智能终端；
b) 应能远程擦除移动智能终端存储的敏感业务数据；
c) 应能远程备份移动智能终端存储的敏感业务数据；
d) 应能远程卸载移动智能终端安装的违规应用软件。其中，违规应用软件是指，本标准4.1.2中黑白名单列出的违规应用软件。

5.1.1.6 数据保密性

应能对SD卡和移动智能终端存储空间上的敏感业务数据应进行加密处理，并能擦除未加密的敏感业务数据。

5.1.1.7 数据完整性

应保障移动智能终端中存储的敏感业务数据的完整性，并采取必要的措施对其完整性进行检验。

5.1.1.8 账户安全

应具备移动智能终端强制设置密码保护的功能。

5.1.1.9 终端集中管理

应具备终端集中管理功能：

a) 移动智能终端客户端软件统一安装；
b) 移动智能终端应用程序白名单统一下发；
c) 移动智能终端操作系统、应用软件、客户端软件等的统一升级。

5.1.2 应用管理

应支持设置应用白名单、黑名单的功能，并支持根据白名单、黑名单执行相应的应用程序管理策略。

5.1.3 数据安全

5.1.3.1 远程传输安全

应保障远程数据传输的安全：

a) 应采用加密、数据完整性保护等安全机制，保障远程数据传输安全；
b) 应采用会话超时检测机制，保障远程数据传输的可用性。

5.1.3.2 数据安全存储

应对敏感数据加密存储。

应采用基于角色的数据访问控制机制。

5.1.3.3 数据防泄漏

应具备敏感数据防泄漏相关安全策略设置功能，并基于策略配置实现对终端敏感数据访问操作行为的安全监测。

5.1.3.4 数据安全监测

应支持对业务系统数据流向的实时监测，具备信息内容扫描、过滤和阻断等功能。

5.1.4 终端接入控制

5.1.4.1 终端用户认证管理

5.1.4.1.1 终端用户管理

应具备以下终端用户管理功能：

a) 对终端用户进行管理的功能，可以创建、修改和删除终端用户；

b) 对终端用户组进行管理的功能，包括：创建、修改和删除终端用户组，以及修改终端用户所属的用户组。

5.1.4.1.2 终端接入认证

当终端用户请求远程接入应用资源时，应采用双向认证机制鉴别用户身份，并采用安全机制保障传输数据的保密性、完整性。

5.1.4.1.3 **鉴别失败处理**

应能为终端用户身份鉴别设定一个鉴别尝试次数阈值，当终端用户的鉴别不成功次数超过阈值时，应阻止鉴别请求。

5.1.4.1.4 鉴别信息保密性

若在终端用户身份鉴别的过程中，终端用户鉴别信息必须通过网络进行传输，应保障数据保密性，防止鉴别信息的泄露。

5.1.4.1.5 **报警功能**

应具备以下报警功能：

a) 移动智能终端越狱或root的操作；

b) 移动智能终端非授权外联行为。

5.1.4.2 接入控制策略

5.1.4.2.1 终端用户远程访问控制策略

应能够针对不同终端用户制定不同的应用资源远程访问控制能力。

5.1.4.3 远程访问限制能力

应提供以下远程访问限制能力：

a) 用户限制：只有授权终端用户能够对应用资源进行远程访问；
b) 访问内容限制：授权终端用户对应用资源进行远程访问的内容不能超出预定义的范围；
c) 动作限制：授权终端用户对应用资源进行远程访问的动作（如对文件、文件夹进行读、写、复制、下载等操作）不能超出预定义的范围（有则适用）；
d) 时间限制：授权终端用户对应用资源进行远程访问的时间不能超出预定义的范围（有则适用）；
e) 序列号/地址限制：授权终端用户通过网络对应用资源进行远程访问时，该终端用户所使用的移动智能终端的序列号/地址不能超出预定义的范围（有则适用）；
f) 次数限制：授权终端用户对应用资源进行远程访问的次数不能超出预定义的范围（有则适用）。

5.1.4.4 远程访问控制策略不可旁路

应保障终端用户对应用资源的远程接入都要受到远程访问控制策略的制约。

5.1.5 安全管理

5.1.5.1 管理员属性初始化

应具备授权管理员属性的初始化功能。

5.1.5.2 管理员唯一性标识

应为授权管理员建立唯一的身份标识，同时将授权管理员的身份标识与所有可审计事件进行关联。

5.1.5.3 管理员属性修改

应具备授权管理员的属性（至少包括管理员口令）的修改功能。

5.1.5.4 管理员身份鉴别

应在执行任何与安全功能相关的操作之前，对声称履行授权管理员职责的人员进行身份鉴别。

5.1.5.5 配置管理能力

应具备授权管理员对产品进行安全配置和管理的功能，至少包括：
a) 增加、删除和修改远程接入控制等相关策略；
b) 查看当前远程接入控制策略配置；
c) 查看和管理审计日志。

5.1.5.6 管理角色

应采用基于角色的管理员授权机制，实现对系统管理、审计管理、安全管理等管理角色的划分。
a) 具有至少两种不同权限的管理员角色；
b) 应能根据不同的功能模块，自定义各种不同权限角色，并可对管理员分配角色。

5.1.6 客户端保护

应具备对安装在移动智能终端上的客户端软件进行安全保护的功能，防止非授权用户进行以下操作：
a) 强行终止客户端软件运行；
b) 强制取消客户端软件在系统启动时自动加载；
c) 强行卸载、删除或修改客户端软件。

5.1.7 安全审计

5.1.7.1 审计数据生成

应能对下列事件生成审计记录：

a) 授权管理员鉴别的成功和失败；
b) 终端用户身份鉴别的成功和失败事件；
c) 授权管理员鉴别尝试不成功的次数超出了设定的限制导致会话连接终止；
d) 终端用户身份鉴别尝试不成功的次数超出了设定的限制导致会话连接终止；
e) 授权管理员的重要操作，如增加、删除管理员，终端用户管理，远程备份移动智能终端的业务数据，远程锁定移动智能终端，远程擦除移动智能终端的业务数据等；
f) 终端用户对应用资源远程接入的所有请求，包括成功和失败。

应在每一个审计记录中记录事件发生的日期和时间、事件主体身份、事件描述，成功或失败的标志。

5.1.7.2 审计日志存储

应提供以下功能对审计日志进行存储：

a) 存储在掉电非易失性存储介质中；
b) 当存储空间达到阈值时，应通知授权管理员。

5.1.7.3 审计日志管理

应对审计日志进行如下管理：

a) 仅允许授权管理员访问审计日志；
b) 具备按日期、时间、终端用户标识、网络资源标识等条件对审计日志进行组合查询的功能；
c) 具备对审计日志进行备份的功能。

5.2 安全保障要求

5.2.1 开发

5.2.1.1 安全架构

开发者应提供产品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产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全特性被旁路。

5.2.1.2 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) 完全描述产品的安全功能；
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；
g) **描述安全功能实施过程中，与安全功能接口相关的所有行为；**

h) **描述可能由安全功能接口的调用而引起的所有直接错误消息。**

5.2.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：

a) **提供产品设计描述与实现表示实例之间的映射，并证明其一致性；**
b) **按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；**
c) **以开发人员使用的形式提供。**

5.2.1.4 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) 根据子系统描述产品结构；
b) 标识和描述产品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；
e) **根据模块描述安全功能；**
f) **提供安全功能子系统到模块间的映射关系；**
g) **描述所有安全功能实现模块，包括其目的及与其它模块间的相互作用；**
h) **描述所有实现模块的安全功能要求相关接口、其它接口的返回值、与其它模块间的相互作用及调用的接口；**
i) **描述所有安全功能的支撑或相关模块，包括其目的及与其它模块间的相互作用。**

5.2.2 指导性文档

5.2.2.1 操作用户指南

开发者应提供明确、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产品提供的可用接口；
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) 标识产品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必须执行的安全策略。

5.2.2.2 准备程序

开发者应提供产品及其准备程序，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产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

5.2.3 生命周期支持

5.2.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品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；
d) **配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；**
e) **配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；**
f) **配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。**

5.2.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：
a) 产品、安全保障要求的评估证据和产品的组成部分；
b) **实现表示、安全缺陷报告及其解决状态。**

5.2.3.3 交付程序

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

5.2.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

5.2.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行必要的控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

5.2.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

5.2.4 测试

5.2.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：
a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；
b) **表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。**

5.2.4.2 深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：
a) **证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；**
b) **证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。**

5.2.4.3 功能测试

开发者应测试产品安全功能，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它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。

5.2.4.4 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。

5.2.4.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a) 具有基本攻击潜力的攻击者的攻击；

b) **具有增强型基本攻击潜力的攻击者的攻击。**