ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30284—2020
代替 GB/T 30284—2013

信息安全技术　移动通信智能终端操作系统安全技术要求

**Information security techniques—
Security technical requirements for operating system on smart mobile terminal**

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
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。

本标准代替 GB/T 30284—2013《移动通信智能终端操作系统安全技术要求(EAL2 级)》。

本标准与 GB/T 30284—2013 相比，主要技术变化如下：

——修改了标准名称为《信息安全技术　移动通信智能终端操作系统安全技术要求》；

——修改了“范围”中安全技术要求级别(见第 1 章)；

——修改了第 2 章规范性引用文件(见第 2 章和 2013 年版的第 2 章)；

——增加了术语“可信信道”“可信路径”和“TSF 数据”及其定义(见 3.1.9、3.1.10、3.1.11)；

——修改了术语“移动通信智能终端”和“用户数据”的定义(见 3.1.7、3.1.12)；

——删除了部分术语(见 2013 年版的第 3 章)；

——增加了部分缩略语(见 3.2)；

——修改了移动通信智能终端操作系统描述(见 4.1)；

——修改了安全问题定义中“威胁”“组织安全策略”和“假设”的规定(见 5.2、5.3、5.4)；

——修改了安全目的的规定(见第 6 章)；

——将原标准第 7 章“安全功能要求”和第 8 章“安全保障要求”合并为 “安全要求”(见第 7 章)；

——删除了“安全审计类：FAU”中的“审计查阅(FAU_SAR.1)”和“有限审计查阅(FAU_SAR.2)”(见 2013 年版的 7.9.4 和 7.9.5)；

——删除了“密码支持类：FCS”中的扩展组件“密码支持基本要求(FCS_CBR_EXT.1)”和“密码操作应用(FCS_COA_EXT.1)”(见 2013 年版的 7.7.2 和 7.7.3)；

——删除了“安全管理类：FMT”中的“安全属性撤销(FMT_REV.1)” (见 2013 年版的 7.5.10)；

——删除了“TOE 访问类：FTA”中“TOE 会话建立(FTA_TSE.1)”和“可选属性范围限定(FTA_LSA.1)”(见 2013 年版的 7.6.4 和 7.6.5)；

——增加了“安全审计(FAU 类)”中的“防止审计数据丢失(FAU_STG.4)”(见 7.1.2.4)；

——增加了“密码支持(FCS 类)”(见 7.1.3)；

——增加了“用户数据保护(FDP 类)”中的“子集残余信息保护(FDP_RIP.1)”和“基本回退(FDP_ROL.1)”(见 7.1.4.9 和 7.1.4.10)；

——增加了“安全管理(FMT 类)”中的“TSF 数据限值的管理(FMT_MTD.2)”(见 7.1.6.6)；

——增加了“TSF 保护(FPT 类)”中的“失效即保持安全状态(FPT_FLS.1)”(见 7.1.7.1)；

——增加了“资源利用(FRU 类)”(见 7.1.8)；

——增加了 EAL3、EAL4 级的安全保障要求(见 7.2)；

——修改了安全目的和安全要求的基本原理的规定(见 8.1 和 8.2)；

——增加了组件依赖关系的规定(见 8.3)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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：中国信息安全测评中心、兴唐通信科技有限公司、国网思极网安科技(北京)有限公司、北京元心科技有限公司、中国科学院软件研究所、北京邮电大学、中国信息通信研究院、展讯通信(上海)有限公司。

本标准主要起草人：张宝峰、贾炜、杨永生、石竑松、李凤娟、许源、殷树刚、宁华、饶华一、毕海英、

张骁、熊琦、邓辉、高金萍、张阳、梁洪亮、邹仕洪、毛军捷、王蓓蓓、庞博、朱瑞瑾、刘昱函、许勇刚、陈佳哲、李贺鑫、李祉岐、魏伟、孙亚飞、王宇航、王亚楠、李静、朱克雷、黄小莉、骆扬、王书毅、王峰、张翀斌、郭颖。

本标准所代替标准的历次版本发布情况为：

——GB/T 30284—2013。

信息安全技术　移动通信智能终端操作系统安全技术要求

1　范围

本标准规定了移动通信智能终端(以下简称移动终端)操作系统的安全功能要求和达到EAL2、EAL3和EAL4保障级的安全保障要求。

本标准适用于移动终端操作系统产品的设计、开发、测试和采购。

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 18336.1—2015　信息技术　安全技术　信息技术安全评估准则　第1部分:简介和一般模型

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 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、定义和缩略语

3.1　术语和定义

GB/T 18336.1—2015及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

管理员　administrator

一个授权用户,拥有管理部分或全部移动终端操作系统安全功能的权限,同时可拥有旁路部分移动终端操作系统安全策略的特权。

3.1.2

应用软件　application software

移动终端操作系统之外,向用户提供服务功能的软件。

3.1.3

鉴别数据　authentication data

用于验证用户所声称身份的信息。

3.1.4

授权用户　authorized user

依据安全策略可执行某项操作的用户。

3.1.5

资源　resource

一组有限的逻辑或物理实体。

注：操作系统为用户、主体和客体分配或管理资源，如存储空间、电源、CPU、无线通信设备等。

3.1.6

会话　session

用户与 TSF 的一段交互。

注：会话建立受控于多种因素，如用户鉴别、对 TOE 访问的时间和方法及允许建立会话的最大数等。

3.1.7

移动通信智能终端　smart mobile terminal

能接入移动通信网，提供应用软件开发接口，并能安装和运行第三方应用软件的移动终端设备。

3.1.8

TOE 安全功能　TOE security functionality

正确执行 SFR 应依赖的 TOE 的所有硬件、软件和固件的组合功能。

3.1.9

可信信道　trusted channel

TSF 同远程可信 IT 产品能在必要的信任基础上进行通信的一种通信手段。

3.1.10

可信路径　trusted path

用户和 TSF 能在必要的信任基础上进行通信的一种通信手段。

3.1.11

TSF 数据　TSF data

实施移动终端操作系统安全功能所依赖的数据。

3.1.12

用户数据　user data

由用户产生或为用户服务的数据。

3.2　缩略语

下列缩略语适用于本文件。

API　应用编程接口(Application Programming Interface)

CM　配置管理(Configuration Management)

EAL　评估保障级(Evaluation Assurance Level)

IP　互联网协议(Internet Protocol)

IT　信息技术(Information Technology)

PP　保护轮廓(Protection Profile)

SFP　安全功能策略(Security Function Policy)

SFR　安全功能要求(Security Functional Requirements)

ST　安全目标(Security Target)

TOE　评估对象(Target of Evaluation)

TSF　TOE 安全功能(TOE Security Functionality)

TSFI　TSF 接口(TSF Interface)

4 概述

4.1 移动终端操作系统描述

移动终端操作系统是运行在智能移动终端上的系统软件，是智能移动终端的组成部分，用于控制、管理移动终端上的硬件、软件和固件，提供用户操作界面和应用软件编程接口（API）。

移动终端操作系统应具备下述特征：

a） 运行在智能移动终端上；

b） 支持多个用户角色；

c） 支持应用软件安装；

d） 应用软件通过操作系统访问数据、传感器及无线通信资源；

e） 支持基于互联网协议的网络通信；

f） 可与远程信息系统协同工作。

4.2 移动终端操作系统安全特征

移动终端操作系统需要抵御的威胁主要来自非授权用户的访问、授权用户的恶意访问、恶意应用软件的访问和互联网非授权实体的访问等。

移动终端失去物理保护时，可能受到非授权用户的恶意访问。因此，移动终端操作系统应利用会话建立、会话锁定、会话解锁、数据备份、备份数据保护、防丢失等功能应对此类威胁，防范用户数据的泄露和丢失。

移动终端操作系统应通过安全角色划分，把对用户数据、通信资源的访问授权管理职能赋予移动终端授权用户。移动终端操作系统可选择把复杂的安全管理职能赋予在远程可信信息系统上的专业技术用户，以实现远程可信信息系统对移动终端的管理。移动终端授权用户可能有旁路或部分旁路移动终端操作系统安全机制的特权，应通过划分角色对授权用户的权限加以限制，并通过审计对授权用户的操作行为进行记录和跟踪。

移动终端操作系统应具备数据传输保护、完整性校验等安全特性维系与应用软件责任担保者之间的信任传递链条，抵御恶意软件的安装。同时移动终端操作系统应通过实施访问控制策略限制应用软件的访问权限，使应用软件对用户数据、通信资源、传感器的访问均被访问控制策略覆盖。

移动终端操作系统应对 IP 网络信息实施信息流控制策略，过滤无法鉴别、未经授权的 IP 网络数据包，保护移动终端的带宽资源、话费和电源能量。

移动终端操作系统及其安全功能自身也应得到保护，移动终端安全架构应保证移动终端操作系统不受不可信用户、不可信主体的干扰和破坏。

移动终端操作系统部分安全功能的实现还应得到密码服务的支持，这些安全功能包括：标识与鉴别、可信信道等。

移动终端操作系统应具备的安全功能如下：

a） 对用户、应用、进程等进行唯一标识；

b） 对用户和远程 IT 实体进行鉴别；

c） 执行访问控制和网络信息流控制策略；

d） 执行应用软件限制策略；

e） 执行设备安全管理，即具有可配置的安全和管理策略，实现远程可信信息系统对移动终端的安全管理；

f） 执行访问授权管理，即管理员能根据需要初始化、配置、修改应用软件的访问权限；

g） 对用户行为审计；

h） 提供密码支持。

5 安全问题定义

5.1 资产

应保护的评估对象资产：

——TSF 数据（如鉴别数据、安全属性、访问控制列表、安全配置数据等信息）；

——用户数据（如用户身份标识、位置信息、账户信息、通信记录、通讯录等信息）；

——敏感资源（包含通信资源、外设资源，如摄像头、位置传感器等）。

注：ST 作者宜根据具体的应用情况细化对资产的描述。

5.2 安全威胁

5.2.1 数据传输窃听（T.EAVESDROP）

恶意用户或进程可能监听或修改移动终端操作系统之间或者移动终端操作系统与远程可信 IT 产品间传递的用户数据或 TSF 数据。

5.2.2 安全功能失效（T.TSF_COMPROMISE）

恶意用户或进程通过攻击手段非法地浏览、修改或删除 TSF 数据或可执行代码。这可能让恶意用户或进程获得移动终端操作系统的配置信息，或可能导致移动终端操作系统的安全功能对于数据资产保护的安全机制不再正常工作。

5.2.3 授权用户恶意行为（T.ACCESS_MALICIOUS）

授权用户因安全意识薄弱或误操作，对移动终端操作系统进行不正确地配置，或授权用户恶意利用权限进行非法操作，使移动终端安全受到威胁。

5.2.4 非授权网络流量（T.UNAUTHORIZED_NETFLOW）

未授权外部 IT 实体向移动终端操作系统发送网络数据或接收经由移动终端操作系统传输的网络数据。

5.2.5 残余信息利用（T.RESIDUAL_DATA）

恶意用户或进程可能利用移动终端操作系统残留信息的处理缺陷，在执行过程中对未删除的残留信息进行利用，以获取敏感信息或滥用移动终端操作系统的安全功能。

5.2.6 恶意软件（T.MALICIOUSAPP）

恶意软件可能通过伪装成授权应用或进程访问用户数据和系统敏感资源。

5.2.7 非授权访问（T.UNAUTHORIZED_ACCESS）

非授权用户或进程访问移动终端操作系统的安全功能数据和用户数据，并对安全功能数据和用户数据进行恶意操作。

5.2.8 重放攻击（T.REPLAY）

非授权用户利用所截获的授权用户信息，重新提交给移动终端操作系统，以假冒授权用户访问移动

终端操作系统的功能和数据。

5.2.9 会话冒用(T.UNATTENDED_SESSION)

非授权用户可以利用不被使用的会话,假冒授权用户对移动终端操作系统的功能和数据产生威胁。

5.2.10 设备丢失(T.LOST)

移动终端操作系统所运行的物理设备在被出售、交换、遗失的情况下,非授权用户可通过攻击方式获取授权用户数据。

5.3 组织安全策略

组织应为移动终端操作系统提供敏感数据加密存储和通讯功能的密码策略。

5.4 假设

5.4.1 物理安全(A.PHYSICAL)

假设移动终端操作系统所依赖的运行环境能提供移动终端操作系统安全运行所需的物理安全保护。

5.4.2 人员(A.PERSONNEL)

假设移动终端操作系统的合法用户能按照管理员指南来管理移动终端操作系统的安全功能,对移动终端操作系统不存在恶意的破坏企图。

5.4.3 远程设备安全(A.REMOTE)

假定用于管理移动终端操作系统的远程 IT 设备、应用设备是安全的。

6 安全目的

6.1 移动终端操作系统安全目的

6.1.1 事件审计(O.AUDIT)

移动终端操作系统应记录安全相关的事件,应对记录的事件进行保护并且只允许授权用户查看。移动终端操作系统应保证审计迹已满的情况下,不影响审计功能和其他安全功能的执行。

6.1.2 身份认证(O.AUTH)

移动终端操作系统应提供鉴别用户身份的机制,并且在用户使用移动终端操作系统功能前对用户身份进行鉴别和标识。移动终端操作系统应只提供有限的鉴权反馈信息,并且在鉴权失败达到一定次数时限制用户的鉴权行为。

6.1.3 数据加密(O.ENCRYPT)

移动终端操作系统应提供加解密机制,保证移动终端操作系统能对其保护的数据采取加密措施。

6.1.4 残留信息清除(O.RESIDUAL_INFO)

移动终端操作系统应保证重要的数据在使用完成后会被删除或被安全处理,不会留下可被攻击者利用的残留数据信息。

6.1.5 可信信道(O.TRUSTED_CHANNEL)

移动终端操作系统应提供通过受保护的通道向远程可信 IT 产品提交数据的能力,同时也提供受保护的网络通道供应用使用。

6.1.6 网络数据流控制(O.NETWORK_FLOW)

移动终端操作系统应提供基本的网络防护能力,阻止已知的恶意网络攻击行为。移动终端操作系统应当控制移动终端操作系统内的 IT 实体和外部 IT 实体之间的 IP 网络数据和移动通信网络数据传输。移动终端操作系统控制这些数据传输的规则只能通过授权用户来改变。

6.1.7 访问控制(O.ACCESS_CONTROL)

移动终端操作系统应提供访问控制机制,防止移动终端操作系统重要数据、进程及资源等在未授权情况下被访问、修改或删除。

6.1.8 会话管理(O.SESSION_MANAGEMENT)

移动终端操作系统应临时暂停不被使用的用户会话,并且只有在重新验证用户身份后才恢复已暂停的用户会话。

6.1.9 资源限制(O.RESOURCE_QUOTA)

移动终端操作系统应提供移动终端操作系统资源使用的控制机制,防止因应用程序错误或恶意行为无限制消耗资源,导致系统资源被耗尽。

6.1.10 数据回滚(O.ROLLBACK)

移动终端操作系统应提供用户关键数据备份和回滚的功能,保证用户数据能回到一个备份过的状态。这种行为要求应是授权用户,并应保证用户数据的安全性。

6.1.11 安全管理(O.MANAGE)

移动终端操作系统应划分不同用户角色来管理移动终端操作系统,并对角色赋予的权限进行限制,防止授权用户的权限滥用。

6.1.12 可信时间(O.TIME)

移动终端操作系统应提供设置或获取可信时间的功能,保证系统时间是由授权用户设定或者是从可靠的时钟源同步获得。

6.1.13 丢失保护(O.LOST_PROTECT)

移动终端操作系统应提供丢失保护机制。保证在物理终端丢失的情况下授权用户对用户敏感数据的控制。

6.2 环境安全目的

6.2.1 物理安全(OE.PHYSICAL)

移动终端操作系统的运行环境可提供操作系统运行所需的物理安全保护。

6.2.2 人员(OE.PERSONNEL)

负责管理移动终端操作系统安全策略和数据的用户是可信的,经过学习和培训的,并且对管理和操作行为负责。

6.2.3 远程通信(OE.REMOTE)

移动终端操作系统的远程管理设备、应用商店等远程 IT 实体是安全的且其数据和用户信息是被保护的。

7 安全要求

7.1 安全功能要求

7.1.1 概述

移动终端操作系统的安全功能要求由 GB/T 18336.2—2015 规定的组件构成,移动终端操作系统的安全功能要求组件见表 1,7.1.2～7.1.10 对各组件给出了说明。

表 1 安全功能要求组件

组件分类	安全功能要求组件
FAU 类:安全审计	FAU_GEN.1 审计数据产生
	FAU_GEN.2 用户身份关联
	FAU_STG.1 受保护的审计迹存储
	FAU_STG.4 防止审计数据丢失
FCS 类:密码支持	FCS_CKM.1 密钥生成
	FCS_COP.1 密码运算
FDP 类:用户数据保护	FDP_ACC.1 子集访问控制
	FDP_ACF.1 基于安全属性的访问控制
	FDP_ETC.1 不带安全属性的用户数据输出
	FDP_ETC.2 带有安全属性的用户数据输出
	FDP_IFC.1 子集信息流控制
	FDP_IFF.1 简单安全属性
	FDP_ITC.1 不带安全属性的用户数据输入
	FDP_ITC.2 带有安全属性的用户数据输入
	FDP_RIP.1 子集残余信息保护
	FDP_ROL.1 基本回退
	FDP_UCT.1 基本的数据交换机密性
	FDP_UIT.1 数据交换完整性

表 1（续）

组件分类	安全功能要求组件
FIA 类：标识和鉴别	FIA_AFL.1 鉴别失败处理
	FIA_ATD.1 用户属性定义
	FIA_SOS.1 秘密的验证
	FIA_UAU.1 鉴别的时机
	FIA_UAU.5 多重鉴别机制
	FIA_UAU.6 重鉴别
	FIA_UAU.7 受保护的鉴别反馈
	FIA_UID.1 标识的时机
	FIA_USB.1 用户-主体绑定
FMT 类：安全管理	FMT_MOF.1 安全功能行为的管理
	FMT_MSA.1 安全属性的管理
	FMT_MSA.2 安全的安全属性
	FMT_MSA.3 静态属性初始化
	FMT_MTD.1 TSF 数据的管理
	FMT_MTD.2 TSF 数据限值的管理
	FMT_MTD.3 安全的 TSF 数据
	FMT_SMF.1 管理功能规范
	FMT_SMR.1 安全角色
FPT 类：TSF 保护	FPT_FLS.1 失效即保持安全状态
	FPT_ITC.1 传送过程中 TSF 间的机密性
	FPT_ITI.1 TSF 间篡改的检测
	FPT_STM.1 可靠的时间戳
	FPT_TDC.1 TSF 间基本的 TSF 数据一致性
	FPT_TST.1 TSF 测试
FRU 类：资源利用	FRU_RSA.1 最高配额
FTA 类：TOE 访问	FTA_SSL.1 TSF 原发会话锁定
	FTA_SSL.2 用户原发会话锁定
FTP 类：可信路径/信道	FTP_ITC.1 TSF 间可信信道

7.1.2 安全审计（FAU 类）

7.1.2.1 审计数据产生（FAU_GEN.1）

从属于：无其他组件。

依赖关系：FPT_STM.1 可信时间戳。

FAU_GEN.1.1 TSF 应能为下述可审计事件产生审计记录：

a) 审计功能的开启和关闭；

b) 有关最小级审计级别的所有可审计事件；

c) 可审计事件包括【赋值：其他影响移动终端操作系统运行状态的可审计事件】。

FAU_GEN.1.2 TSF 应在每个审计记录中至少记录下列信息：

a) 事件的日期和时间、事件类型、主体身份、事件的结果；

b) 对每种审计事件类型，基于 ST 中功能组件的可审计事件定义，【赋值：其他审计相关信息】。

7.1.2.2 用户身份关联(FAU_GEN.2)

从属于：无其他组件。

依赖关系：FAU_GEN.1 审计数据产生；

FIA_UID.2 任何动作前的用户标识。

FAU_GEN.2.1 对于已标识身份的用户的行为所产生的审计事件，TSF 应能将每个可审计事件与引起该事件的用户身份相关联。

7.1.2.3 受保护的审计迹存储(FAU_STG.1)

从属于：无其他组件。

依赖关系：FAU_GEN.1 审计数据产生。

FAU_STG.1.1 TSF 应保护所存储的审计记录，以避免未授权的删除。

FAU_STG.1.2 TSF 应能防止对审计迹中所存审计记录的未授权修改。

7.1.2.4 防止审计数据丢失(FAU_STG.4)

从属于：FAU_STG.3 审计数据可能丢失时的行为。

依赖关系：FAU_STG.1 受保护的审计迹存储。

FAU_STG.4.1 如果审计迹已满，TSF 应【选择，选取一个：忽略可审计事件、“阻止可审计事件，除非具有特权的授权用户产生的审计事件”、覆盖所存储的最早的审计记录】和【赋值：审计存储失效时所采取的其他动作】。

7.1.3 密码支持(FCS 类)

7.1.3.1 密钥生成(FCS_CKM.1)

从属于：无其他组件。

依赖关系：FCS_COP.1 密钥运算；

FCS_CKM.4 密钥销毁。

FCS_CKM.1.1 TSF 应根据符合下列标准【赋值：国家、行业或组织要求的密码管理相关标准或规范】的一个特定的密钥生成算法【赋值：密钥生成算法】和规定的密钥长度【赋值：密钥长度】来生成密钥。

注：若密钥由外部环境生成，则可以不选择此组件。该组件仅适用于由移动终端操作系统本身完成的情况，此时 ST 作者宜根据密码算法的具体情况，赋值评估对象用户单位主管部门认可的相关标准及参数。

7.1.3.2 密码运算(FCS_COP.1)

从属于：无其他组件。

依赖关系：[FDP_ITC.1 不带安全属性的用户数据输入，或

FCS_CKM.1 密钥生成]；

FCS_CKM.4 密钥销毁。

FCS_COP.1.1 TSF 应根据符合下列标准【赋值：国家、行业或组织要求的密码管理相关标准或规范】的特定的密码算法【赋值：密码算法】和密钥长度【赋值：密钥长度】来执行【赋值：密码运算列表】。

注：密码运算可用于支持一个或多个移动终端操作系统的安全服务，本组件可根据需要重复多次，这取决于：

a) 不同密码算法或密钥长度的使用；

b) 所运算数据的类型或敏感度。ST 作者宜根据密码算法的具体情况赋值国家、行业或组织主管部门认可的相关标准及参数。

7.1.4 用户数据保护（FDP 类）

7.1.4.1 子集访问控制（FDP_ACC.1）

从属于：无其他组件。

依赖关系：FDP_ACF.1 基于安全属性的访问控制。

FDP_ACC.1.1 TSF 应对【赋值：主体、客体及 SFP 所涵盖主体和客体之间的操作列表】执行【赋值：访问控制策略】。

7.1.4.2 基于安全属性的访问控制（FDP_ACF.1）

从属于：无其他组件。

依赖关系：FDP_ACC.1 子集访问控制。

FDP_ACF.1.1 TSF 应基于【赋值：指定 SFP 控制下的主体和客体列表，以及每个对应的 SFP 相关安全属性或 SFP 相关安全属性的已命名组】对客体执行【赋值：访问控制 SFP】。

FDP_ACF.1.2 TSF 应执行以下规则，以决定在受控主体与受控客体间的一个操作是否被允许：【赋值：在受控主体和受控客体间，通过对受控客体采取受控操作来管理访问的一些规则】。

FDP_ACF.1.3 TSF 应基于以下附加规则【赋值：基于安全属性，明确授权主体访问客体的一些规则】，明确授权主体访问客体。

FDP_ACF.1.4 TSF 应基于【赋值：基于安全属性，明确拒绝主体访问客体的一些规则】，明确拒绝主体访问客体。

7.1.4.3 不带安全属性的用户数据输出（FDP_ETC.1）

从属于：无其他组件。

依赖关系：FDP_ACC.1 子集访问控制，或

FDP_IFC.1 子集信息流控制。

FDP_ETC.1.1 在安全功能策略控制下将用户数据输出到移动终端操作系统之外时，TSF 应执行【赋值：访问控制 SFP 和/或信息流控制 SFP】。

FDP_ETC.1.2 TSF 应输出用户数据但不带用户数据关联的安全属性。

7.1.4.4 带有安全属性的用户数据输出（FDP_ETC.2）

从属于：无其他组件。

依赖关系：FDP_ACC.1 子集访问控制，或

FDP_IFC.1 子集信息流控制。

FDP_ETC.2.1 在安全功能策略控制下将用户数据输出到移动终端操作系统之外时，TSF 应执行【赋值：访问控制 SFP 和/或信息流控制 SFP】。

FDP_ETC.2.2 TSF 应输出用户数据且带有用户数据关联的安全属性。

FDP_ETC.2.3 TSF 应确保输出安全属性到移动终端操作系统之外时，与所输出的用户数据确切关联。

FDP_ETC.2.4 当从移动终端操作系统输出用户数据时，TSF 应执行下列规则【赋值：附加的输出控制规则】。

7.1.4.5 子集信息流控制（FDP_IFC.1）

从属于：无其他组件。

依赖关系：FPT_IFF.1 简单安全属性。

FDP_IFC.1.1 TSF 应对【赋值：移动终端处理或传输的信息流，如：IP 数据报文、语音呼叫请求、短信息数据】执行【信息流控制策略】。

7.1.4.6 简单安全属性（FDP_IFF.1）

从属于：无其他组件。

依赖关系：FDP_IFC.1 子集信息流控制。

FDP_IFF.1.1 TSF 应基于下列类型主体和信息的安全属性：【赋值：指定 SFP 控制下的主体和信息列表，以及每个对应的安全属性】执行【赋值：信息流控制 SFP】；

FDP_IFF.1.2 如果支持下列规则：【赋值：对每一个操作，主体和信息的安全属性之间应支持基于安全属性的关系】，TSF 应允许信息在受控主体和受控信息之间经由受控操作流动；

FDP_IFF.1.3 TSF 应执行【赋值：附加的信息流控制 SFP 规则】；

FDP_IFF.1.4 TSF 应下列【赋值：附加的 SFP 能力列表】；

FDP_IFF.1.5 TSF 应根据下列规则：【赋值：基于安全属性，明确批准信息流的规则】明确批准一个信息流；

FDP_IFF.1.6 TSF 应根据下列规则：【赋值：基于安全属性，明确拒绝信息流的规则】明确拒绝一个信息流。

7.1.4.7 不带安全属性的用户数据输入（FDP_ITC.1）

从属于：无其他组件。

依赖关系：[FDP_ACC.1 子集访问控制，或
FDP_IFC.1 子集信息流控制]；
FMT_MSA.3 静态属性初始化。

FDP_ITC.1.1 在安全功能策略控制下从移动终端操作系统之外输入用户数据时，TSF 应执行【赋值：访问控制 SFP 和/或信息流控制 SFP】。

FDP_ITC.1.2 从移动终端操作系统外部输入用户数据时，TSF 应忽略任何与用户数据相关的安全属性。

FDP_ITC.1.3 在 SFP 控制下从移动终端操作系统之外输入用户数据时，TSF 应执行下面的规则：【赋值：附加的输入控制规则】。

7.1.4.8 带有安全属性的用户数据输入（FDP_ITC.2）

从属于：无其他组件。

依赖关系：[FDP_ACC.1 子集访问控制，或

FDP_IFC.1 子集信息流控制]；

FDP_ITC.1 TSF 间的可信信道；

FPT_TDC.1 TSF 间基本的 TSF 数据一致性。

FDP_ITC.2.1 在安全功能策略控制下从移动终端操作系统之外输入用户数据时，TSF 应执行【赋值：访问控制 SFP 和/或信息流控制 SFP】。

FDP_ITC.2.2 TSF 应使用与锁输入数据相关的安全属性。

FDP_ITC.2.3 TSF 应确保所使用的协议在安全属性和接收到的用户数据之间进行了明确的关联。

FDP_ITC.2.4 TSF 应确保对所输入用户数据的安全属性的解释与用户源数据所预期的安全属性是一样的。

FDP_ITC.2.5 当在 SFP 控制下从移动终端操作系统之外输入用户数据时，TSF 应执行【赋值：附加的输入控制规则】。

7.1.4.9 子集残余信息保护(FDP_RIP.1)

从属于：无其他组件。

依赖关系：无依赖关系。

FDP_RIP.1.1 TSF 应确保一个资源的任何先前信息内容，在【选择：分配资源到、释放资源自】下列客体：【赋值：客体列表】时不再可用。

7.1.4.10 基本回退(FDP_ROL.1)

从属于：无其他组件。

依赖关系：FDP_ACC.1 子集访问控制。

FDP_ROL.1.1 TSF 应执行【自主访问控制和强制访问控制】，以允许对【赋值：用户数据及配置数据】的【修改】进行回退。

FDP_ROL.1.2 TSF 应允许用户对【赋值：用户数据及配置数据】【选择：基于时间、其他可选择的条件】进行回退操作。

7.1.4.11 基本的数据交换机密性(FDP_UCT.1)

从属于：无其他组件。

依赖关系：FTP_ITC.1 TSF 间的可信信道；

[FDP_ACC.1 子集访问控制，或

FDP_IFC.1 子集信息流控制]

FDP_UCT.1.1 TSF 应执行【赋值：访问控制 SFP 和/或信息流控制 SFP】，以便能【选择：传送、接收】用户数据，并保护其免遭未授权泄露。

7.1.4.12 数据交换完整性(FDP_UIT.1)

从属于：无其他组件。

依赖关系：FDP_ACC.1 子集访问控制；

FTP_ITC.1 TSF 间的可信信道。

FDP_UIT.1.1 TSF 应执行【访问控制策略】，以便能【选择：传送、接收】用户数据，并保护数据避免带来【选择：篡改、删除、插入、重放】错误。

FDP_UIT.1.2 TSF 应能判断用户数据的接收过程，是否发生了【选择：篡改、删除、插入、重放】。

7.1.5 标识和鉴别(FIA 类)

7.1.5.1 鉴别失败处理(FIA_AFL.1)

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

FIA_AFL.1.1 TSF 应检测发生【赋值:错误次数】与【身份鉴别】相关的未成功鉴别尝试;

FIA_AFL.1.2 当不成功鉴别尝试的指定次数达到所定义的未成功鉴别尝试次数时,TSF 应采取【选择:延时登录、锁定终端、【赋值:其他保护措施】】。

7.1.5.2 用户属性定义(FIA_ATD.1)

7.1.5.2.1 用户属性定义[FIA_ATD.1(1)](终端操作用户)

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_ATD.1(1).1 TSF 应维护属于单个用户的下列安全属性列表:【用户标识、用户鉴权信息】。

7.1.5.2.2 用户属性定义[FIA_ATD.1(2)](应用程序)

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_ATD.1(2).1 TSF 应维护属于单个用户的下列安全属性列表:【应用标识、应用鉴权信息】。

7.1.5.2.3 用户属性定义[FIA_ATD.1(3)](远程管理用户)

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_ATD.1(3).1 TSF 应维护属于单个用户的下列安全属性列表:【用户标识、用户鉴权信息】。

7.1.5.3 秘密的验证(FIA_SOS.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_SOS.1.1 TSF 应提供一种机制以验证秘密满足【选择:

a) 口令形式:字符不少于【赋值:正整数】,并且满足【赋值:字符和数字组合的规则】;

b) 其他秘密形式:【赋值:其他验证方式】】。

7.1.5.4 鉴别的时机(FIA_UAU.1)

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

FIA_UAU.1.1 在用户被鉴别前,TSF 应允许执行代表用户的以下行为:

a) 显示消息状态;

b) 显示未接来电;

c) 显示时间/日期信息;

d) 显示移动终端状态信息;

e) 显示移动用户信息(如:运营商信息等);

f) 显示某些通知(低电量通知等);
g) 输入鉴别数据;
h) 拨打紧急电话;
i) 接收来电;
j) 接收短信息;
k) 【赋值:其他 TSF 促成的动作列表】。

FIA_UAU.1.2 在允许执行代表该用户的任何其他由 TSF 促成的动作前,TSF 应要求每个用户都已被成功鉴别。

7.1.5.5 多重鉴别机制(FIA_UAU.5)

从属于:无其他组件。
依赖关系:无依赖关系。

FIA_UAU.5.1 TSF 应提供【选择:口令、指纹、图案、【赋值:ST 作者提供的其他鉴别机制】】以支持用户鉴别。

FIA_UAU.5.2 TSF 应根据【选择:口令匹配、指纹匹配、图案匹配、【赋值:ST 作者提供的其他鉴别规则】】鉴别任何用户所声称的身份。

7.1.5.6 重鉴别(FIA_UAU.6)

从属于:无其他组件。
依赖关系:无依赖关系。

FIA_UAU.6.1 TSF 应在:【选择:用户变更鉴权信息、【赋值:其他需要鉴别的时机】】条件下重新鉴别用户。

7.1.5.7 受保护的鉴别反馈(FIA_UAU.7)

从属于:无其他组件。
依赖关系:FIA_UAU.1 鉴别的时机。

FIA_UAU.7.1 终端操作用户身份鉴别进行时,TSF 应仅向用户提供受保护的鉴别反馈:
a) 口令解锁时反馈为占位符;
b) 图案解锁时不反馈解锁图案路径;
c) 【赋值:其他受保护的鉴别反馈方式】。

7.1.5.8 标识的时机(FIA_UID.1)

从属于:无其他组件。
依赖关系:无依赖关系。

FIA_UID.1.1 在应用程序被识别之前,TSF 应允许执行应用程序的安装。

FIA_UID.1.2 在允许执行代表该用户的任何其他 TSF 仲裁动作之前,TSF 应要求每个应用程序都已被成功识别。

注:应用程序安装成功后,移动终端操作系统为应用程序分配唯一代表其身份的标识。

7.1.5.9 用户-主体绑定(FIA_USB.1)

7.1.5.9.1 用户-主体绑定[FIA_USB.1(1)](终端操作用户)

从属于:无其他组件。

依赖关系：FIA_ATD.1 用户属性定义。

FIA_USB.1.1(1) TSF 应将下列用户安全属性：【用户标识、鉴权信息】与代表用户活动的主体相关联；

FIA_USB.1.2(1) TSF 应对用户安全属性与代表用户活动的主题初始关联关系执行下列规则【赋值：属性初始关联规则】；

FIA_USB.1.3(1) TSF 应执行下列规则管理与代表用户活动的主体见的关联关系的变化：【赋值：属性更改规则】。

7.1.5.9.2 用户-主体绑定[FIA_USB.1(2)](应用程序)

从属于：无其他组件。

依赖关系：FIA_ATD.1 用户属性定义。

FIA_USB.1.1(2) TSF 应将下列用户安全属性：【赋值：应用标识、应用鉴权信息】与代表用户活动的主体相关联；

FIA_USB.1.2(2) TSF 应对用户安全属性与代表用户活动的主题初始关联关系执行下列规则【赋值：属性初始关联规则】；

FIA_USB.1.3(2) TSF 应执行下列规则管理与代表用户活动的主体见的关联关系的变化：【赋值：属性更改规则】。

7.1.5.9.3 用户-主体绑定[FIA_USB.1(3)](远程管理用户)

从属于：无其他组件。

依赖关系：FIA_ATD.1 用户属性定义。

FIA_USB.1.1(3) TSF 应将下列用户安全属性：【赋值：用户标识、用户鉴权信息】与代表用户活动的主体相关联；

FIA_USB.1.2(3) TSF 应对用户安全属性与代表用户活动的主题初始关联关系执行下列规则【赋值：属性初始关联规则】；

FIA_USB.1.3(3) TSF 应执行下列规则管理与代表用户活动的主体见的关联关系的变化：【赋值：属性更改规则】。

7.1.6 安全管理(FMT 类)

7.1.6.1 安全功能行为的管理(FMT_MOF.1)

从属于：无其他组件。

依赖关系：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MOF.1.1 TSF 应仅限于【授权用户】对功能【赋值：定义的管理功能列表】具有【赋值：操作动作】的能力。

7.1.6.2 安全属性的管理(FMT_MSA.1)

从属于：无其他组件。

依赖关系：[FDP_ACC.1 子集访问控制，或

FDP_IFC.1 子集信息流控制]；

FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MSA.1.1 TSF 应执行【赋值：访问控制 SFP、信息流控制 SFP】，以仅限于【赋值：已标识的授权角色】能对安全属性【赋值：安全属性列表】进行【选择：改变默认值、查询、修改、删除、【赋值：其他操作】】。

7.1.6.3 安全的安全属性（FMT_MSA.2）

从属于：无其他组件。

依赖关系：ADV_SPM.1 非形式化的 TOE 安全策略模型；

[FDP_ACC.1 子集访问控制，或

FDP_IFC.1 子集信息流控制]；

FMT_MSA.1 安全属性的管理；

FMT_SMR.1 安全角色。

FMT_MSA.2.1 TSF 应确保安全属性【赋值：安全属性列表】只接受安全的值。

7.1.6.4 静态属性初始化（FMT_MSA.3）

从属于：无其他组件。

依赖关系：FMT_MSA.1 安全属性的管理；

FMT_SMR.1 安全角色。

FMT_MSA.3.1 TSF 应执行【赋值：访问控制 SFP、信息流控制 SFP】，以便为用于执行 SFP 的安全属性提供【选择，从中选取一个：受限的、许可的、【赋值：其他特性】】默认值。

FMT_MSA.3.2 TSF 应允许【赋值：已标识的授权角色】在创建客体或信息时指定替换性的初始值以代替原来的默认值。

7.1.6.5 TSF 数据的管理（FMT_MTD.1）

从属于：无其他组件。

依赖关系：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MTD.1.1 TSF 应仅限于【授权用户】能对【赋值：TSF 数据列表】【选择：查询、修改、删除、【赋值：其他的数据管理操作】】。

7.1.6.6 TSF 数据限值的管理（FMT_MTD.2）

从属于：无其他组件。

依赖关系：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MTD.2.1 TSF 应仅限于【赋值：已标识的授权角色】规定【赋值：TSF 数据列表】的限值。

FMT_MTD.2.2 如果 TSF 数据达到或超过了设定的限值，TSF 应采取下面的动作：【赋值：要采取的动作】。

7.1.6.7 安全的 TSF 数据（FMT_MTD.3）

从属于：无其他组件。

依赖关系：FMT_MTD.1 TSF 数据的管理。

FMT_MTD.3.1 TSF 应确保 TSF 数据【赋值：TSF 数据列表】只接受安全的值。

7.1.6.8 管理功能规范(FMT_SMF.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FMT_SMF.1.1 TSF 应能执行如下安全管理功能【赋值:安全管理功能列表】。其中【赋值:远程管理功能列表】只能由远程管理员执行;【赋值:远程管理功能】可以由远程管理员执行;其他功能由终端操作员执行。

7.1.6.9 安全角色(FMT_SMR.1)

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

FMT_SMR.1.1 TSF 应维护角色【赋值:已标识的授权角色】。

FMT_SMR.1.2 TSF 应能把用户和角色关联起来。

7.1.7 TSF 保护(FPT 类)

7.1.7.1 失效即保持安全状态(FPT_FLS.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_FLS.1.1 TSF 在下列失效发生时应保持一种安全状态【赋值:TSF 的失效类型列表】。

7.1.7.2 传送过程中 TSF 间的机密性(FPT_ITC.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_ITC.1.1 TSF 应保护所有从 TSF 传送到另一个可信 IT 产品的 TSF 数据在传送过程中不会被未授权泄漏。

7.1.7.3 TSF 间篡改的检测(FPT_ITI.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_ITI.1.1 TSF 应提供能力,以检测在下列度量下:【赋值:一个既定的修改度量】TSF 与另一个可信 IT 产品间所传送的所有 TSF 数据是否被修改。

FPT_ITI.1.2 TSF 应提供能力,以验证 TSF 与另一个可信 IT 产品间所传送的所有 TSF 数据的完整性,以及如果检测到修改将执行【赋值:采取的动作】。

7.1.7.4 可靠的时间戳(FPT_STM.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_STM.1.1 TSF 应能为它自己的使用提供可靠的时间戳,这个时间的来源【赋值:时间获取的方式】。

7.1.7.5 TSF 间基本的 TSF 数据一致性(FPT_TDC.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_TDC.1.1 当 TSF 与其他可信 IT 产品共享 TSF 数据时,TSF 应提供对【赋值:TSF 数据类型列表】进行一致性解释的能力。

FPT_TDC.1.2 当解释来自其他可信 IT 产品的 TSF 数据时,TSF 应使用【赋值:TSF 使用的解释规则列表】。

7.1.7.6 TSF 测试(FPT_TST.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_TST.1.1 TSF 应在【选择:初始化启动期间、正常工作期间周期性地、在【赋值:产生自检的条件】条件时】运行一套自检程序以证明【选择:【赋值:TSF 的组成部分】、TSF】运行的正确性。

FPT_TST.1.2 TSF 应为授权用户提供验证【选择:【赋值:TSF 的组成部分】、TSF 数据】完整性的能力。

FPT_TST.1.3 TSF 应为授权用户提供验证所存储的 TSF 可执行代码完整性的能力。

7.1.8 资源利用(FRU 类)

最高配额(FRU_RSA.1)

从属于:无其他组件。

依赖关系:无依赖关系。

FRU_RSA.1.1 TSF 应对以下资源【选择:存储空间、内存、带宽、【赋值:ST 定义指定的资源列表】】分配最高配额,以便【赋值:主体列表】能【选择:同时、在规定的时间间隔内】使用。

7.1.9 TOE 访问(FTA 类)

7.1.9.1 TSF 原发会话锁定(FTA_SSL.1)

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

FTA_SSL.1.1 TSF 应在达到【赋值:用户不活动的时间间隔】后,通过以下方式锁定一个交互式会话:

a) 清除或覆写显示设备,使当前的内容不可读;

b) 除了会话解锁活动之外,终止用户数据存取/显示设备的任何活动,但允许短信数据写入,允许电话呼入并显示来电信息界面且在通话结束后应恢复锁定,允许使用相机,【赋值:其他允许的操作】。

FTA_SSL.1.2 TSF 应要求在解锁会话之前成功地完成对终端用户的鉴别。

7.1.9.2 用户原发会话锁定(FTA_SSL.2)

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

FTA_SSL.2.1 TSF 应允许移动终端用户通过【赋值:锁定方式列表】实现对自己拥有的交互会话进

行用户原发锁定：

a） 清除或覆写显示设备，使当前的内容不可读；

b） 除了会话解锁活动之外，终止用户数据存取/显示设备的任何活动，但允许短信数据写入，允许电话呼入并显示来电信息界面且在通话结束后应恢复锁定，允许使用相机，【赋值：其他允许的操作】。

FTA_SSL.2.2 TSF 应要求在解锁会话之前成功地完成对终端用户的鉴别。

7.1.10 可信路径/信道（FTP 类）

TSF 间可信信道（FTP_ITC.1）

从属于：无其他组件。

依赖关系：无依赖关系。

FTP_ITC.1.1 TSF 应在它自己和一个远程可信 IT 产品之间提供一条通信信道，此信道在逻辑上与其他通信信道截然不同，其端点是具有保证标识，并且能保护数据免遭修改或泄露。

FTP_ITC.1.2 TSF 应允许【选择：TSF、【赋值：ST 作者指定的另一个可信 IT 产品】】经由可信信道发起通信。

FTP_ITC.1.3 对于【赋值：需要可信信道的功能列表】，TSF 应经由可信信道发起通信。

7.2 安全保障要求

7.2.1 概述

移动终端操作系统的安全保障要求由 GB/T 18336.3—2015 规定的安全保障组件组成，移动终端操作系统 EAL2、EAL3 和 EAL4 保障级的安全保障要求组件见表 2，7.2.2 至 7.2.7 对各组件给出了说明。

表 2 安全保障要求组件

保障类	保障组件	备注		
		EAL2	EAL3	EAL4
开发	ADV_ARC.1 安全架构描述	√	√	√
	ADV_FSP.2 安全执行功能规范	√	—	—
	ADV_FSP.3 带完整摘要的功能规范	—	√	—
	ADV_FSP.4 完备的功能规范	—	—	√
	ADV_IMP.1 TSF 实现表示	—	—	√
	ADV_TDS.1 基础设计	√	—	—
	ADV_TDS.2 结构化设计	—	√	—
	ADV_TDS.3 基础模块设计	—	—	√
指导性文档	AGD_OPE.1 操作用户指南	√	√	√
	AGD_PRE.1 准备程序	√	√	√

表 2（续）

保障类	保障组件	备注		
		EAL2	EAL3	EAL4
生命周期支持	ALC_CMC.2 CM 系统的使用	√	—	—
	ALC_CMC.3 授权控制	—	√	—
	ALC_CMC.4 生产支持和接受程序及其自动化	—	—	√
	ALC_CMS.2 部分 TOE CM 覆盖	√	—	—
	ALC_CMS.3 实现表示 CM 覆盖	—	√	—
	ALC_CMS.4 问题跟踪 CM 覆盖	—	—	√
	ALC_DEL.1 交付程序	√	√	√
	ALC_DVS.1 安全措施标识	—	√	√
	ALC_LCD.1 开发者定义的生命周期模型	—	√	√
	ALC_TAT.1 明确定义的开发工具	—	—	√
安全目标评估	ASE_CCL.1 符合性声明	√	√	√
	ASE_ECD.1 扩展组件定义	√	√	√
	ASE_INT.1 ST 引言	√	√	√
	ASE_OBJ.2 安全目的	√	√	√
	ASE_REQ.2 推导出的安全要求	√	√	√
	ASE_SPD.1 安全问题定义	√	√	√
	ASE_TSS.1 TOE 概要规范	√	√	√
测试	ATE_COV.1 覆盖证据	√	—	—
	ATE_COV.2 覆盖分析	—	√	√
	ATE_DPT.1 测试：基本设计	—	√	—
	ATE_DPT.2 测试：安全执行模块	—	—	√
	ATE_FUN.1 功能测试	√	√	√
	ATE_IND.2 独立测试——抽样	√	√	√
脆弱性评估	AVA_VAN.2 脆弱性分析	√	√	—
	AVA_VAN.3 关注点脆弱性分析	—	—	√

7.2.2 开发（ADV 类）

7.2.2.1 安全架构描述（ADV_ARC.1）

依赖关系：ADV_FSP.1 基本功能规范；

ADV_TDS.1 基础设计。

开发者行为元素：

ADV_ARC.1.1D 开发者应设计并实现移动终端操作系统，确保 TSF 的安全特性不可旁路。

ADV_ARC.1.2D 开发者应设计并实现 TSF，以防止不可信主体的破坏。

ADV_ARC.1.3D 开发者应提供 TSF 安全架构描述。

内容和形式元素：

ADV_ARC.1.1C 安全架构的描述应与在移动终端操作系统设计文档中对 SFR-执行的抽象描述的级别一致。

ADV_ARC.1.2C 安全架构的描述应描述与安全功能要求一致的 TSF 安全域。

ADV_ARC.1.3C 安全架构的描述应描述 TSF 初始化过程为何是安全的。

ADV_ARC.1.4C 安全架构的描述应证实 TSF 可防止被破坏。

ADV_ARC.1.5C 安全架构的描述应证实 TSF 可防止 SFR-执行的功能被旁路。

评估者行为元素：

ADV_ARC.1.1E 评估者应确认提供的信息符合证据的内容和形式要求。

7.2.2.2 安全执行功能规范(ADV_FSP.2)

依赖关系：ADV_TDS.1 基础设计。

开发者行为元素：

ADV_FSP.2.1D 开发者应提供一个功能规范。

ADV_FSP.2.2D 开发者应提供功能规范到安全功能要求的追溯。

内容和形式元素：

ADV_FSP.2.1C 功能规范应完全描述 TSF。

ADV_FSP.2.2C 功能规范应描述所有 TSFI 的目的和使用方法。

ADV_FSP.2.3C 功能规范应识别和描述每个 TSFI 相关的所有参数。

ADV_FSP.2.4C 对于每个 SFR-执行 TSFI，功能规范应描述 TSFI 相关的 SFR-执行行为。

ADV_FSP.2.5C 对于 SFR-执行 TSFI，功能规范应描述由 SFR-执行行为相关处理而引起的直接错误消息。

ADV_FSP.2.6C 功能规范应证实安全功能要求到 TSFI 的追溯。

评估者行为元素：

ADV_FSP.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV_FSP.2.2E 评估者应确定功能规范是安全功能要求的一个准确且完备的实例化。

7.2.2.3 带完整摘要的功能规范(ADV_FSP.3)

依赖关系：ADV_TDS.1 基础设计。

开发者行为元素：

ADV_FSP.3.1D 开发者应提供一个功能规范。

ADV_FSP.3.2D 开发者应提供功能规范到安全功能要求的追溯。

内容和形式元素：

ADV_FSP.3.1C 功能规范应完全描述 TSF。

ADV_FSP.3.2C 功能规范应描述所有 TSFI 的目的和使用方法。

ADV_FSP.3.3C 功能规范应识别和描述每个 TSFI 相关的所有参数。

ADV_FSP.3.4C 对于每个 SFR-执行 TSFI，功能规范应描述 TSFI 相关的 SFR-执行行为。

ADV_FSP.3.5C 对于 SFR-执行 TSFI，功能规范应描述与 TSFI 的调用相关的安全实施行为和异常而引起的直接错误消息。

ADV_FSP.3.6C 功能规范应总结与每个 TSFI 相关的 SFR-支撑和 SFR-无关的行为。

ADV_FSP.3.7C 功能规范应证实安全功能要求到 TSFI 的追溯。

评估者行为元素：

ADV_FSP.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV_FSP.3.2E 评估者应确定功能规范是安全功能要求的一个准确且完备的实例化。

7.2.2.4 完备的功能规范(ADV_FSP.4)

依赖关系：ADV_TDS.1 基础设计。

开发者行为元素：

ADV_FSP.4.1D 开发者应提供一个功能规范。

ADV_FSP.4.2D 开发者应提供功能规范到安全功能要求的追溯。

内容和形式元素：

ADV_FSP.4.1C 功能规范应完全描述 TSF。

ADV_FSP.4.2C 功能规范应描述所有 TSFI 的目的和使用方法。

ADV_FSP.4.3C 功能规范应识别和描述每个 TSFI 相关的所有参数。

ADV_FSP.4.4C 对于每个 SFR-执行 TSFI，功能规范应描述 TSFI 相关的所有行为。

ADV_FSP.4.5C 功能规范应描述可能由每个 TSFI 的调用而引起的所有直接错误消息。

ADV_FSP.4.5C 功能规范应证实安全功能要求到 TSFI 的追溯。

评估者行为元素：

ADV_FSP.4.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV_FSP.4.2E 评估者应确定功能规范是安全功能要求的一个准确且完备的实例化。

7.2.2.5 TSF 实现表示(ADV_IMP.1)

依赖关系：ADV_TDS.3 基础模块设计；

ALC_TAT.1 明确定义的开发工具。

开发者行为元素：

ADV_IMP.1.1D 开发者应为全部 TSF 提供实现表示。

ADV_IMP.1.2D 开发者应提供移动终端操作系统设计描述与实现表示实例之间的映射。

内容和形式元素：

ADV_IMP.1.1C 实现表示应按详细级别定义 TSF，且详细程度达到无须进一步设计就能生成 TSF 的程度。

ADV_IMP.1.2C 实现表示应以开发人员使用的形式提供。

ADV_IMP.1.3C 移动终端操作系统设计描述与实现表示示例之间的映射应能证实它们的一致性。

评估者行为元素：

ADV_IMP.1.1E 对于选取的实现表示示例，评估者应确认提供的信息满足证据的内容和形式的所有要求。

7.2.2.6 基础设计(ADV_TDS.1)

依赖关系：ADV_FSP.2 安全执行功能规范。

开发者行为元素：

ADV_TDS.1.1D 开发者应提供移动终端操作系统的设计。

ADV_TDS.1.2D 开发者应提供从功能规范的 TSFI 到移动终端操作系统设计中获取到的最低层分

解的映射。

内容和形式元素：

ADV_TDS.1.1C 设计应根据子系统描述移动终端操作系统的结构。

ADV_TDS.1.2C 设计应标识 TSF 的所有子系统。

ADV_TDS.1.3C 设计应对每一个 SFR-支撑或 SFR-无关的 TSF 子系统的行为进行详细的描述，以确定它不是 SFR-执行。

ADV_TDS.1.4C 设计应概括 SFR-执行子系统的 SFR-执行行为。

ADV_TDS.1.5C 设计应描述 TSF 的 SFR-执行子系统间的相互作用和 TSF 的 SFR-执行子系统与其他 TSF 子系统间的相互作用。

ADV_TDS.1.6C 映射关系应证实移动终端操作系统设计中描述的所有行为能映射到调用它的 TSFI。

评估者行为元素：

ADV_TDS.1.1E 评估者应确认提供的信息满足证据的内容与形式的所有要求。

ADV_TDS.1.2E 评估者应确定设计是所有安全功能要求的正确且完备的实例。

7.2.2.7 结构化设计（ADV_TDS.2）

依赖关系：ADV_FSP.3 带完整摘要的功能规范。

开发者行为元素：

ADV_TDS.2.1D 开发者应提供移动终端操作系统的设计。

ADV_TDS.2.2D 开发者应提供从功能规范的 TSFI 到移动终端操作系统设计中获取到的最低层分解的映射。

内容和形式元素：

ADV_TDS.2.1C 设计应根据子系统描述移动终端操作系统的结构。

ADV_TDS.2.2C 设计应标识 TSF 的所有子系统。

ADV_TDS.2.3C 设计应对每一个 TSF 的 SFR-无关子系统的行为进行足够详细的描述，以确定它是 SFR-无关。

ADV_TDS.2.4C 设计应描述 SFR-执行子系统的 SFR-执行行为。

ADV_TDS.2.5C 设计应概括 SFR-执行子系统的 SFR-支撑和 SFR-无关行为。

ADV_TDS.2.6C 设计应概括 SFR-支撑子系统的行为。

ADV_TDS.2.7C 设计应描述 TSF 所有子系统间的相互作用。

ADV_TDS.2.8C 映射关系应证实移动终端操作系统设计中描述的所有行为能映射到调用它的 TSFI。

评估者行为元素：

ADV_TDS.2.1E 评估者应确认提供的信息满足证据的内容与形式的所有要求。

ADV_TDS.2.2E 评估者应确定设计是所有安全功能要求的正确且完备的实例。

7.2.2.8 基础模块设计（ADV_TDS.3）

依赖关系：ADV_FSP.4 完备的功能规范。

开发者行为元素：

ADV_TDS.3.1D 开发者应提供移动终端操作系统的设计。

ADV_TDS.3.2D 开发者应提供从功能规范的 TSFI 到移动终端操作系统设计中获取到的最低层分

解的映射。

内容和形式元素：

ADV_TDS.3.1C 设计应根据子系统描述移动终端操作系统的结构。

ADV_TDS.3.2C 设计应根据模块描述 TSF。

ADV_TDS.3.3C 设计应标识 TSF 的所有子系统。

ADV_TDS.3.4C 设计应描述每一个 TSF 子系统。

ADV_TDS.3.5C 设计应描述 TSF 所有子系统间的相互作用。

ADV_TDS.3.6C 设计应提供 TSF 子系统到 TSF 模块间的映射关系。

ADV_TDS.3.7C 设计应描述每一个 SFR-执行模块，包括它的目的及与其他模块间的相互作用。

ADV_TDS.3.8C 设计应描述每一个 SFR-执行模块，包括它的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口。

ADV_TDS.3.9C 设计应描述每一个 SFR-支撑或 SFR-无关模块，包括它的目的及与其他模块间的相互作用。

ADV_TDS.3.10C 映射关系应论证实 TOE 设计中描述的所有行为能映射到调用它的 TSFI。

评估者行为元素：

ADV_TDS.3.1E 评估者应确认提供的信息满足证据的内容与形式的所有要求。

ADV_TDS.3.2E 评估者应确定设计是所有安全功能要求的正确且完全的实例。

7.2.3 指导性文档(AGD 类)

7.2.3.1 操作用户指南(AGD_OPE.1)

依赖关系：ADV_FSP.1 基本功能规范。

开发者行为元素：

AGD_OPE.1.1D 开发者应提供操作用户指南。

内容和形式元素：

AGD_OPE.1.1C 操作用户指南应对每一种用户角色进行描述，在安全处理环境中应被控制的用户可访问的功能和特权，包含适当的警示信息。

AGD_OPE.1.2C 操作用户指南应对每一种用户角色进行描述，怎样以安全的方式使用移动终端操作系统提供的可用接口。

AGD_OPE.1.3C 操作用户指南应对每一种用户角色进行描述，可用功能和接口，尤其是受用户控制的所有安全参数，适当时应指明安全值。

AGD_OPE.1.4C 操作用户指南应对每一种用户角色明确说明，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 TSF 所控制实体的安全特性。

AGD_OPE.1.5C 操作用户指南应标识移动终端操作系统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)，它们与维持安全运行之间的因果关系和联系。

AGD_OPE.1.6C 操作用户指南应对每一种用户角色进行描述，为了充分实现 ST 中描述的运行环境安全目的应执行的安全策略。

AGD_OPE.1.7C 操作用户指南应是明确和合适的。

评估者行为元素：

AGD_OPE.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.3.2 准备程序(AGD_PRE.1)

依赖关系：无依赖关系。

开发者行为元素：

AGD_PRE.1.1D 开发者应提供移动终端操作系统，包括它的准备程序。

内容和形式元素：

AGD_PRE.1.1C 准备程序应描述与开发者交付程序相一致的安全接收所交付移动终端操作系统所需的所有步骤。

AGD_PRE.1.2C 准备程序应描述安全安装移动终端操作系统以及安全准备与 ST 中描述的运行环境安全目的一致的运行环境所需的所有步骤。

评估者行为元素：

AGD_PRE.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AGD_PRE.1.2E 评估者应运用准备程序确认移动终端操作系统运行能被安全的准备。

7.2.4 生命周期支持（ALC 类）

7.2.4.1 CM 系统的使用（ALC_CMC.2）

依赖关系：ALC_CMS.1 TOE CM 覆盖。

开发者行为元素：

ALC_CMC.2.1D 开发者应提供移动终端操作系统及其参照号。

ALC_CMC.2.2D 开发者应提供 CM 文档。

ALC_CMC.2.3D 开发者应使用 CM 系统。

内容和形式元素：

ALC_CMC.2.1C 应给移动终端操作系统标注唯一参照号。

ALC_CMC.2.2C CM 文档应描述用于唯一标识配置项的方法。

ALC_CMC.2.3C CM 系统应唯一标识所有配置项。

评估者行为元素：

ALC_CMC.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.2 授权控制（ALC_CMC.3）

依赖关系：ALC_CMS.1 TOE CM 覆盖；
ALC_DVS.1 安全措施标识；
ALC_LCD.1 开发者定义的生命周期模型。

开发者行为元素：

ALC_CMC.3.1D 开发者应提供移动终端操作系统及其参照号。

ALC_CMC.3.2D 开发者应提供 CM 文档。

ALC_CMC.3.3D 开发者应使用 CM 系统。

内容和形式元素：

ALC_CMC.3.1C 应给移动终端操作系统标注唯一参照号。

ALC_CMC.3.2C CM 文档应描述用于唯一标识配置项的方法。

ALC_CMC.3.3C CM 系统应唯一标识所有配置项。

ALC_CMC.3.4C CM 系统应提供措施使得只能对配置项进行授权变更。

ALC_CMC.3.5C CM 文档应包括一个 CM 计划。

ALC_CMC.3.6C CM 计划应描述 CM 系统是如何应用于移动终端操作系统的开发过程。

ALC_CMC.3.7C 证据应证实所有配置项都正在 CM 系统下进行维护。

ALC_CMC.3.8C 证据应证实 CM 系统的运行与 CM 计划是一致的。

评估者行为元素：

ALC_CMC.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.3 生产支持和接受程序及其自动化(ALC_CMC.4)

依赖关系：ALC_CMS.1 TOE CM 覆盖；

ALC_DVS.1 安全措施标识；

ALC_LCD.1 开发者定义的生命周期模型。

开发者行为元素：

ALC_CMC.4.1D 开发者应提供移动终端操作系统及其参照号。

ALC_CMC.4.2D 开发者应提供 CM 文档。

ALC_CMC.4.3D 开发者应使用 CM 系统。

内容和形式元素：

ALC_CMC.4.1C 应给移动终端操作系统标注唯一参照号。

ALC_CMC.4.2C CM 文档应描述用于唯一标识配置项的方法。

ALC_CMC.4.3C CM 系统应唯一标识所有配置项。

ALC_CMC.4.4C CM 系统应提供措施使得只能对配置项进行授权变更。

ALC_CMC.4.5C CM 系统应以自动化的方式支持移动终端操作系统的生产。

ALC_CMC.4.6C CM 文档应包括 CM 计划。

ALC_CMC.4.7C CM 计划应描述 CM 系统是如何应用于移动终端操作系统的开发的。

ALC_CMC.4.8C CM 计划应描述用来接受修改过的或新创建的作为移动终端操作系统组成部分的配置项的程序。

ALC_CMC.4.9C 证据应证实所有配置项都正在 CM 系统下进行维护。

ALC_CMC.4.10C 证据应证实 CM 系统的运行与 CM 计划是一致的。

评估者行为元素：

ALC_CMC.4.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.4 部分 TOE CM 覆盖(ALC_CMS.2)

依赖关系：无依赖关系。

开发者行为元素：

ALC_CMS.2.1D 开发者应提供移动终端操作系统配置项列表。

内容和形式元素：

ALC_CMS.2.1C 配置项列表应包括：移动终端操作系统本身、安全保障要求的评估证据和移动终端操作系统的组成部分。

ALC_CMS.2.2C 配置项列表应唯一标识配置项。

ALC_CMS.2.3C 对于每一个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。

评估者行为元素：

ALC_CMS.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.5 实现表示 CM 覆盖(ALC_CMS.3)

依赖关系：无依赖关系。

开发者行为元素：

ALC_CMS.3.1D 开发者应提供移动终端操作系统配置项列表。

内容和形式元素：

ALC_CMS.3.1C 配置项列表应包括：移动终端操作系统本身、安全保障要求的评估证据、移动终端操作系统的组成部分和实现表示。

ALC_CMS.3.2C 配置项列表应唯一标识配置项。

ALC_CMS.3.3C 对于每一个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。

评估者行为元素：

ALC_CMS.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.6 问题跟踪 CM 覆盖(ALC_CMS.4)

依赖关系：无依赖关系。

开发者行为元素：

ALC_CMS.4.1D 开发者应提供移动终端操作系统配置项列表。

内容和形式元素：

ALC_CMS.4.1C 配置项列表应包括：移动终端操作系统本身、安全保障要求的评估证据、移动终端操作系统的组成部分、实现表示和安全缺陷报告及其解决状态。

ALC_CMS.4.2C 配置项列表应唯一标识配置项。

ALC_CMS.4.3C 对于每一个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。

评估者行为元素：

ALC_CMS.4.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.7 交付程序(ALC_DEL.1)

依赖关系：无依赖关系。

开发者行为元素：

ALC_DEL.1.1D 开发者应将把移动终端操作系统或其部分交付给消费者的程序文档化。

ALC_DEL.1.2D 开发者应使用交付程序。

内容和形式元素：

ALC_DEL.1.1C 交付文档应描述，在向消费者分发移动终端操作系统版本时，用以维护安全性所需的所有程序。

评估者行为元素：

ALC_DEL.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.8 安全措施标识(ALC_DVS.1)

依赖关系：无依赖关系。

开发者行为元素：

ALC_DVS.1.1D 开发者应提供开发安全文档。

内容和形式元素：

ALC_DVS.1.1C 开发安全文档应描述在移动终端操作系统的开发环境中，保护移动终端操作系统设计和实现的机密性和完整性所需的所有物理的、程序的、人员的及其他方面的安全措施。

评估者行为元素：

ALC_DVS.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_DVS.1.2E 评估者应确认安全措施正在被使用。

7.2.4.9 开发者定义的生命周期模型(ALC_LCD.1)

依赖关系:无依赖关系。

开发者行为元素:

ALC_LCD.1.1D 开发者应建立一个生命周期模型,用于移动终端操作系统的开发和维护。

ALC_LCD.1.2D 开发者应提供生命周期定义文档。

内容和形式元素:

ALC_LCD.1.1C 生命周期定义文档应描述用于开发和维护移动终端操作系统的模型。

ALC_LCD.1.2C 生命周期模型应为移动终端操作系统的开发和维护提供必要的控制。

评估者行为元素:

ALC_LCD.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.4.10 明确定义的开发工具(ALC_TAT.1)

依赖关系:ADV_IMP.1 TSF 实现表示。

开发者行为元素:

ALC_TAT.1.1D 开发者应标识用于开发移动终端操作系统的每个工具。

ALC_TAT.1.2D 开发者应在文档中描述每个开发工具所选取的实现依赖选项。

内容和形式元素:

ALC_TAT.1.1C 用于实现的每个开发工具都应是明确定义的。

ALC_TAT.1.2C 每个开发工具的文档应无歧义地定义所有语句和实现用到的所有协定与命令的含义。

ALC_TAT.1.3C 每个开发工具的文档应无歧义地定义所有实现依赖选项的含义。

评估者行为元素:

ALC_TAT.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.5 安全目标评估(ASE 类)

7.2.5.1 符合性声明(ASE_CCL.1)

依赖关系:ASE_INT.1 ST 引言;

ASE_ECD.1 扩展组件定义;

ASE_REQ.1 陈述性的安全要求。

开发者行为元素:

ASE_CCL.1.1D 开发者应提供符合性声明。

ASE_CCL.1.2D 开发者应提供符合性声明的基本原理。

内容和形式元素:

ASE_CCL.1.1C ST 的符合性声明应包含 GB/T 18336.1—2015、GB/T 18336.2—2015 和 GB/T 18336.3—2015 符合性声明,标识出 ST 和 TOE 声明符合性遵从的标准版本。

ASE_CCL.1.2C ST 的符合性声明应描述 ST 和 GB/T 18336.2—2015 的符合性,无论是与 GB/T 18336.2—2015相符或是与 GB/T 18336.2—2015 的扩展部分相符。

ASE_CCL.1.3C 符合性声明应描述 ST 和 GB/T 18336.3—2015 的符合性,无论是与

GB/T 18336.3—2015相符或是与 GB/T 18336.3—2015 的扩展部分相符。

ASE_CCL.1.4C 符合性声明应与扩展组件定义是相符的。

ASE_CCL.1.5C 符合性声明应标识 ST 声明遵从的所有 PP 和安全要求包。

ASE_CCL.1.6C 符合性声明应描述 ST 和包的符合性，无论是与包的相符或是与扩展包相符。

ASE_CCL.1.7C 符合性声明的基本原理应证实 TOE 类型与符合性声明所遵从的 PP 中的 TOE 类型是相符的。

ASE_CCL.1.8C 符合性声明的基本原理应证实安全问题定义的陈述与符合性声明所遵从的 PP 中的安全问题定义陈述是相符的。

ASE_CCL.1.9C 符合性声明的基本原理应证实安全目的陈述与符合性声明所遵从的 PP 中的安全目的陈述是相符的。

ASE_CCL.1.10C 符合性声明的基本原理应证实安全要求的陈述与符合性声明所遵从的 PP 中的安全要求的陈述是相符的。

评估者行为元素：

ASE_CCL.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.5.2 扩展组件定义(ASE_ECD.1)

依赖关系：无依赖关系。

开发者行为元素：

ASE_ECD.1.1D 开发者应提供安全要求的陈述。

ASE_ECD.1.2D 开发者应提供扩展组件的定义。

内容和形式元素：

ASE_ECD.1.1C 安全要求陈述应标识所有扩展的安全要求。

ASE_ECD.1.2C 扩展组件定义应为每一个扩展的安全要求定义一个扩展的组件。

ASE_ECD.1.3C 扩展组件定义应描述每个扩展的组件与已有组件、族和类的关联性。

ASE_ECD.1.4C 扩展组件定义应使用已有的组件、族、类和方法学作为陈述的模型。

ASE_ECD.1.5C 扩展组件应由可测量的和客观的元素组成，以便于证实这些元素之间的符合性或不符合性。

评估者行为元素：

ASE_ECD.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ASE_ECD.1.2E 评估者应确认扩展组件不能利用已经存在的组件明确的表达。

7.2.5.3 ST 引言(ASE_INT.1)

依赖关系：无依赖关系。

开发者行为元素：

ASE_INT.1.1D 开发者应提供 ST 引言。

内容和形式元素：

ASE_INT.1.1C ST 引言应包含 ST 参照号，TOE 参照号，TOE 概述和 TOE 描述。

ASE_INT.1.2C ST 参照号应唯一标识 ST。

ASE_INT.1.3C TOE 参照号应标识 TOE。

ASE_INT.1.4C TOE 概述应概括 TOE 的用法及其主要安全特性。

ASE_INT.1.5C TOE 概述应标识 TOE 类型。

ASE_INT.1.6C TOE 概述应标识任何 TOE 要求的非 TOE 范围内的硬件/软件/固件。

ASE_INT.1.7C TOE 描述应描述移动终端操作系统的物理范围。

ASE_INT.1.8C TOE 描述应描述移动终端操作系统的逻辑范围。

评估者行为元素：

ASE_INT.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ASE_INT.1.2E 评估者应确认 TOE 参考、TOE 概述和 TOE 描述是相互一致的。

7.2.5.4 安全目的(ASE_OBJ.2)

依赖关系：ASE_SPD.1 安全问题定义。

开发者行为元素：

ASE_OBJ.2.1D 开发者应提供安全目的的陈述。

ASE_OBJ.2.2D 开发者应提供安全目的的基本原理。

内容和形式元素：

ASE_OBJ.2.1C 安全目的的陈述应描述移动终端操作系统的安全目的和运行环境安全目的。

ASE_OBJ.2.2C 安全目的基本原理应追溯到移动终端操作系统的每一个安全目的，以便于能追溯到安全目的所对抗的威胁及安全目的实施的组织安全策略。

ASE_OBJ.2.3C 安全目的基本原理应追溯到运行环境的每一个安全目的，以便于能追溯到安全目的所对抗的威胁、安全目的实施的组织安全策略和安全目的支持的假设。

ASE_OBJ.2.4C 安全目的基本原理应证实安全目的能抵抗所有威胁。

ASE_OBJ.2.5C 安全目的基本原理应证实安全目的执行所有组织安全策略。

ASE_OBJ.2.6C 安全目的基本原理应证实运行环境安全目的支持所有的假设。

评估者行为元素：

ASE_OBJ.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.5.5 推导出的安全要求(ASE_REQ.2)

依赖关系：ASE_OBJ.2 安全目的；

ASE_ECD.1 扩展组件定义。

开发者行为元素：

ASE_REQ.2.1D 开发者应提供安全要求的陈述。

ASE_REQ.2.2D 开发者应提供安全要求的基本原理。

内容和形式元素：

ASE_REQ.2.1C 安全要求的陈述应描述安全功能要求和安全保障要求。

ASE_REQ.2.2C 应对安全功能要求和安全保障要求中使用的所有主体、客体、操作、安全属性、外部实体及其他术语进行定义。

ASE_REQ.2.3C 安全要求的陈述应对安全要求的所有操作进行标识。

ASE_REQ.2.4C 所有操作应被正确地执行。

ASE_REQ.2.5C 应满足安全要求间的依赖关系，或者安全要求基本原理应论证不需要满足某个依赖关系。

ASE_REQ.2.6C 安全要求基本原理应描述每一个安全功能要求可追溯至对应的移动终端操作系统安全目的。

ASE_REQ.2.7C 安全要求基本原理应证实安全功能要求可满足所有的移动终端操作系统安全

目的。

ASE_REQ.2.8C 安全要求基本原理应说明选择安全保障要求的理由。

ASE_REQ.2.9C 安全要求的陈述应是内在一致的。

评估者行为元素：

ASE_REQ.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.5.6 安全问题定义(ASE_SPD.1)

依赖关系：无依赖关系。

开发者行为元素：

ASE_SPD.1.1D 开发者应提供安全问题定义。

内容和形式元素：

ASE_SPD.1.1C 安全问题定义应描述威胁。

ASE_SPD.1.2C 所有的威胁都应根据威胁主体、资产和敌对行为进行描述。

ASE_SPD.1.3C 安全问题定义应描述组织安全策略。

ASE_SPD.1.4C 安全问题定义应描述移动终端操作系统运行环境的相关假设。

评估者行为元素：

ASE_SPD.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.2.5.7 TOE 概要规范(ASE_TSS.1)

依赖关系：ASE_INT.1 ST 引言；

ASE_REQ.1 安全要求的陈述；

ADV_FSP.1 基本功能规范。

开发者行为元素：

ASE_TSS.1.1D 开发者应提供 TOE 概要规范。

内容和形式元素：

ASE_TSS.1.1C TOE 概要规范应描述移动终端操作系统是如何满足每一项安全功能要求的。

评估者行为元素：

ASE_TSS.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ASE_TSS.1.2E 评估者应确认 TOE 概要规范与 TOE 概述、TOE 描述是一致的。

7.2.6 测试(ATE 类)

7.2.6.1 覆盖证据(ATE_COV.1)

依赖关系：ADV_FSP.2 安全执行功能规范；

ATE_FUN.1 功能测试。

开发者行为元素：

ATE_COV.1.1D 开发者应提供测试覆盖的证据。

内容和形式元素：

ATE_COV.1.1C 测试覆盖的证据应表明测试文档中的测试与功能规范中的 TSF 接口之间的对应性。

评估者行为元素：

ATE_COV.1.1E 评估者应确认所提供的信息满足证据的所有内容和形式要求。

7.2.6.2 覆盖分析(ATE_COV.2)

依赖关系:ADV_FSP.2 安全执行功能规范;
ATE_FUN.1 功能测试。

开发者行为元素:

ATE_COV.2.1D 开发者应提供对测试覆盖的分析。

内容和形式元素:

ATE_COV.2.1C 测试覆盖分析应证实测试文档中的测试与功能规范中 TSF 接口之间的对应性。

ATE_COV.2.2C 测试覆盖分析应证实已经对功能规范中的所有 TSF 接口都进行了测试。

评估者行为元素:

ATE_COV.2.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.2.6.3 测试:基本设计(ATE_DPT.1)

依赖关系:ADV_ARC.1 安全架构描述;
ADV_TDS.2 结构化设计;
ATE_FUN.1 功能测试。

开发者行为元素:

ATE_DPT.1.1D 开发者应提供测试深度分析。

内容和形式元素:

ATE_DPT.1.1C 测试深度分析应证实测试文档中的测试与移动终端操作系统设计中 TSF 子系统之间的对应性。

ATE_DPT.1.2C 测试深度分析应证实移动终端操作系统设计中的所有 TSF 子系统都已经进行过测试。

评估者行为元素:

ATE_DPT.1.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.2.6.4 测试:安全执行模块(ATE_DPT.2)

依赖关系:ADV_ARC.1 安全架构描述;
ADV_TDS.3 基础模块设计;
ATE_FUN.1 功能测试。

开发者行为元素:

ATE_DPT.2.1D 开发者应提供测试深度分析。

内容和形式元素:

ATE_DPT.2.1C 深度测试分析应证实测试文档中的测试与移动终端操作系统设计中的 TSF 子系统、SFR-执行模块之间的一致性。

ATE_DPT.2.2C 测试深度分析应证实移动终端操作系统设计中的所有 TSF 子系统都已经进行过测试。

ATE_DPT.2.3C 测试深度分析应证实移动终端操作系统设计中的 SFR-执行模块都已经进行过测试。

评估者行为元素:

ATE_DPT.2.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.2.6.5 功能测试(ATE_FUN.1)

依赖关系:ATE_COV.1 覆盖证据。

开发者行为元素:

ATE_FUN.1.1D 开发者应测试 TSF,并文档化测试结果。

ATE_FUN.1.2D 开发者应提供测试文档。

内容和形式元素:

ATE_FUN.1.1C 测试文档应包括测试计划、预期的测试结果和实际的测试结果。

ATE_FUN.1.2C 测试计划应标识要执行的测试并描述执行每个测试的方案,这些方案应包括对于其他测试结果的任何顺序依赖性。

ATE_FUN.1.3C 预期的测试结果应指出测试成功执行后的预期输出。

ATE_FUN.1.4C 实际的测试结果应和预期的测试结果一致。

评估者行为元素:

ATE_FUN.1.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.2.6.6 独立测试—抽样(ATE_IND.2)

依赖关系:ADV_FSP.2 安全执行功能规范;
AGD_OPE.1 操作用户指南;
AGD_PRE.1 准备程序;
ATE_COV.1 覆盖证据;
ATE_FUN.1 功能测试。

开发者行为元素:

ATE_IND.2.1D 开发者应提供用于测试的移动终端操作系统。

内容和形式元素:

ATE_IND.2.1C 移动终端操作系统应适合测试。

ATE_IND.2.2C 开发者应提供一组与开发者 TSF 功能测试中同等的一系列资源。

评估者行为元素:

ATE_IND.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ATE_IND.2.2E 评估者应执行测试文档中的测试样本,以验证开发者的测试结果。

ATE_IND.2.3E 评估者应测试 TSF 的一个子集以确认 TSF 按照规定运行。

7.2.7 脆弱性评估(AVA 类)

7.2.7.1 脆弱性分析(AVA_VAN.2)

依赖关系:ADV_ARC.1 安全架构描述;
ADV_FSP.2 安全执行功能规范;
ADV_TDS.1 基础设计;
AGD_OPE.1 操作用户指南;
AGD_PRE.1 准备程序。

开发者行为元素:

AVA_VAN.2.1D 开发者应提供用于测试的移动终端操作系统。

内容和形式元素:

AVA_VAN.2.1C 移动终端操作系统应适合测试。

评估者行为元素：

AVA_VAN.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AVA_VAN.2.2E 评估者应执行公共领域的调查以标识移动终端操作系统的潜在脆弱性。

AVA_VAN.2.3E 评估者应执行独立的移动终端操作系统脆弱性分析去标识移动终端操作系统潜在的脆弱性，在分析过程中使用指导性文档、功能规范、移动终端操作系统设计和安全结构描述。

AVA_VAN.2.4E 评估者应基于已标识的潜在脆弱性实施穿透性测试，确定移动终端操作系统能抵抗具有基本攻击潜力的攻击者的攻击。

7.2.7.2 关注点脆弱性分析(AVA_VAN.3)

依赖关系：ADV_ARC.1 安全架构描述；

ADV_FSP.4 完备的功能描述；

ADV_TDS.3 基础模块设计；

ADV_IMP.1 TSF 实现表示；

AGD_OPE.1 用户操作指南；

AGD_PRE.1 准备过程；

ATE_DPT.1 测试：基本设计。

开发者行为元素：

AVA_VAN.3.1D 开发者应提供用于测试的移动终端操作系统。

内容和形式元素：

AVA_VAN.3.1C 移动终端操作系统应适合测试。

评估者行为元素：

AVA_VAN.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AVA_VAN.3.2E 评估者应执行一个公共领域的调查以标识移动终端操作系统的潜在脆弱性。

AVA_VAN.3.3E 评估者应针对移动终端操作系统执行一个独立的脆弱性分析去标识移动终端操作系统中潜在的脆弱性，在分析过程中使用指导性文档、功能规范、移动终端操作系统设计、安全结构描述和实现表示。

AVA_VAN.3.4E 评估者应基于已标识的潜在脆弱性实施穿透性测试，确定移动终端操作系统能抵抗具有增强型基本攻击潜力的攻击者的攻击。

8 基本原理

8.1 安全目的基本原理

移动终端操作系统安全目的能应对所有可能的威胁、假设和组织安全策略，即每一种威胁、假设和组织安全策略都至少有一个或一个以上安全目的与其对应，因此是完备的。每一个安全目的都有相应的威胁、假设和组织安全策略与之对应，这证明每个安全目的都是必要的；每一个威胁、假设和组织安全策略都有相应的一个或多个安全目的与之对应，因此说明了安全目的是充分的。

表 3 说明了移动终端操作系统的安全目的能应对所有可能的威胁、假设和组织安全策略。

表 3　威胁、组织安全策略、假设与安全目的的对应关系

安全目的	安全威胁、假设和策略													
	T.ACCESS_MALICIOUS	T.UNAUTHORIZED_ACCESS	T.TSF_COMPROMISE	T.EAVESDROP	T.REPLAY	T.RESIDUAL_DATA	T.MALICIOUSAPP	T.UNAUTHORIZED_NETFLOW	T.UNATTENDED_SESSION	T.LOST	P.CRYPTO	A.REMOTE	A.PERSONNEL	A.PHYSICAL
O.AUDIT	√													
O.AUTH		√												
O.MANAGE	√							√						
O.ENCTYPT		√	√	√							√			
O.RESIDUAL_INFO						√				√				
O.TRUSTED_CHANNLE				√							√			
O.ACCESS_CONTROL		√					√							
O.SESSION_MANAGEMENT									√					
O.ROLLBACK			√											
O.NETWORK_FLOW								√						
O.RESOURCE_QUOTA							√							
O.TIME					√									
O.LOST_PROTECT										√				
OE.ADMIN													√	
OE.PHYSICAL														√
OE.REMOTE												√		

下面的 a)～n)给出了威胁、组织安全策略、假设与安全目的之间的对应关系：

a)　T.EAVESDROP

恶意用户或进程可能监听或修改移动终端操作系统之间或者移动终端操作系统与远程可信 IT 产品间传递的用户数据或 TSF 数据。O.TRUSTED_CHANNEL 能保证为移动终端操作系统之间以及移动终端操作系统与外部可信 IT 实体间的通信提供可信通道，防止数据备监听和修改，同时 O.ENCTYPT保证传输数据采用加密方式，防止被窃取。

b)　T.TSF_COMPROMISE

恶意用户或进程通过安全攻击非法地浏览、修改或删除 TSF 数据或可执行代码。这可能让恶意用户或进程获得移动终端操作系统的配置信息，或可能导致移动终端操作系统的安全功能对于数据资产

保护的安全机制不再正常工作。O.ENCTYPT 保证传输数据采用加密方式，防止被窃取。O.ROLLBACK 保证数据回滚到安全状态，保证安全功能的正常运行。

c) T.ACCESS_MALICIOUS

授权用户因安全意识薄弱或误操作，对移动终端操作系统进行不正确地配置，或授权用户恶意利用权限进行非法操作，使移动终端安全受到威胁。O.AUDIT 能保证对用户操作行为的审计，可用于误操作或非法操作行为的追溯，并对审计数据进行保护并且只允许授权用户查看，同时保证审计迹已满的情况下，不影响审计功能和其他安全功能的执行。O.MANAGE 可对授权用户的权限进行限制，避免权限滥用。

d) T.UNAUTHORIZED_NETFLOW

未授权外部 IT 实体向移动终端操作系统发送网络数据或接收经由移动终端操作系统的网络数据。O.NETWORK_FLOW 可阻止已知的恶意网络攻击行为，并可控制移动终端操作系统内的 IT 实体和外部 IT 实体之间的网络数据传输。O.MANAGE 可控制这些数据传输的规则只能通过授权用户来改变。

e) T.RESIDUAL_DATA

恶意用户或进程可能利用移动终端操作系统残留信息的处理缺陷，在执行过程中对未删除的残留信息进行利用，以获取敏感信息或滥用评估对象的安全功能。O.RESIDUAL_INFO 能保证重要的数据在使用完成后会被删除或被安全处理，不会留下可被攻击者利用的残留数据信息。

f) T.MALICIOUSAPP

恶意软件可能通过伪装成授权应用或进程访问用户数据和系统敏感资源。O.ACCESS_CONTROL 保障移动终端操作系统具备访问控制措施，用户对数据和资源的访问应严格依照访问控制策略。

g) T.UNAUTHORIZED_ACCESS

非授权用户或进程访问移动终端操作系统的安全功能数据和用户数据，并对安全功能数据和用户数据进行恶意操作。O.AUTH 能保障未授权用户在访问移动终端操作系统时应经过用户身份认证，未通过认证的用户无法访问安全功能和数据，并保障移动终端操作系统在鉴权失败达到一定次数时限制用户的鉴权行为，限制攻击者反复猜测鉴别数据。O.ENCTYPT 保障对重要数据进行加密，防止未授权用户的访问。O.ACCESS_CONTROL 保障移动终端操作系统具备访问控制措施，用户对数据和资源的访问应严格依照访问控制策略。

h) T.REPLAY

针对攻击者可以利用所截获的有效标识和鉴别数据，访问和使用由移动终端操作系统提供的相关功能。O.TIME 提供时间戳抵御重放攻击。

i) T.UNATTENDED_SESSION

非授权用户可以利用不被使用的会话，假冒授权用户对移动终端操作系统的功能和数据产生威胁。O.SESSION_MANAGEMENT 可保证临时不被使用的用户会话只有在重新验证用户身份后才能恢复使用。

j) T.LOST

移动终端操 作系统所运行的物理设备在被出售、交换、遗失的情况下，非授权用户可通过攻击方式获取授权用户数据。O.RESIDUAL_INFO 保证重要的数据在使用完成后会被删除或被安全处理，不会留下可被攻击者利用的残留数据信息。O.LOST_PROTECT 提供丢失保护机制，保证在物理终端丢失的情况下授权用户对用户敏感数据的控制。

k） P.CRYPTO

O.ENCRYPT 保证移动终端操作系统使用的密码算法应符合国家、行业或组织要求的密码管理相关标准或规范，并且移动终端操作系统应提供密码功能以维护移动智能操作系统的保密性和完整性。O.TRUSTED_CHANNEL 通过可信信道实现通信数据的保密性保护。

l） A.PHYSICAL

假设移动终端操作系统所依赖的运行环境能提供移动终端操作系统安全运行所需的物理安全防护。OE.PHYSICAL 保证 IT 环境应提供与移动终端操作系统及其所包含数据所需的物理安全保护。

m） A.PERSONNEL

假设移动终端操作系统的合法用户能按照管理员指南来管理移动终端操作系统的安全功能的，对移动终端操作系统不存在恶意的破坏企图。OE.PERSONNEL 保证了负责管理移动终端操作系统安全策略和数据的用户是可信的，经过学习和培训的，并且对管理和操作行为负责。

n） A.REMOTE

假定用于管理移动终端操作系统的远程 IT 设备、应用设备是安全可靠的。OE.REMOTE 保证了移动终端操作系统的远程管理设备、应用商店等远程 IT 是安全的且其数据和用户信息是被保护的。

8.2 安全要求的基本原理

表 4 说明了安全要求的充分必要性基本原理，即每个安全目的都至少有一个安全要求组件与其对应，每个安全要求都至少解决了一个安全目的，因此安全要求对安全目的而言是充分和必要的。

表 4 安全要求与安全目的的对应关系

安全功能要求	安全目的												
	O.AUDIT	O.AUTH	O.MANAGE	O.RESIDUAL_INFO	O.ENCTYPT	O.TRUSTED_CHANNEL	O.ACCESS_CONTROL	O.SESSION_MANAGEMENT	O.ROLLBACK	O.NETWORK_FLOW	O.RESOURCE_QUOTA	O.TIME	O.LOST_PROTECT
FAU_GEN.1	√												
FAU_GEN.2	√												
FAU_STG.1	√												
FAU_STG.4	√												
FCS_CKM.1					√	√							
FCS_COP.1					√	√							
FDP_ACC.1							√						
FDP_ACF.1							√						
FDP_ETC.1										√			

表 4（续）

安全功能要求	安全目的												
	O.AUDIT	O.AUTH	O.MANAGE	O.RESIDUAL_INFO	O.ENCTYPT	O.TRUSTED_CHANNEL	O.ACCESS_CONTROL	O. SESSION_MANAGEMENT	O.ROLLBACK	O.NETWORK_FLOW	O.RESOURCE_QUOTA	O.TIME	O.LOST_PROTECT
FDP_ETC.2										√			
FDP_IFC.1										√			
FDP_IFF.1										√			
FDP_ITC.1										√			
FDP_ITC.2										√			
FDP_UCT.1										√			
FDP_UIT.1										√			
FDP_RIP.1				√									
FDP_ROL.1									√				
FIA_AFL.1		√											
FIA_ATD.1		√					√						
FIA_SOS.1		√											
FIA_UAU.1		√											
FIA_UAU.5		√											
FIA_UAU.6		√						√					
FIA_UAU.7		√											
FIA_UID.1		√											
FIA_USB.1		√					√						
FMT_MOF.1	√		√							√	√	√	
FMT_MSA.1		√	√										
FMT_MSA.2		√	√										
FMT_MSA.3		√	√										
FMT_MTD.1	√	√	√				√	√		√	√	√	

表 4（续）

安全功能要求	安全目的												
	O.AUDIT	O.AUTH	O.MANAGE	O.RESIDUAL_INFO	O.ENCTYPT	O.TRUSTED_CHANNEL	O.ACCESS_CONTROL	O.SESSION_MANAGEMENT	O.ROLLBACK	O.NETWORK_FLOW	O.RESOURCE_QUOTA	O.TIME	O.LOST_PROTECT
FMT_MTD.2			√										
FMT_MTD.3			√										
FMT_SMF.1			√										
FMT_SMR.1			√										
FPT_FLS.1													√
FPT_ITC.1								√					
FPT_ITI.1								√					
FPT_STM.1												√	
FPT_TDC.1								√					
FPT_TST.1								√					
FRU_RSA.1											√		
FTA_SSL.1								√					
FTA_SSL.2								√					
FTP_ITC.1					√	√							

下面的 a)～m)给出了安全目的与安全功能要求之间的对应关系：

a) O.AUDIT

该目的可通过安全功能要求 FAU_GEN.1、FAU_GEN.2 来实现审计日志生成以及身份关联的目的。通过安全功能要求 FAU_STG.1、FAU_STG.4 可保障审计迹的存储安全。通过安全功能要求 FMT_MOF.1、FMT_MTD.1 实现审计功能和审计数据的管理。

b) O.AUTH

该目的可通过安全功能要求 FIA_UAU.1 对访问用户进行鉴别处理，以区分授权用户和非授权用户。通过安全功能要求 FIA_AFL.1 提供鉴别失败的锁定机制。通过安全功能要求 FIA_ATD.1 标识用户，以符合 FIA_UID.2 要求任何动作前应进行用户标识和 FIA_USB.1 要求的用户主体绑定。通过安全功能要求 FIA_SOS.1 规定了用户鉴别数据（如：口令）的强度要求。通过安全功能要求 FIA_UAU.5、FIA_UAU.6、FIA_UAU.7 提供用户鉴别的时机、用户多重鉴别方式，密码输入的显示以及会

话恢复时的重鉴别，通过安全功能要求 FMT_MTD.1 提供对鉴别数据的管理。通过安全功能要求 FMT_MSA.1、FMT_MSA2、FMT_MSA.3 提供对安全属性的管理。

c） O.MANAGE

该目的可通过安全功能要求 FMT_MOF.1 实现安全功能管理。通过安全功能要求 FMT_MTD.1、FMT_MTD.2、FMT_MTD.3 实现安全功能数据的管理。通过安全功能要求 FMT_SMF.1 实现管理功能规范的管理。通过安全功能要求 FMT_SMR.1 实现用户角色的管理。通过安全功能要求 FMT_MSA.1、FMT_MSA2、FMT_MSA.3 实现安全属性的管理。

d） O.ENCRYPT

该目的可通过安全功能要求 FCS_CKM.1 和 FCS_COP.1 实现数据加密过程中的密钥生成和密码运算进行要求。

e） O.TIME

该目的可通过安全功能要求 FPT_STM.1 提供可靠时间戳。通过安全功能要求 FMT_MOF.1 和 FMT_MTD.1 实现授权用户对时钟功能的配置和管理。

f） O.TRUSTED_CHANNLE

该目的可通过安全功能要求 FTP_ITC.1 提供 TSF 间可信信道。通过安全功能要求 FCS_CKM.1、FCS_COP.1 提供可信信道中数据加密的功能。

g） O.ROLLBACK

该目的可通过安全功能要求 FDP_ROL.1 实现用户数据回滚备份以及安全功能恢复的目的。

h） O.NETWORK_FLOW

该目的可通过安全功能要求 FMT_MOF.1、FMT_MTD.1 管理和配置网络数据流控制功能。通过安全功能要求 FDP_IFC.1、FDP_IFF.1 提供网络数据流控制。通过安全功能要求 FDP_ITC.1、FDP_ITC.2、FDP_UCT.1、FDP_UIT.1 提供数据输入和输出的要求。

i） O.ACCESS_CONTROL

该目的可通过安全功能要求 FDP_ACC.1、FDP_ACF.1 基于安全属性进行访问控制，防止非授权用户的恶意访问。通过安全功能要求 FIA_ATD.1 定义用户的安全属性并通过 FIA_USB.1 将用户与主体绑定。通过安全功能要求 FMT_MTD.1 对访问控制策略参数的管理和配置。

j） O.SESSION_MANAGEMENT

该目的可通过安全功能要求 FTA_SSL.1、FTA_SSL.2 实现会话锁定管理，解锁时通过 FIA_UAU.6实现会话恢复时的重鉴别功能。通过安全功能要求 FMT_MTD.1 提供会话锁定参数配置。通过安全功能要求 FPT_ITC.1、FPT_ITI.1、FPT_TDC.1 保证会话中 TSF 数据的机密性和完整性。通过安全功能要求 FPT_TST.1 实现移动终端操作系统功能的自检。

k） O.RESOURCE_QUOTA

该目的可通过安全功能要求 FRU_RSA.1 提供系统资源最高配额的限定。通过安全功能要求 FMT_MOF.1、FMT_MTD.1 管理和配置资源配额。

l） O.RESIDUAL_INFO

该目的可通过安全功能要求 FDP_RIP.1 实现残余数据和属性的保护和控制，保证残余数据不会被非授权用户使用从而导致用户敏感信息的丢失。

m） O.LOST_PROTECT

该目的可通过安全功能要求 FPT_FLS.1 实现移动终端操作系统保持安全状态功能。通过安全功能要求 FMT_MOF.1、FMT_MTD.1 提供防丢功能的管理和参数配置。

8.3 组件依赖关系

选取组件时，应符合所选组件之间的相互依赖关系。表5和表6分别列出了所选安全功能组件和安全保障组件的内部依赖关系。

表5 安全功能组件依赖关系表

序号	安全功能要求	安全功能要求依赖
1	FAU_GEN.1 审计数据产生	FPT_STM.1
2	FAU_GEN.2 用户身份关联	FAU_GEN.1；FIA_UID.1
3	FAU_STG.1 受保护的审计迹存储	FAU_GEN.1
4	FAU_STG.4 防止审计数据丢失	FAU_STG.1
5	FCS_CKM.1 密钥生成	FCS_COP.1 ；FCS_CKM.4
6	FCS_COP.1 密码运算	FDP_ITC.1 或 FCS_CKM.1； FCS_CKM.4
7	FDP_ACC.1 子集访问控制	FDP_ACF.1
8	FDP_ACF.1 基于安全属性的访问控制	FDP_ACC.1；FMT_MSA.3
9	FDP_ETC.1 不带安全属性的用户数据输出	FDP_ACC.1 或 FDP_IFC.1
10	FDP_ETC.2 带有安全属性的用户数据输出	FDP_ACC.1 或 FDP_IFC.1
11	FDP_IFC.1 子集信息流控制	FDP_IFF.1
12	FDP_IFF.1 简单安全属性	FDP_ACC.1；FMT_MSA.3
13	FDP_ITC.1 不带安全属性的用户数据输入	FDP_ACC.1 或 FDP_IFC.1； FMT_MSA.3
14	FDP_ITC.2 带有安全属性的用户数据输入	FDP_ACC.1 或 FDP_IFC.1； FDP_ITC.1；FPT_TDC.1
15	FDP_RIP.1 子集残余信息保护	无依赖组件
16	FDP_ROL.1 基本回退	FDP_ACC.1 或 FMT_IFC.1
17	FDP_UCT.1 基本的数据交换保密性	FTP_ITC.1； FDP_ACC.1 或 FDP_IFC.1
18	FDP_UIT.1 数据交换完整性	FDP_ACC.1 或 FDP_IFC.1； FDP_ITC.1
19	FIA_AFL.1 鉴别失败处理	FIA_UAU.1
20	FIA_ATD.1 用户属性定义	无依赖关系
21	FIA_SOS.1 秘密的验证	无依赖关系
22	FIA_UAU.1 鉴别的时机	FIA_UID.1
23	FIA_UAU.5 多重鉴别机制	无依赖关系
24	FIA_UAU.6 重鉴别	无依赖关系

表 5（续）

序号	安全功能要求	安全功能要求依赖
25	FIA_UAU.7 受保护的鉴别反馈	FIA_UAU.1
26	FIA_UID.1 标识的时机	无依赖关系
27	FIA_USB.1 用户-主体绑定	FIA_ATD.1
28	FMT_MOF.1 安全功能行为的管理	FMT_SMR.2；FMT_SMF.1
29	FMT_MSA.1 安全属性的管理	FDP_ACC.1 或 FDP_IFC.1； FMT_SMR.1；FMT_SMF.1
30	FMT_MSA.2 安全的安全属性	ADV_SPM.1； FDP_ACC.1 或 FDP_IFC.1； FMT_MSA.1；FMT_SMR.1
31	FMT_MSA.3 静态属性初始化	FMT_MSA.1；FMT_SMR.1
32	FMT_MTD.1 TSF 数据的管理	FMT_SMR.1；FMT_SMF.1
33	FMT_MTD.2 TSF 数据限值的管理	FMT_MTD.1；FMT_SMR.1
34	FMT_MTD.3 安全的 TSF 数据	FMT_MTD.1
35	FMT_SMF.1 管理功能规范	无依赖关系
36	FMT_SMR.1 安全角色	FIA_UID.1
37	FPT_FLS.1 失效即保持安全状态	无依赖关系
38	FPT_ITC.1 传送过程中 TSF 间的机密性	无依赖关系
39	FPT_ITI.1 TSF 间篡改的检测	无依赖关系
40	FPT_STM.1 可靠的时间戳	无依赖关系
41	FPT_TDC.1 TSF 间基本的 TSF 数据一致性	无依赖关系
42	FPT_TST.1 TSF 测试	无依赖关系
43	FRU_RSA.1 最高配额	无依赖关系
44	FTA_SSL.1 TSF 原发会话锁定	FIA_UAU.1
45	FTA_SSL.2 用户原发会话锁定	FIA_UAU.1
46	FTP_ITC.1 TSF 间可信信道	无依赖关系

表 6　安全保障组件依赖关系表

序号	安全保障要求	安全保障要求依赖
1	ADV_ARC.1 安全架构描述	ADV_FSP.1；ADV_TDS.1
2	ADV_FSP.2 安全执行功能规范	ADV_TDS.1
3	ADV_FSP.3 带完整摘要的功能规范	ADV_TDS.1

表 6（续）

序号	安全保障要求	安全保障要求依赖
4	ADV_FSP.4 完备的功能规范	ADV_TDS.1
5	ADV_IMP.1 TSF 实现表示	ADV_TDS.3；ALC_TAT.1
6	ADV_TDS.1 基础设计	ADV_FSP.2
7	ADV_TDS.2 结构化设计	ADV_FSP.3
8	ADV_TDS.3 基础模块设计	ADV_FSP.4
9	AGD_OPE.1 操作用户指南	ADV_FSP.1
10	AGD_PRE.1 准备程序	无依赖关系
11	ALC_CMC.2 CM 系统的使用	ALC_CMS.1
12	ALC_CMC.3 授权控制	ALC_CMS.1；ALC_DVS.1；ALC_LCD.1
13	ALC_CMC.4 生产支持和接受程序及其自动化	ALC_CMS.1；ALC_DVS.1；ALC_LCD.1
14	ALC_CMS.2 部分 TOE CM 覆盖	无依赖关系
15	ALC_CMS.3 实现表示 CM 覆盖	无依赖关系
16	ALC_CMS.4 问题跟踪 CM 覆盖	无依赖关系
17	ALC_DEL.1 交付程序	无依赖关系
18	ALC_DVS.1 安全措施标识	无依赖关系
19	ALC_LCD.1 开发者定义的生命周期模型	无依赖关系
20	ALC_TAT.1 明确定义的开发工具	ADV_IMP.1
21	ASE_CCL.1 符合性声明	ASE_INT.1；ASE_ECD.1 ；ASE_REQ.1
22	ASE_ECD.1 扩展组件定义	无依赖关系
23	ASE_INT.1 ST 引言	无依赖关系
24	ASE_OBJ.2 安全目的	ASE_SPD.1
25	ASE_REQ.2 推导出的安全要求	ASE_OBJ.2；ASE_ECD.1
26	ASE_SPD.1 安全问题定义	无依赖关系
27	ASE_TSS.1 TOE 概要规范	ASE_INT.1；ASE_REQ.1；ADV_FSP.1
28	ATE_COV.1 覆盖证据	ADV_FSP.2；ATE_FUN.1
29	ATE_COV.2 覆盖分析	ADV_FSP.2；ATE_FUN.1
30	ATE_DPT.1 测试：基本设计	ADV_ARC.1；ADV_TDS.2；ATE_FUN.1
31	ATE_DPT.2 安全执行模块	ADV_ARC.1；ADV_TDS.3；ATE_FUN.1
32	ATE_FUN.1 功能测试	ATE_COV.1

表 6（续）

序号	安全保障要求	安全保障要求依赖
33	ATE_IND.2 独立测试-抽样	ADV_FSP.2；AGD_OPE.1；AGD_PRE.1；ATE_COV.1；ATE_FUN.1
34	AVA_VAN.2 脆弱性分析	ADV_ARC.1 ；ADV_FSP.2 ；ADV_TDS.1；AGD_OPE.1 ；AGD_PRE.1
35	AVA_VAN.3 关注点脆弱性分析	ADV_ARC.1 ；ADV_FSP.4 ；ADV_TDS.3；ADV_IMP.1；AGD_OPE.1 ；AGD_PRE.1 ；ATE_DPT.1

参 考 文 献

[1] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

[2] GB/T 20272 信息安全技术 操作系统安全技术要求

[3] GB/Z 20283—2006 信息安全技术 保护轮廓和安全目标的产生指南

[4] ISO/IEC TR 15446:2009 Information technology—Security techniques—Guide for the production of Protection Profiles and Security Targets

[5] Protection Profile for General Purpose Operationg Systems Version 4.1,March 2016

[6] Operating System Protection Profile, Version 2.0 2010

[7] Protection Profile for Mobile Device Fundamentals Version 2.0, March 2015

[8] Protection Profile for Mobile Device Management Version 2.0, December 2014