ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30284—2013

移动通信智能终端操作系统安全技术要求（EAL2级）

Technical requirements of security for operating system in smart mobile terminal (EAL2)

2013-12-31 发布　　2014-07-15 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。

请注意本文件的某些内容可能涉及专利，本文件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。

本标准的起草单位：兴唐通信科技有限公司。

本标准的主要起草人：朱晖、孙正红、李健巍、李茜、侯长江、刘尚焱、周斌。

移动通信智能终端操作系统安全技术要求（EAL2级）

1 范围

本标准规定了EAL2级移动通信智能终端操作系统的安全技术要求。

本标准适用于移动通信智能终端操作系统安全的设计、开发、测试和评估。

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 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型

GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求

ISO/IEC 15408-3:2008 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求(Information technology—Security techniques—Evaluation criteria for IT security—Part 3:Security assurance components)

IEEE 802(所有部分) 局域网和城域网 (Local and metropolitan area networks)

3 术语、定义和缩略语

3.1 术语和定义

GB/T 18336.1—2008界定的以及下列术语和定义适用于本文件。

3.1.1

移动通信智能终端 smart mobile terminal

通过蜂窝移动通信网络向用户提供语音、消息、电子邮件、Web浏览等服务，集成照相机、摄像机、音乐、视频播放器、电视机、定位导航等功能的个人手持通信设备，可以下载、安装应用软件，是具备移动通信功能的手持式电脑。

3.1.2

移动通信智能终端操作系统 smart mobile terminal operating system

运行在移动通信终端上的系统软件，控制、管理移动终端上的硬件和软件，提供用户操作界面和应用软件编程接口。

注：移动通信智能终端操作系统管理的资源中涉及用户利益的资源有通信资源、信源传感器和存储用户信息的存储器等。

3.1.3

用户 user

在移动通信智能终端操作系统之外，与移动通信智能终端操作系统交互的任何实体(人员用户或外部IT实体)。

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

持有者　holder

移动通信智能终端的合法使用者。

3.1.6

管理员　administrator

是一个授权用户，拥有管理部分或全部移动通信智能终端操作系统安全功能的权限，同时可能拥有旁路部分移动通信智能终端操作系统安全策略的特权。

3.1.7

人员用户　human user

与移动通信智能终端操作系统交互的任何人员。

3.1.8

角色　role

一组预先确定的规则，规定用户和移动通信智能终端操作系统之间所允许的交互行为。

3.1.9

应用软件　application software

移动智能终端操作系统之外，向用户提供服务功能的软件。

3.1.10

主体　subject

在移动通信智能终端操作系统安全功能控制下实施操作的实体。

3.1.11

客体　object

在移动通信智能终端操作系统安全功能控制下被主体实施操作的实体。

3.1.12

介导　mediate

以一个中间步骤来传递或起媒介的作用。

注：授权主体通过操作系统安全功能介导实现对系统资源、用户数据的访问。

3.1.13

鉴别数据　authentication data

用于验证用户所声称身份的信息。

3.1.14

用户数据　user data

由用户产生或为用户服务的数据，这些数据不影响 TOE 安全功能的运行。

3.1.15

安全属性　security attribute

是用户、主体、客体、信息、会话及资源的特性，此特性用于定义安全功能要求，其值用于实施安全功能要求。

3.1.16

移动终端安全功能数据　TSF data

实施移动终端操作系统安全功能所依赖的数据。

3.1.17

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。

3.1.18

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。

3.1.19

评估对象　target of evaluation

被评估的 IT 产品，包括使用指南。本标准指移动通信智能终端操作系统。

3.1.20

移动终端操作系统安全功能　TOE security functions

移动终端操作系统正确、完整实现安全功能要求所依赖的所有软件、固件、硬件的功能集合。

3.2　缩略语

下列缩略语适用于本文件。

SFP：安全功能策略（Security Function Policy）

TOE：评估对象（Target of Evaluation）

TSF：TOE 安全功能（TOE Security Functions）

TSFI：TOE 安全功能接口（TSF Interface）

4　概述

4.1　TOE 类型

移动通信智能终端（以下简称移动终端）操作系统是单人员用户使用的手持操作系统，主要目的是向用户提供良好的操作界面，便于用户使用移动终端的功能。随着处理器能力的提高及移动通信技术的发展，移动终端能够通过多种方式接入互联网或其他计算机系统，并支持各种商业应用。

移动终端操作系统的特点是开放应用软件可编程接口（API）或开放操作系统源文件，由此带来的安全威胁使得安全功能成为移动智能终端操作系统必不可少的组成部分。

移动终端操作系统管理移动终端硬件、软件。移动终端上与用户利益直接相关的硬件包括：通信设备（蜂窝移动通信设备、无线局域网设备）、终端信源传感器（麦克、摄像头、加速度计、定位导航系统）、终端输入输出设备（红外线接口、蓝牙、USB 接口、SDIO 接口）等。与用户利益直接相关的软件包括存储用户信息的文件（通讯录、通信记录、短消息、电子邮件、记事本等）以及相关应用软件。

操作系统边界内的软件由操作系统的核心软件部分组成，边界内的软件受到操作系统运行平台保护不被非可信主体干扰，并且不受操作系统安全策略限制。操作系统边界外的应用软件对系统资源的访问受到操作系统安全策略的限制，应用软件对系统资源的访问应在操作系统安全功能介导下进行。

移动终端操作系统应具备下述特征：

a)　在手持式单机硬件平台上工作；

b)　单人员用户使用；

c)　支持多个管理员角色；

d)　支持应用软件安装；

e)　应用软件通过操作系统介导访问数据、传感器及无线通信资源；

f) 支持基于 IP 协议的网络通信；

g) 可以与远程 IT 系统协同工作。

4.2 TOE 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。

移动终端操作系统不提供多人员用户的隔离机制，移动终端失去物理保护时，可能受到非授权人员用户的恶意访问。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、备份数据保护等功能应对此类威胁，防范用户数据的泄露和丢失。

除使用者外，移动终端还可能存在多个授权用户，包括维修人员、各种服务人员和开发者等理论上的可信用户。这些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。本标准并不要求充分抵御授权用户的恶意行为，但要求移动终端操作系统依据最小特权原则，通过划分角色对授权用户的权限加以限制。

支持应用软件是移动智能终端的基本特征，恶意软件的安装和运行构成移动终端主要的安全威胁。移动终端可通过两类措施抵御恶意软件的威胁：

a) 安装可信的应用软件；

b) 执行安全功能策略(访问控制策略和信息流控制策略)对应用软件的访问加以限制。

移动终端安装可信应用软件的基础是采取技术手段维系移动终端与应用软件责任担保者之间的信任传递链条，因此移动终端操作系统应具备下述安全功能：

a) TSF 间用户数据保密性传送、完整性传送(如由可信应用商店承担应用软件的担保责任)；

b) 带安全属性的用户数据输入(如由可信第三方承担应用软件的担保责任)；

c) 可信信道(如终端与可信应用商店或可信第三方建立可信通道)。

移动终端很难完全避免恶意软件的安装，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权限，使移动终端自身具备一定的安全防护能力。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。

与大型的专业计算机系统不同，通常情况下，移动终端没有实时在线管理员对安全异常事件做出响应，移动终端使用者也难以胜任全部安全管理职能。移动终端操作系统应通过安全角色的划分，把对用户数据、通信资源的访问授权管理职能赋予使用者，即移动终端持有者，而允许选择把复杂的安全管理职能(例如卸载已安装的恶意软件、操作系统升级、安全策略的更改)赋予在远程可信 IT 系统上工作的专业技术用户(比如，远程管理员)，以实现远程可信 IT 系统对移动终端的管理。

移动终端操作系统内置 IP 网络通信协议。IP 网所有数据包和控制包都在一个公共管道上传送，不能将不同用户、不同用途的信息流分割到独立的通道中，IP 网又提供了“任意到任意”和“端到端”的连通性。因此，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。

此外，移动终端操作系统及其安全功能也应得到保护，移动终端安全构架应确保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。

移动终端操作系统高级别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特征如下：

a) 给每个用户、应用、主体、进程分配唯一的标识；

b) 在允许授权人员用户或远程 IT 实体施行操作前，对他们的身份进行鉴别；

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 IT 系统对移动终端的安全管理；
f) 执行访问授权管理，即持有者能够根据需要初始化、配置、修改应用软件的访问权限；
g) 对个体行为审计；
h) 提供密码支持。

5 移动终端操作系统安全问题

5.1 假设

5.1.1 授权用户（A.AUTHORIZED_USER）

授权用户是负责的、无恶意的，没有违背持有人意愿的行为。

5.1.2 可信的 SIM 卡（A.TRUSTED SIM）

移动终端操作系统与 SIM 卡的交互符合国际相关通信及安全标准，SIM 卡承载的应用是可信应用。

5.1.3 远程可信 IT 系统（A.TRUSTED_REMOTE）

移动终端操作系统与远程可信 IT 实体配合，实施某些安全功能。

5.1.4 TSF 保护（A.HARDWARE_PROTECTION 或 A.PRIVILEGE_MODE）

移动终端操作系统运行的基础平台提供特对操作系统的保护，保证移动终端操作系统安全功能得到保护，不被干扰、破坏和篡改。

5.2 资产

在移动终端中需要保护的资产有：
——用户数据：包含位置信息、账户信息、通信记录、通讯录等。
——移动终端敏感资源：包含通信资源、外设接口，如摄像头、位置传感器等。
——移动终端操作系统安全功能数据：包含鉴别数据、安全属性等。

5.3 安全威胁

5.3.1 用户数据丢失（T.LOSS_THEFT）

由于丢失或被盗，可能导致用户数据丢失。

5.3.2 非授权人员访问（T.UNAUTHORIZED_ENTRY）

非授权人员试图访问移动终端上的用户数据和系统敏感资源，例如在手机丢失或被盗的情况下非授权人员访问移动终端。

5.3.3 用户配置错误（T.USER_CONFIGRATION_ERROR）

不具备安全意识或安全意识薄弱的用户通过不正确地配置，使移动终端安全受到威胁。

5.3.4 危及 TSF 安全（T.TSF_COMPROMISE）

恶意用户、进程可能查看、更改或删除 TSF 数据或可执行代码，危及 TSF 的安全。

5.3.5 非授权网络流量(T.UNAUTHORIZED_ NETTRAFFIC)

未授权外部 IT 实体向 TOE 发送网络数据或接收经由 TOE 路由的网络数据。

5.3.6 授权人员用户的恶意行为(T.ACCESS_MALICIOUS)

授权用户利用权限进行非法操作,比如,维修人员在设备维护期间窃取用户隐私、安装恶意软件,或进行其他违背持有者意愿的行为。

5.3.7 恶意软件(T.MALICIOUS_SOFTWARE)

恶意软件可能通过伪装成授权应用或进程非授权访问用户数据和系统敏感资源,比如,木马或病毒。

5.3.8 数据备份(T.DATA_BACKUP)

攻击者可能在备份数据传送过程中被窃取或破坏用户数据。

5.3.9 设备管理(T. DEVICE_MANAGEMENT)

攻击者可能在设备管理过程中篡改、破坏管理数据、配置数据和系统更新数据。

5.4 组织安全策略

5.4.1 按需授予(P.NEED_TO_KNOW)

限制授权用户及主体访问能力的原则是按需给予。

5.4.2 访问授权管理(P.ACCESS_ AUTHORIZATION_MANAGE)

移动终端操作系统应向用户提供访问授权管理能力。(比如,用户可进行一定的访问限制管理配置,以限制应用软件的访问能力。因为手机没有一个实时在线的管理员对手机安全进行管理。)

5.4.3 明确提示(P. VISIBLE_PROMPT)

当访问与安全、法律有关的用户数据和系统敏感资源时,移动终端操作系统应能够向用户提供明确的提示。

5.4.4 标识和鉴别(P.I_AND_A)

移动终端的用户、应用软件、进程、主体、客体都应被分配唯一的标识,并在执行访问和实施动作之前加以鉴别。

5.4.5 追溯(P.TRACE)

主体行为可以被追溯。

5.4.6 密码(P.CRYPTOGRAPHY)

移动终端操作系统安全功能应得到密码技术的支持,密码算法应符合国家和行业的信息技术安全标准或规范。

5.4.7 网络连接(P.NETWORK)

移动终端操作系统用户通过互联网访问远程可信 IT 实体(应用软件商店、运营商服务器、设备管

理系统、邮件服务器)时应能够建立安全连接。

6 移动通信智能终端操作系统安全目的

6.1 设备访问(O.DEVICE_ACCESS)

用户、进程、主体应通过授权访问方式访问用户数据及系统敏感资源。

6.2 管理员角色(O.ADMINISTRATOR_ROLE)

设置管理员角色以隔离管理员行为。

6.3 会话锁定(O.SESSION_LOCK)

移动终端操作系统应能在不活动时间达到规定值时锁定会话。同时也应支持由用户发起的会话锁定。重新激活终端应经过用户的再次鉴别。

6.4 审计产生(O.AUDIT_GENERATION)

移动终端操作系统具备检测与安全有关事件的能力,并产生审计记录。

6.5 审计保护(O.AUDIT_PROTECTION)

保护审计信息。

6.6 审计调阅(O.AUDIT_REVIEW)

具备选择性审阅审计信息的能力。

6.7 管理(O.MANAGE)

向管理员提供管理移动终端操作系统安全的功能,并限制非授权用户使用此项功能。

6.8 用户数据备份(O.USERDATA_BACKUP)

移动终端操作系统应提供用户数据备份机制。

6.9 域隔离(O.DOMAIN_ISOLATION)

提供域隔离机制,保护自身及资源不受到外部冲突、篡改或破坏。

6.10 密码服务(O.CRYPTOGRAPHIC_SERVICES)

移动终端操作系统应为安全功能的实施提供密码服务。

6.11 鉴别(O.USER_AUTHENTICATION)

鉴别用户、应用软件的身份。

6.12 标识(O.USER_IDENTIFICATION)

给用户、应用软件分配唯一的标识。

6.13 应用软件限制(O.APPLICATION_RESTRICT)

在应用软件安装、运行时,对应用软件进行限制。

6.14 网络信息流控制(O.NETWORK_FLOW_CONTROL)

移动终端操作系统依据信息流控制策略与远程 IT 实体通信。

6.15 备份数据保护(O.BACKUP_DATA_PROTECT)

移动终端操作系统应在备份数据输出前对数据进行保密性和完整性保护。

6.16 设备管理 (O.DEVICE_MANAGEMENT)

移动终端操作系统应保护设备管理过程中传送的管理数据、配置数据和系统更新数据。

6.17 网络连接(O.NETWORK)

移动终端操作系统与远程可信 IT 实体通信应建立安全连接。

7 移动终端操作系统安全功能要求

7.1 表达方式

依据 GB/T 18336.1—2008,对安全功能要求的表达使用赋值、反复、选择、细化的方式。

注:本文用正常字体表示已完成的赋值、选择和细化。用括号"【】"内的加粗字体表示有待赋值和选择的内容。用安全功能组件后括号"()"内的字符,表示对一个安全功能组件的反复使用或限定使用。用"_EXT"表示族或组件的扩展。

7.2 扩展组件说明

移动终端操作系统扩展的安全功能组件在表 1 中列出。

表 1 扩展的安全功能要求组件

扩展组件	扩展组件名称	说 明
FCS_CBR_EXT.1	密码支持基本要求	7.7.2
FCS_COA_EXT.1	密码操作应用	7.7.3

7.3 用户数据保护

7.3.1 安全功能策略

移动终端操作系统安全功能策略包含应用软件限制 SFP、设备访问控制 SFP、网络信息流控制 SPF、管理信息流控制 SFP:

a) 应用软件限制 SFP 用于限制非可信应用软件的安装和执行;
b) 设备访问控制 SFP 用于防止非授权用户对用户数据的访问和对系统敏感资源的使用;
c) 网络信息流控制 SFP 用于防止移动终端产生或接收未知的网络流量,造成移动用户资费及无线资源的损失;
d) 管理信息流控制 SFP 是预防非授权或假冒的管理信息造成对移动终端的安全危害。

7.3.2 用户数据保护类架构

用户数据保护类架构见图 1。

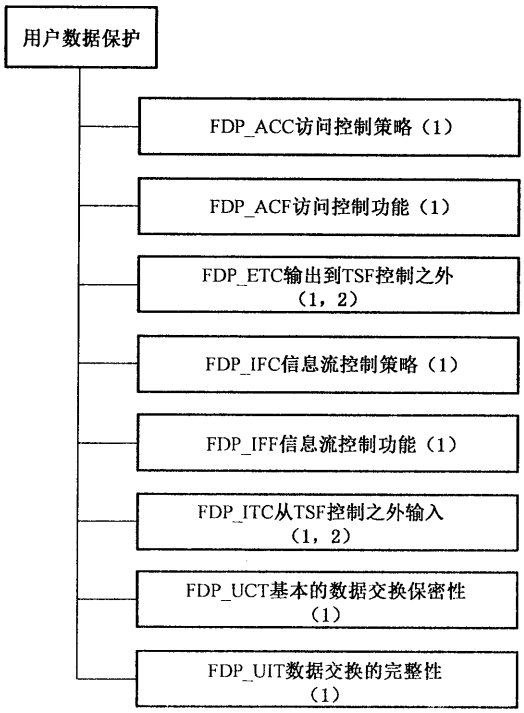

图 1　用户数据保护类架构

7.3.3　子集访问控制(AP)(FDP_ACC.1)(AP:应用软件)

从属于:无。

依赖:FDP_ACF.1(AP)　基于安全属性的访问控制。

FDP_ACC.1.1 移动终端操作系统的安全功能应对如下主体、客体及主体和客体之间的操作执行应用软件限制 SFP:

a)　主体:代表安装文件、动态链接文件和可执行文件行为的系统管理进程;

b)　客体:移动设备资源;

c)　操作:安装、加载。

7.3.4　基于安全属性的访问控制(AP)(FDP_ACF.1)(AP:应用软件)

从属于:无。

依赖:FDP_ACC.1 (AP)子集访问控制;

FMT_MSA.3 静态属性初始化。

FDP_ACF.1.1 移动终端操作系统的安全功能应在代表安装文件、动态链接文件和可执行文件行为的系统管理进程对客体进行操作时,依据主体的安全属性,实施应用软件限制 SFP:

a)　安装文件:安装文件提供商的标识或数字签名、文件撤销列表、**【赋值:其他属性】**;

b)　动态链接文件:动态链接文件提供商的标识或数字签名、文件撤销列表、**【赋值:其他属性】**;

c)　可执行文件:可执行文件提供商的标识或数字签名、文件撤销列表、**【赋值:其他属性】**。

FDP_ACF.1.2 移动终端操作系统的安全功能应依据如下规则,决定安装文件、动态链接文件和可执行文件的安装和加载是否允许:

a)　若安装文件、动态链接文件和可执行文件提供商的标识或数字签名是可信的,则允许安装和加载;

b) 若安装文件、动态链接文件和可执行文件提供商的标识或数字签名是不可识别或无标识、无数字签名，则需要明确提示持有者，由其决定安装和加载。

FDP_ACF.1.3 移动终端操作系统的安全功能应无附加规则，明确允许安装文件、动态链接文件和可执行文件的安装和加载：

FDP_ACF.1.4 移动终端操作系统的安全功能应维护应用软件撤销列表，若安装文件、动态链接文件和可执行文件在应用软件撤销列表中、**【赋值：其他附加规则】**中，则明确拒绝安装和加载。

7.3.5 子集访问控制(DA)(FDP_ACC.1)(DA：设备访问控制)

从属于：无。

依赖：FDP_ACF.1(DA) 基于安全属性的访问控制。

FDP_ACC.1.1 移动终端操作系统的安全功能应对所有代表应用软件的进程，对**【赋值：与用户隐私及用户利益相关的客体，如用户数据文件、敏感资源等】**进行**【赋值：执行动作列表(如读、写、执行、打开/关闭等操作)】**时，执行设备访问控制 SFP。

应用注释：与用户利益相关的敏感资源有：终端通信设备(如移动通信设备、无线局域网设备)，终端信源传感器(如麦克、摄像头、加速度计、定位导航系统)，终端外部输入输出设备等(如红外线接口、蓝牙)；与用户隐私相关的客体有：存储用户信息的文件(如通讯录本、通信记录、短消息、电子邮件等)。

7.3.6 基于安全属性的访问控制(DA)(FDP_ACF.1)(DA：设备访问控制)

从属于：无。

依赖：FDP_ACC.1 (DA)子集访问控制；

FMT_MSA.3 静态属性初始化。

FDP_ACF.1.1 移动终端操作系统的安全功能应对所有代表应用软件的进程对用户数据及系统敏感资源进行访问时，依据如下的安全属性，实施设备访问控制 SFP：

【选择：

a) **应用标识、应用组标识、及其访问能力参数；**

b) **客体标识及访问控制列表；**

c) **【赋值：应用软件的其他属性，客体的其他属性】。**

】

FDP_ACF.1.2 移动终端操作系统的安全功能应依据如下规则，决定代表应用软件的进程对受控客体的操作是否允许：

a) 如果应用软件要求的访问方式没有允许，则拒绝访问；

b) 如果应用软件要求的访问方式被允许，则允许访问；

c) 如果应用软件所属于的每一个组所要求的访问方式被拒绝，则拒绝访问；

d) 如果应用软件所属于的任何一个组所要求的访问方式被允许，则允许访问；

e) 其他，则拒绝访问。

FDP_ACF.1.3 移动终端操作系统的安全功能应无附加规则，明确允许代表应用软件的进程对受控客体的授权访问。

FDP_ACF.1.4 移动终端操作系统的安全功能应依据如下附加规则，明确拒绝代表应用软件的进程对受控客体的访问：

a) 应用软件在应用软件撤销列表中；

b) **【赋值：与用户隐私或利益相关的客体列表】**的访问未获用户许可。

7.3.7 不带安全属性的用户数据输出(UD)(FDP_ETC.1)(UD：用户数据)

从属于：无。

依赖:FDP_ACC.1 (DA)子集访问控制和/或 FDP_IFC.1 (NIC)子集信息流控制。

FDP_ETC.1.1 在安全功能策略覆盖下的用户数据输出到 TOE 之外时,移动终端操作系统的安全功能应实施设备访问控制 SFP 和/或网络信息流控制 SFP。

FDP_ETC.1.2 移动终端操作系统的安全功能应能输出用户数据,但不带有用户数据关联的安全属性。

应用注释:在不带与用户数据关联的安全属性输出用户数据时,对用户数据的保护要依赖环境。

7.3.8 带安全属性的用户数据输出(FDP_ETC.2)

从属于:无。

依赖:FDP_ACC.1 (DA)子集访问控制和/或 FDP_IFC.1(NIC)子集信息流控制和/或
FDP_IFC.1 (MIC)子集信息流控制;
FCS_CPR_EXT.1 密码提供要求。

FDP_ETC.2.1 在安全功能策略覆盖下的用户数据输出到 TOE 之外时,移动终端操作系统的安全功能应实施设备访问控制 SFP 和/或网络信息流控制 SFP 和/或管理信息流控制 SFP。

FDP_ETC.2.2 移动终端操作系统的安全功能应输出用户数据且带有与用户数据关联的安全属性。

FDP_ETC.2.3 移动终端操作系统的安全功能应确保安全属性,在输出到 TOE 之外时,与所输出的用户数据明确关联。

FDP_ETC.2.4 当用户数据输出到 TOE 之外时,移动终端操作系统的安全功能应实施规则**【选择:对用户数据加密保护,【赋值:附加的输出控制规则】】**。

7.3.9 子集信息流控制(NIC)(FDP_IFC.1)(NIC:网络信息流控制 SFP)

从属于:无。

依赖:FDP_IFF.1 (NIC)简单安全属性。

FDP_IFC.1.1 移动终端操作系统的安全功能应对下列主体和网络信息流及其操作实施网络信息流控制 SFP:

a) 主体:
   1) 在 TOE 介导下发送和接收网络信息的没有鉴别的外部 IT 实体;
   2) **【赋值:其他由 TOE 介导发送、接收网络信息的其他主体】**。
b) 信息:经 TOE 路由的网络数据;
c) 操作:导致信息流动的所有操作。

应用注释:操作可能是发送、接收、转发、丢弃或对发送方的一个应答。

7.3.10 简单安全属性(NIC)(FDP_IFF.1)(NIC:网络信息流控制 SFP)

从属于:无。

依赖:FDP_IFC.1(NIC) 子集信息流控制;
FMT_MSA.3 静态属性初始化。

FDP_IFF.1.1 移动终端操作系统的安全功能应基于下列主体类型和网络信息的安全属性,实施网络信息流控制 SFP:

a) 客体属性(与主体类型相关):
   1) 网络数据所通过的逻辑或物理的网络接口;
   2) **【赋值:其他客体属性】**。
b) TCP/IP 信息的安全属性:
   1) 源和目的的 IP 地址;

2) 源和目的的 TCP 端口；

3) 源和目的的 UDP 端口；

4) IP、TCP、UDP、ICMP 或**【赋值：其他】**的协议；

5) TCP 的头标识**【选择：SYN、ACK、【赋值：其他标识】】**；

6) **【赋值：IP 包的其他属性】**。

c) **【选择：**

IEEE 802 信息的安全属性：

1) **MAC 地址；**

2) **【赋值：其他属性】**。

】。

FDP_IFF.1.2 移动终端操作系统的安全功能应在规则**【赋值：对每一个操作，应在主体和信息的安全属性间保持的基于安全属性的关系】**下，允许受控的网络信息通过受控操作经受控主体流动。

FDP_IFF.1.3 移动终端操作系统的安全功能应执行**【赋值：附加的网络数据流 SFP 规则】**。

FDP_IFF.1.4 移动终端操作系统的安全功能应依据规则**【赋值：基于安全属性的明确准许网络数据流 SFP 的规则】**明确准许网络信息流。

FDP_IFF.1.5 移动终端操作系统的安全功能应依据规则**【赋值：基于安全属性的明确拒绝网络数据流 SFP 的规则】**明确拒绝网络信息流。

应用注释：FDP_IFF.1.3 附加规则可以是基于 TCP 连接状态的匹配，基于时间的匹配，统计分析匹配，对符合条件的网络数据进行相应的操作处理。

7.3.11 子集信息流控制(MIC)(FDP_IFC.1)(MIC：管理信息流控制 SFP)

从属于：无。

依赖：FDP_IFF.1 (MIC)简单安全属性。

FDP_IFC.1.1 移动终端操作系统的安全功能应对下列主体和管理信息流及其操作实施管理信息流控制 SFP：

a) 主体：

1) 移动终端/设备管理客户端；

2) 远程可信管理服务器；

3) **【赋值：其他由 TOE 介导发送、接收管理信息的其他主体】**。

b) 信息：管理信息流(如管理策略、安全策略、安全配置数据)等 TSF 数据；

c) 操作：导致管理信息流动的所有操作(如远程管理命令等)。

应用注释：远程可信管理服务器可以是终端设备提供商、系统提供商或移动通信运营商。操作可能是执行某一管理命令，如恢复初始配置命令、防止用户隐私泄露的清除用户数据命令等。

7.3.12 简单安全属性(MIC)(FDP_IFF.1)(MIC：管理信息流控制 SFP)

从属于：无。

依赖：FDP_IFC.1 (MIC)子集信息流控制；

FMT_MSA.3 静态属性初始化。

FDP_IFF.1.1 移动终端操作系统的安全功能应基于下列主体和信息的类型及其安全属性，实施管理信息流 SFP：

a) 移动终端/设备管理客户端：

【选择：

1) **根证书、远程可信管理服务器证书和移动终端私钥；**

2） **对远程可信管理服务器的鉴别数据；**

3） **赋值【其他安全属性】。**

】；

b） 远程可信管理服务器：

【选择：

1） **根证书、移动终端证书和远程可信管理服务器私钥；**

2） **对移动终端的鉴别数据；**

3） **【赋值：其他安全属性】。**

】。

FDP_IFF.1.2 移动终端操作系统的安全功能应依据如下规则：

a） 移动终端和远程可信管理服务器的双向鉴别；

b） **【选择：**

1） **建立移动终端和远程可信管理服务间的 IPSec 连接；**

2） **建立移动终端和远程可信管理服务间的 SSL/TLS 会话；**

3） **【赋值：其他规则】。**

】。

允许受控管理信息从移动终端或远程可信管理服务器通过受控操作流动。

FDP_IFF.1.3 移动终端操作系统的安全功能应执行规则**【赋值：附加的管理信息流控制规则】。**

FDP_IFF.1.4 移动终端操作系统的安全功能应依据规则**【赋值：基于安全属性的明确准许管理信息流的规则】**明确准许管理信息流动。

FDP_IFF.1.5 移动终端操作系统的安全功能应依据规则**【赋值：基于安全属性的明确拒绝管理信息流的规则】**明确拒绝管理信息流动。

7.3.13 不带安全属性的用户数据输入(AP)(FDP_ITC.1)(AP：应用软件)

从属于：无。

依赖：FDP_ACC.1 子集访问控制；

FMT_MSA.3 静态属性初始化。

FDP_ITC.1.1 在应用软件限制 SFP 覆盖下的应用软件安装和可执行文件由 TOE 外输入时，移动终端操作系统的安全功能应实施应用软件限制 SFP。

FDP_ITC.1.2 当从 TOE 外输入非可信应用软件安装和可执行文件时，移动终端操作系统的安全功能应忽略任何与应用软件安装和可执行文件相关的安全属性。

FDP_ITC.1.3 当从 TOE 外输入应用软件限制 SFP 覆盖下的应用软件安装和可执行文件时，移动终端操作系统的安全功能应执行规则**【赋值：附加的输入控制规则】。**

7.3.14 带安全属性的用户数据输入(AP)(FDP_ITC.2)(AP：应用软件)

从属于：无。

依赖：FDP_ACC.1 (AP)子集访问控制和/或 FDP_IFC.1 (NIC)子集信息流控制；

FTP_ITC.1 TSF 间可信信道或 FTP_TRP.1 可信路径；

FPT_TDC.1 TSF 间基本 TSF 数据一致性。

FDP_ITC.2.1 在应用软件限制 SFP 覆盖下的应用软件安装和可执行文件从 TOE 之外输入时，移动终端操作系统的安全功能应实施应用软件限制 SFP 和/或网络信息流控制 SFP。

FDP_ITC.2.2 移动终端操作系统的安全功能应使用与输入的应用软件安装和可执行文件关联的安全属性。

FDP_ITC.2.3 移动终端操作系统的安全功能应保证使用的协议提供了输入的应用软件安装和可执行文件与其安全属性的确定关联。

FDP_ITC.2.4 移动终端操作系统的安全功能应保证对输入的应用软件安装和可执行文件安全属性的解释与来源的意图相同。

FDP_ITC.2.5 在安全功能策略覆盖下的应用软件的安装文件和可执行文件从 TOE 之外输入时，移动终端操作系统的安全功能应实施规则【**赋值：附加的输入控制规则**】对应用软件的安装文件和可执行文件进行储存。

7.3.15 不带安全属性的用户数据输入(UD)(FDP_ITC.1)(UD：用户数据)

从属于：无。

依赖：FDP_ACC.1 (DA)子集访问控制和/或 FDP_IFC.1 (NIC)子集信息流控制；

FMT_MSA.3 静态属性初始化。

FDP_ITC.1.1 在安全功能策略覆盖下的用户数据由 TOE 外输入时，移动终端操作系统的安全功能应实施设备访问控制 SFP 和/或网络信息流控制 SFP。

FDP_ITC.1.2 当从 TOE 外输入用户数据时，移动终端操作系统的安全功能应忽略任何用户数据相关的安全属性。

FDP_ITC.1.3 当从 TOE 外输入设备访问控制 SFP 和/或网络信息流控制 SFP 覆盖下的用户数据时，移动终端操作系统的安全功能应执行规则【**赋值：附加的输入控制规则**】。

7.3.16 带安全属性的用户数据输入(FDP_ITC.2)

从属于：无。

依赖：FDP_ACC.1(DA) 子集访问控制和/或 FDP_IFC.1 (NIC)子集信息流控制；和/或

FDP_IFC.1 (MIC)子集信息流控制；

FTP_ITC.1 TSF 间可信信道或 FTP_TRP.1 可信路径；

FPT_TDC.1 TSF 间基本 TSF 数据一致性。

FDP_ITC.2.1 在安全功能策略覆盖下的用户数据从 TOE 之外输入时，移动终端操作系统的安全功能应实施设备访问控制 SFP 和/或网络信息流控制 SFP 和/或管理信息流控制 SFP。

FDP_ITC.2.2 移动终端操作系统的安全功能应使用与输入的用户数据关联的安全属性。

FDP_ITC.2.3 移动终端操作系统的安全功能应保证使用的协议提供了接收的数据与安全属性的确定关联。

FDP_ITC.2.4 移动终端操作系统的安全功能应保证对输入数据安全属性的解释与用户数据源的意图相同。

FDP_ITC.2.5 在安全功能策略覆盖下的用户数据从 TOE 之外输入时，移动终端操作系统的安全功能应实施规则【**赋值：附加的输入控制规则**】。

7.3.17 基本的数据交换保密性(FDP_UCT.1)

从属于：无。

依赖：FDP_ACC.1 (DA)子集访问控制和/或 FDP_IFC.1 (NIC)子集信息流控制；和/或

FDP_IFC.1 (MIC)子集信息流控制；

FTP_ITC.1 TSF 间可信信道或 FTP_TRP.1 可信路径。

FDP_UCT.1.1 移动终端操作系统的安全功能应实施设备访问控制 SFP 和/或网络信息流控制 SFP 和/或管理信息流控制 SFP，以便保护在传送和接收用户数据时免受非授权泄露。

7.3.18 数据交换的完整性(FDP_UIT.1)

从属于:无。

依赖:FDP_ACC.1 (DA)子集访问控制和/或 FDP_IFC.1(NIC)子集信息流控制;和/或
FDP_IFC.1 (MIC)子集信息流控制;
FTP_ITC.1 TSF 间可信信道或 FTP_TRP.1 可信路径。

FDP_UIT.1.1 移动终端操作系统的安全功能应实施设备访问控制 SFP 和/或网络信息流控制 SFP 和/或管理信息流控制 SFP,以便保护传送和接收用户数据时免于被**【选择:修改、删除、插入、重放】**。

FDP_UIT.1.2 移动终端操作系统的安全功能应能判断用户数据接收过程中是否发生了**【选择:修改、删除、插入、重放】**的错误。

7.4 标识与鉴别

7.4.1 标识与鉴别类架构

标识与鉴别类架构见图 2。

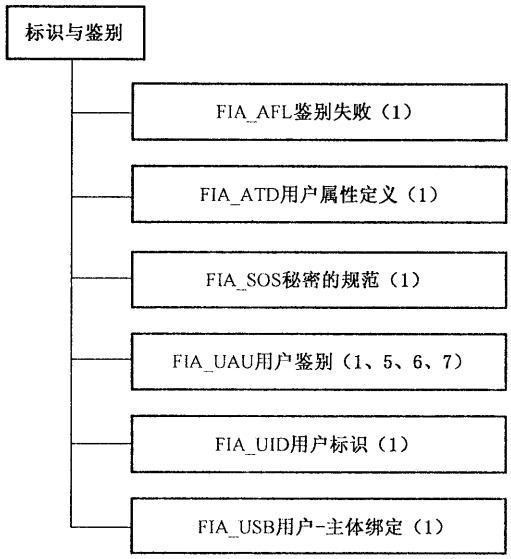

图 2 标识与鉴别类架构

7.4.2 鉴别失败处理(HU)(FIA_AFL.1)(HU:本地人员用户)

从属于:无。

依赖:FIA_UAU.1 鉴别的时机。

FIA_AFL.1.1 移动终端操作系统的安全功能应检测何时发生**【选择:【赋值:正整数】,管理员可设置的【赋值:可接受数值范围】内的整数】**次本地人员用户身份的未成功鉴别尝试。

FIA_AFL.1.2 当达到或超过所定义的未成功鉴别尝试次数时,移动终端操作系统安全功能应**【选择:删除用户数据、使终端失效、会话锁定一定时间、【赋值:其他动作列表】】**。

7.4.3 鉴别失败处理(RU)(FIA_AFL.1)(RU:远程用户)

从属于:无。

依赖:FIA_UAU.1 鉴别的时机。

FIA_AFL.1.1 移动终端操作系统的安全功能应检测何时发生**【选择：【赋值：正整数】，管理员可设置的【赋值：可接受数值范围】内的整数】**次远程访问的未成功鉴别尝试。

FIA_AFL.1.2 当达到或超过所定义的未成功鉴别尝试次数时，移动终端操作系统安全功能应**【选择：禁止建立会话、【赋值：其他动作列表】】**。

应用注释：如果移动终端操作系统开发商需要定义除上述之外的安全属性，则需在赋值中增加。移动终端操作系统远程用户可以是同一安全体系下的应用软件商店、设备管理系统等等，比如对应用来源的鉴别。

7.4.4 鉴别失败处理（RE）（FIA_AFL.1）（RE：重鉴别）

从属于：无。

依赖：FIA_UAU.1 鉴别的时机；FIA_UAU.6 重鉴别。

FIA_AFL.1.1 移动终端操作系统的安全功能应检测何时发生**【赋值：正整数】**次在 FIA_UAU.6 中定义的重鉴别事件的未成功鉴别尝试。

FIA_AFL.1.2 当达到或超过所定义的未成功鉴别尝试次数时，移动终端操作系统安全功能应：

a) FIA_UAU.6 定义的 1）失败处理：会话锁定一定时间；

b) FIA_UAU.6 定义的 2）失败处理：**【赋值：其他动作列表】**。

7.4.5 用户属性定义（HRU）（FIA_ATD.1）（HRU：本地人员及远程用户）

从属于：无。

依赖：无。

FIA_ATD.1.1 移动终端操作系统安全功能应维护人员用户和远程 IT 系统的下列安全属性：

a) 用户标识；

b) 鉴别数据；

c) 安全相关角色；

d) **【赋值：其他安全属性（如远程用户访问所使用的逻辑或物理外部接口、逻辑或物理网络接口）】**。

7.4.6 用户属性定义（AP）（FIA_ATD.1）（AP：应用软件）

从属于：无。

依赖：无。

FIA_ATD.1.1 移动终端操作系统安全功能应维护应用软件的下列安全属性：

a) 应用标识；

b) 组标识；

c) 完整性校验数据；

d) 访问能力参数；

e) **【赋值：其他安全属性】**。

7.4.7 秘密的规范（FIA_SOS.1）

从属于：无。

依赖：无。

FIA_SOS.1.1 移动终端操作系统的安全功能应针对不同的秘密形式，提供机制以验证秘密是否满足相应的质量度量：

【选择：

a) 口令形式：字符数应不少于【赋值：正整数】，并且满足【赋值：数字、字母、符号的组合规则】；

b) 图形方式：输入的像素个数不少于【赋值：正整数】；

c) PIN 码方式：输入的数字个数不少于 4；

d) 其他秘密形式：【赋值：其他的验证方式】。

】

7.4.8 鉴别的时机(HU)(FIA_UAU.1)(HU：本地人员用户)

从属于：无。

依赖：FIA_UID.1 标识的时机。

FIA_UAU.1.1 在人员用户被鉴别前，移动终端操作系统安全功能应允许执行以下行为：

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(用户所选的运营商和照片的信息)；

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：其他在 TSF 介导下的动作】。**

FIA_UAU.1.2 在执行任何其他 TSF 介导的动作前，移动终端操作系统安全功能应要求每个人员用户都已被成功鉴别。

7.4.9 鉴别的时机(RU)(FIA_UAU.1)(RU：远程用户)

从属于：无。

依赖：FIA_UID.1 标识的时机。

FIA_UAU.1.1 在远程用户被鉴别前，移动终端操作系统安全功能应允许执行：

a) 网络信息流控制策略覆盖下的信息流动；

b) **【赋值：其他在 TSF 介导下的动作】。**

FIA_UAU.1.2 在执行任何其他 TSF 介导的动作前，移动终端操作系统安全功能应要求每个远程用户都已被成功鉴别。

应用注释：此远程用户为同一安全体系下的 IT 系统，如应用软件商店、设备管理系统等。

7.4.10 多种鉴别(FIA_UAU.5)

从属于：无。

依赖：无。

FIA_UAU.5.1 移动终端操作系统安全功能应提供下述鉴别机制：

a) 基于口令的鉴别；

b) 基于密码技术的鉴别；

c) **【赋值：其他鉴别机制】。**

FIA_UAU.5.2 移动终端操作系统安全功能应依据下述规则鉴别用户所声称的身份：

a) 鉴别人员用户所声称的身份时，采用**【选择：基于口令的鉴别机制，【赋值：其他鉴别机制】】**；

b) 鉴别应用软件来源时，采用**【选择：基于密码技术的鉴别机制，【赋值：其他鉴别机制】】**；

c) 鉴别远程 IT 实体时，采用**【选择：基于密码技术的鉴别机制，【赋值：其他鉴别机制】】**；

d) **【赋值：其他多种鉴别机制如何提供鉴别的规则】**。

应用注释：如果移动终端操作系统还支持生物识别、SDIO 等鉴别机制，则可以在 FIA_UAU.5.1 的赋值中添加。

7.4.11 重鉴别(FIA_UAU.6)

从属于：无。

依赖：无。

FIA_UAU.6.1 移动终端操作系统安全功能应在下述条件重新鉴别用户：

a) 用户重新设置鉴别数据；

b) **【赋值：其他需要重鉴别的条件】**。

应用注释：当用户访问 TOE 某些安全相关重要功能(比如安全管理等)或用户隐私数据时可进行重鉴别。

7.4.12 受保护的鉴别反馈(FIA_UAU.7)

从属与：无。

依赖：FIA_UAU.1 鉴别的时机。

FIA_UAU.7.1 移动终端操作系统安全功能应针对不同的鉴别形式，提供受保护的鉴别反馈：

a) 口令形式：仅向用户反馈字符占位，而不反馈鉴别数据原始字符；

b) 图形形式：仅向用户反馈图形点位，而不反馈图形的串联轨迹。

7.4.13 标识的时机(AP)(FIA_UID.1)(AP：应用软件)

从属于：无。

依赖：FDP_ITC.1 不带安全属性的用户数据输入和/或 FDP_ITC.2 带安全属性的用户数据输入。

FIA_ UID.1.1 在标识应用软件之前，移动终端操作系统安全功能应允许执行应用软件的安装。

FIA_ UID.1.2 在允许执行代表该应用软件的任何其他移动终端操作系统安全功能介导动作之前，移动终端操作系统安全功能应要求每个应用软件都已被成功标识。

应用注释：当应用软件被成功安装后，移动终端操作系统安全功能应为其分配唯一代表其身份的标识。

7.4.14 用户_主体绑定(FIA_USB.1)

从属于：无。

依赖：FIA_ATD.1 用户属性定义。

FIA_USB.1.1 移动终端操作系统安全功能应将下述用户安全属性与代表用户行为的主体(进程)进行关联：

a) FIA_ATD.1(HRU)定义的 a)、c)和 d)中与 TOE 安全策略实施相关的用户属性；

b) FIA_ATD.1(AU)定义的 a)、b)、d)和 e)中与 TOE 安全策略实施相关的用户属性。

FIA_USB.1.2 移动终端操作系统安全功能应执行规则**【赋值：属性初始关联规则】**将用户安全属性与代表用户活动的主体初始关联。

FIA_USB.1.3 移动终端操作系统安全功能应执行规则**【赋值：属性更改规则】**管理与代表用户活动的主体相关联的用户安全属性的改变。

应用注释：访问控制策略和审计策略要求每个代表用户行为的主体具备一个与用户相关联的身份。

比如自主访问控制策略将依据用户的身份执行访问控制决策。并非所有的用户安全属性都与主体关联，只有与 TOE 安全策略执行相关的属性才与主体关联。

7.5 安全管理

7.5.1 安全管理类架构

安全管理类架构见图 3。

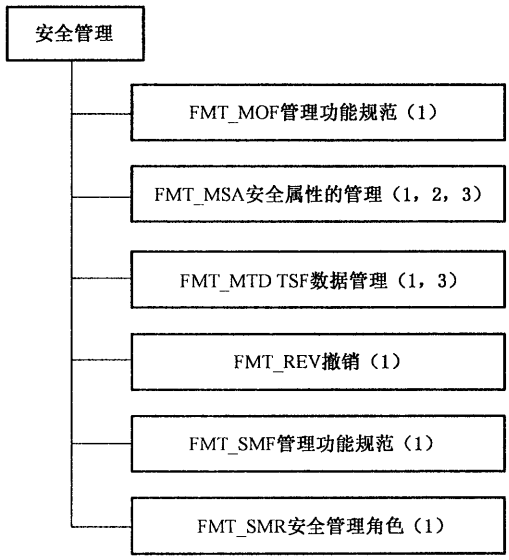

图 3 安全管理类架构

7.5.2 安全功能行为的管理(ADM)(FMT_MOF.1)(ADM：管理员角色)

从属于：无。

依赖：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MOF.1.1 移动终端操作系统的安全功能应仅限于管理员角色对应用软件限制、设备访问控制功能具有确定其行为、终止、激活、修改其行为的能力。

7.5.3 安全功能行为的管理(AUM)(FMT_MOF.1)(AUM：审计管理员角色)

从属于：无。

依赖：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MOF.1.1 移动终端操作系统的安全功能应仅限于审计管理员角色对审计功能具有确定其行为、终止、激活、修改其行为的能力。

7.5.4 安全属性管理(DA)(FMT_MSA.1)(DA：设备访问控制)

从属于：无。

依赖：FDP_ACC.1 (DA)子集访问控制；

FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MSA.1.1 移动终端操作系统的安全功能执行设备访问控制 SFP，以仅限于授权用户能够对敏感资源、用户数据的安全属性进行查询、修改。

应用注释：持有者可对应用软件的访问授权进行管理，以授予来源不同的应用软件不同的访问控制权限，如对某微博软件授予允许发送短信的权限，而对某播放器软件不允许其使用摄像镜头、位置信息的权限。

7.5.5 安全的安全属性(FMT_MSA.2)

从属于：无。

依赖：FDP_ACC.1 子集访问控制和/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 移动终端操作系统的安全功能应确保安全属性只接收安全的值。

7.5.6 静态属性初始化(FMT_MSA.3)

从属于：无。

依赖：FMT_MSA.1 安全属性的管理；

FMT_SMR.1 安全角色。

FMT_MSA.3.1 移动终端操作系统的安全功能应执行应用软件限制 SFP、设备访问控制 SFP、IP 网络信息流控制 SFP、管理信息流控制 SFP，为用于执行安全功能策略的安全属性提供受限的默认值。

FMT_MSA.3.2 移动终端操作系统的安全功能应允许管理员、授权用户在创建客体或信息时，用替换性的初始值代替原默认值。

7.5.7 TSF 数据的管理(NON_A)(FMT_MTD.1)(NON_A：非审计数据的 TSF 数据)

从属于：无。

依赖：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MTD.1.1 移动终端操作系统的安全功能应仅限于管理员能够**【赋值：TSF 数据列表】**进行**【选择：改变默认值、查询、修改、删除、清除、【赋值：其他操作】】**。

7.5.8 TSF 数据的管理(AU)(FMT_MTD.1)(AU：审计数据)

从属于：无。

依赖：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

FMT_MTD.1.1 移动终端操作系统的安全功能应仅限于审计管理员能够对审计数据进行**【选择：改变默认值、查询、修改、删除、清除、【赋值：其他操作】】**。

7.5.9 安全的 TSF 数据(FMT_MTD.3)

从属于：无。

依赖：FMT_MTD.1 TSF 数据的管理。

FMT_MTD.3.1 移动终端操作系统的安全功能应确保 TSF 数据仅接收安全的值。

7.5.10 安全属性撤销(AP)(FMT_REV.1)

从属于：无。

依赖：FMT_SMR.1 安全角色。

FMT_REV.1.1 移动终端操作系统的安全功能应仅限于管理员、授权用户能够撤销在 TSF 控制下与应用软件相关联的安全属性。

FMT_REV.1.2 移动终端操作系统的安全功能应执行规则：撤销将发生在对比应用软件撤销列表后。

7.5.11 管理功能规范(FMT_SMF.1)

从属于：无。

依赖：无。

FMT_SMF.1.1 移动终端操作系统的安全功能应能够执行下列安全管理功能：

a) 管理设备访问控制；

b) 管理应用软件限制；

c) 管理审计；

d) 管理网络信息流控制；

e) 管理用户的安全属性；

f) **【赋值：其他管理功能】**。

7.5.12 安全角色(FMT_SMR.1)

从属于：无。

依赖：FIA_UID.1 标识的时机。

FMT_SMR.1.1 移动终端操作系统的安全功能应预设以下角色：

a) 授权用户角色；

b) 非授权用户角色；

c) 审计管理员角色；

d) 管理员角色；

e) **【赋值：其他角色】**。

FMT_SMR.1.2 移动终端操作系统的安全功能应能够将用户与角色正确关联。

应用注释：对移动终端操作系统来说，角色以及对应管理的权限是预先设置。持有者与上述授权用户角色关联，具备一些与安全相关的管理能力，而与管理员角色关联的可以是本地设备维护人员或远程可信用户。

7.6 TOE 访问

7.6.1 TOE 访问类架构

TOE 访问类架构见图 4。

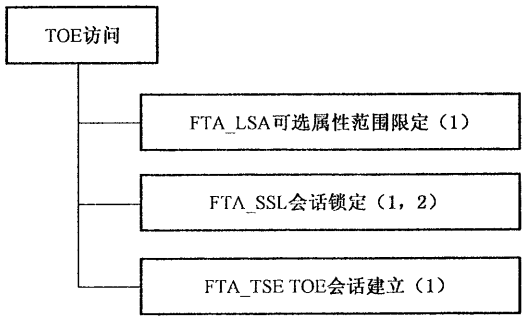

图 4 TOE 访问类架构

7.6.2 TSF 原发会话锁定(FTA_SSL.1)

从属于:无。

依赖:FIA_UAU.1 鉴别的时机。

FTA_SSL.1.1 移动终端操作系统安全功能应在达到管理员设置的用户会话不活动时间间隔后,通过以下方法锁定交互式会话:

a) 锁定显示屏仅显示 FIA_UAU.1 中所允许的通知和信息状态;

b) 使当前用户会话不可用,除了 FIA_UAU.1 中所允许的行为和解锁会话行为。

FTA_SSL.1.2 移动终端操作系统安全功能应要求在解锁会话之前成功地完成移动终端对人员用户的鉴别。

7.6.3 用户原发会话锁定(FTA_SSL.2)

从属于:无。

依赖:FIA_UAU.1 鉴别的时机。

FTA_SSL.2.1 移动终端操作系统安全功能应允许通过以下方法实现对交互会话进行用户原发锁定:

a) 锁定显示屏仅显示 FIA_UAU.1 中所允许的通知和信息状态;

b) 使当前用户会话不可用,除了 FIA_UAU.1 中所允许的行为和解锁会话行为。

FTA_SSL.2.2 移动终端操作系统安全功能应要求在解锁会话之前成功地完成移动终端对人员用户的鉴别。

7.6.4 TOE 会话建立(FTA_TSE.1)

从属于:无。

依赖:无。

FTA_TSE.1.1 移动终端操作系统安全功能应基于属性**【选择:用户身份、访问端口号、【赋值:其他安全属性】】**拒绝会话的建立。

7.6.5 可选属性范围限定(FTA_LSA.1)

从属于:无。

依赖:无。

FTA_LSA.1.1 移动终端操作系统安全功能应基于访问方法(用户身份、访问端口及访问时间等),限制下列会话的安全属性范围:审计管理员角色、管理员角色。

应用注释:此要求说明管理员只能用与普通用户不同的方法(物理和逻辑)建立 TOE 会话。

7.7 密码支持

7.7.1 密码支持类架构

密码支持类架构见图 5。

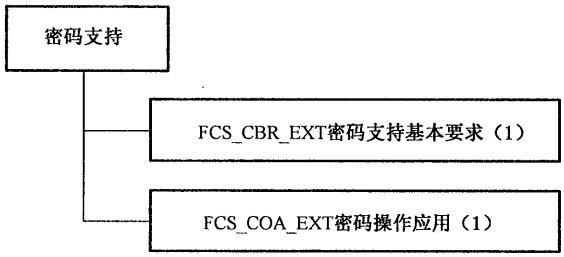

图 5　密码支持类架构

7.7.2　密码支持基本要求(FCS_CBR_EXT.1)

从属于:无。

依赖:无。

FCS_CBR.1.1：移动终端操作系统的安全功能提供的密码算法应符合**【赋值:相关国家标准】**,密码算法的实现应符合**【赋值:相关国家标准】**,密码算法操作所涉及的密钥管理应符合**【选择:国家标准GB/T 17901.1,【赋值:相关国家标准】】**。

7.7.3　密码操作应用(FCS_COA_EXT.1)

从属于:无。

依赖:FCS_CBR.1 密码支持基本要求。

FCS_CPR 1.1 移动终端操作系统的安全功能应提供下列密码操作:

a)　加密和解密;

b)　数字签名;

c)　杂凑;

d)　【赋值:其他密码操作】。

用于可信通道、用户数据保护、【赋值:其他应用】。

7.8　TSF 保护

7.8.1　TSF 保护类架构

TSF 保护类架构见图 6。

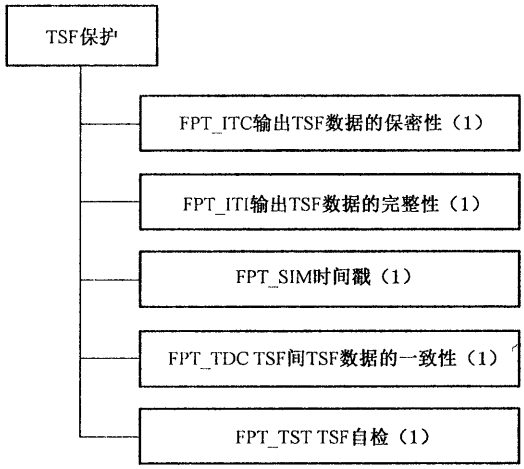

图 6　TSF 保护类架构

7.8.2 传送过程中 TSF 间的保密性(FPT_ITC.1)

从属于:无。

依赖:无。

FPT_ITC.1.1 在 TSF 数据从 TSF 到远程可信 IT 产品的传送过程中,TSF 应保护所有的 TSF 数据不被未授权泄漏。

7.8.3 TSF 间修改的检测(FPT_ITI.1)

从属于:无。

依赖:无。

FPT_ITI.1.1 TSF 应提供能力,在量度标准**【赋值:一个定义的修改度量标准】**下,检测 TSF 与远程可信 IT 产品间传送的所有 TSF 数据是否被修改。

FPT_ITI.1.2 TSF 应提供验证在 TSF 与远程可信 IT 产品间传送的所有 TSF 数据的完整性及执行,如果检测到修改将执行**【赋值:采取的行动】**。

应用注释 1:"一个定义的修改度量标准"指简单的校验和度量与密码技术校验度量,建议使用密码技术校验度量。

应用注释 2:**【赋值:采取的行动】**例如,忽略 TSF 数据,请求原始可信产品重新发送 TSF 数据。

7.8.4 可靠的时间戳(FPT_STM.1)

从属于:无。

依赖:无。

FPT_STM.1.1 TSF 应提供可靠的时间戳。

7.8.5 TSF 间基本 TSF 数据的一致性(FPT_TDC.1)

从属于:无。

依赖:无。

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】**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】**。

应用注释:该组件要求共享 TSF 数据的双方对 TSF 数据类型在同一规则下有相同的意义。

7.8.6 TSF 检测(FPT_TST.1)

从属于:无。

依赖:无。

FPT_TST.1.1 TSF 应在初始化启动期间以及**【赋值:产生自检的其他条件】**运行一套自检,以表明密码模块及**【选择:【赋值: 部分 TSF】,TSF】**操作的正确性。

FPT_TST.1.2 TSF 为授权用户提供对鉴别以及**【选择:【赋值:TSF 的部分】,TSF】**数据完整性的验证能力。

FPT_TST.1.3 TSF 通过密码服务为授权用户提供对所储存的**【选择:【赋值:部分 TSF】,TSF】**可执行代码完整性的验证能力。

7.9 安全审计

7.9.1 安全审计类架构

安全审计类架构见图 7。

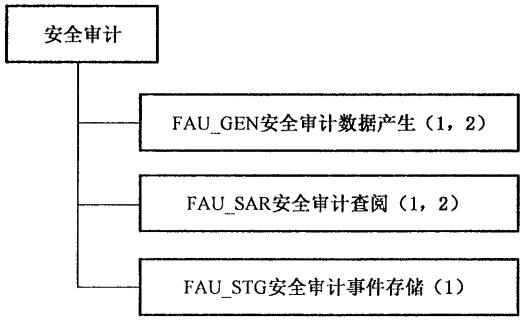

图 7 安全审计类架构

7.9.2 审计数据产生(FAU_GEN.1)

从属于:无。

依赖: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) 审计功能的启动和关闭;

b) 在最小级审计级别以内的所有可审计事件;

c) **【赋值:其他专门定义的可审计事件】**。

FAU_GEN.1.2 TSF 应在每个审计记录中至少记录如下信息:

a) 事件的日期和时间,事件类型,主体身份,事件的结果(成功或失败);

b) 基于安全功能组件中可审计事件定义的**【赋值:其他审计相关信息】**。

应用注释:相关事件的"最小级审计级别"请参考 GB/T 18336.2—2008 的规定。

7.9.3 用户身份关联(FAU_GEN.2)

从属于:无。

依赖:FAU_GEN.1 审计数据产生;

FIA_UID.1 标识时机。

FAU_GEN.2.1 TSF 应能将每个可审计事件与引起该事件的用户及应用软件,远程 IT 用户身份相关联。

7.9.4 审计查阅(FAU_SAR.1)

从属于:无。

依赖:FAU_GEN.1 审计数据产生。

FAU_SAR.1.1 TSF 应为**【赋值:授权用户,审计管理员】**提供从审计记录中读取**【赋值:审计信息列表】**的能力。

FAU_SAR.1.2 TSF 应以便于用户理解的方式提供审计记录。

应用注释:本机可以不提供审计查阅功能,但远程可信 IT 系统应提供该功能。

7.9.5 有限审计查阅(FAU_SAR.2)

从属于:无。

依赖:FAU_SAR.1 审计查阅。

FAU_SAR.2.1 除具有明确读访问权限的用户外,TSF 应禁止所有用户对审计记录的读访问。

7.9.6 受保护的审计迹存储(FAU_STG.1)

从属于:无。

依赖:FAU_GEN.1 审计数据产生。

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

FAU_STG.1.2 TSF 应能**【选择,选取一个:防止、检测】**对审计迹所存储的审计记录的修改。

7.10 可信路径/信道

7.10.1 可信路径/信道类架构

可信路径/信道类架构见图 8。

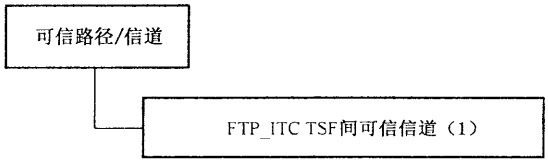

图 8 可信路径/信道类架构

7.10.2 TSF 间可信信道(FTP_ITC.1)

从属于:无。

依赖:无。

FTP_ITC.1.1 TSF 应在它自身和一远程可信 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不同,并且对其端点提供确定的标识,以及通过密码技术保护信道中数据免遭修改和泄露。

FTP_ITC.1.2 TSF 应允许**【选择:TSF,远程的可信 IT 产品】**经可信信道发起通信。

FTP_ITC.1.3 对于与远程可信 IT 产品间的交互,**【赋值:其他需要可信信道的功能列表】**,TSF 应经可信信道发起通信。

应用注释:TSF 间的可信信道应与普通通信信道不同,并要使用密码技术建立此可信信道。

8 移动终端操作系统的安全保证要求

8.1 安全保证级别

移动终端操作系统的安全保证级别选择 EAL2(见 ISO/IEC 15408-3:2008)。

EAL2 级别应包含的保证组件在表 2 中列出。

表 2 保证组件

保证类	保证组件
ADV:开发	ADV_ARC.1 安全架构描述
	ADV_FSP. 2 实施安全功能规范
	ADV_TDS. 1 基本设计
AGD:指导性文件	AGD_OPE. 1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC. 2 配置管理系统的使用
	ALC_CMS. 2 TOE 配置管理覆盖部分
	ALC_DEL.1 交付过程
ASE:安全目标评估	ASE_CCL.1 一致性要求
	ASE_ECD.1 扩充组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 安全要求导出
	ASE_SPD. 1 安全问题定义
	ASE_TSS.1 TOE 概要规范
ATE:测试	ATE_COV.1 覆盖证据
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试-用例
AVA:脆弱性评估	AVA_VAN. 2 脆弱性分析

8.2 开发

8.2.1 安全架构描述（ADV_ARC.1）

依赖:ADV_FSP.1 基本功能规范;

ADV_TDS.1 基本设计。

开发者行为元素:

ADV_ARC.1.1D 开发者应设计和实施 TOE 使得 TSF 的安全特性不能被旁路。

ADV_ARC.1.2D 开发者应设计和实施 TOE 使得 TSF 能够保护自身不受非可信活动实体的干扰。

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 安全架构描述的详细程度应与 TOE 设计文档中实施安全功能要求的抽象描述相当。

ADV_ARC.1.2C 安全架构描述应描述由 TSF 维护的与安全功能要求一致的安全域。

ADV_ARC.1.3C 安全架构描述应描述 TSF 初始化过程是安全的。

ADV_ARC.1.4C 安全架构描述应论证 TSF 保护自身不受干扰。

ADV_ARC.1.5C 安全架构描述应论证 TSF 能够防止安全功要求的执行被旁路。

评估者行为元素：

ADV_ARC.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。

8.2.2 安全执行功能规范(ADV_FSP.2)

依赖：ADV_TDS.1 基本设计。

开发者行为元素：

ADV_FSP.2.1D 开发者应提供功能规范。

ADV_FSP.2.2D 开发者应提供从功能规范到安全功能要求的对应。

内容和形式元素：

ADV_FSP.2.1C 功能规范应完整表达 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 功能规范应标识和描述与每个 TSFI 关联的所有参数。

ADV_FSP.2.4C 对每一个执行安全功能要求的 TSFI，功能规范应描述与此 TSFI 关联的安全功能要求的执行动作。

ADV_FSP.2.5C 对每一个执行安全功能要求的 TSFI，功能规范应描述与安全功能要求执行动作相关的处理所导致的直接错误信息。

ADV_FSP.2.6C 在功能规范中的对应关系应能论证安全功能要求与 TSFI 的对应。

评估者行为元素：

ADV_FSP.2.1E 评估者应能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 评估者应能判断此功能规范是安全功能要求的一个正确和完整的具体例证说明。

8.2.3 基本设计（ADV_TDS.1）

依赖：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 TOE 的设计。

ADV_TDS.1.2D 开发者应提供功能规范中 TSFI 与 TOE 最底层分解设计间的映射关系。

内容和形式元素：

ADV_TDS.1.1C 设计应从子系统的角度描述 TOE 的结构。

ADV_TDS.1.2C 设计应标明 TSF 的全部子系统。

ADV_TDS.1.3C 设计应通过充分的细节描述每个安全功能要求支持或安全功能要求无关 TSF 子系统的行为以确定它不是安全功能要求执行子系统。

ADV_TDS.1.4C 设计应概要说明安全功能执行子系统执行安全功能的行为。

ADV_TDS.1.5C 设计应描述 TSF 安全功能执行子系统间的交互、TSF 安全功能执行子系统与其他 TSF 子系统间的交互。

ADV_TDS.1.6C 映射关系应论证全部的 TSFI 与 TOE 设计中所描述的由它们引发的行为相对应。

评估者行为元素：

ADV_TDS.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。

ADV_TDS.1.2E 评估者应能判断此设计是全部安全功能要求的正确和完整的具体例证说明。

8.3 指导性文件

8.3.1 用户操作指南（AGD_OPE.1）

依赖：ADV_FSP.1 基本功能规范。

开发者行为元素：

AGD_OPE.1.1D 开发者应提供用户操作指南。

内容和形式元素：

AGD_OPE.1.1C 用户操作指南应为每个用户角色描述需要在安全环境控制下可访问的功能、特权，并做适当警告。

AGD_OPE.1.2C 用户操作指南应为每个用户角色描述如何使用 TOE 以安全方式提供的可用接口。

AGD_OPE.1.3C 用户操作指南应为每个用户角色描述可用的功能和接口，特别是所有由用户控制的安全参数，适当指明安全数值。

AGD_OPE.1.4C 用户操作指南应为每个用户角色陈述每一种需要执行的与用户可访问功能相关的安全事件，包括改变 TSF 控制实体的安全特性。

AGD_OPE.1.5C 用户操作指南应标明所有可能的 TOE 操作模式(包括导致失败、操作错误的操作)及它们对保证安全操作的后果和影响。

AGD_OPE.1.6C 用户操作指南应描述每个用户角色所遵循的安全措施以满足 ST 所描述的环境安全目的。

AGD_OPE.1.7C 用户操作指南应清晰合理。

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。

8.3.2 准备过程（AGD_PRE.1）

依赖：无。

开发者行为元素：

AGD_PRE.1.1D 开发者应提供 TOE，包括它的准备过程。

内容和形式元素：

AGD_PRE.1.1C 准备过程应描述按照开发者交付程序安全接收 TOE 必要的全部步骤。

AGD_PRE.1.2C 准备过程应描述安全安装 TOE 及依据 ST 描述的环境安全目的安全准备操作环境必要的全部步骤。

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 评估者应实施准备过程，确认 TOE 能为操作做好安全准备。

8.4 生命周期支持

8.4.1 配置管理系统的使用（ALC_CMC.2）

依赖：ACL_CMS.1：TOE 配置管理覆盖。

开发者行为元素：

ALC_CMC.2.1D 开发者应提供 TOE 和 TOE 的参照号。

ALC_CMC.2.2D 开发者应提供配置管理文档。

ALC_CMC.2.3D 开发者应使用配置管理系统。

内容和形式元素：

ALC_CMC.2.1C TOE 应被其参照号唯一标识。

ALC_CMC.2.2C 配置管理文件应描述用于唯一标识 TOE 所包含配置项的方法。

ALC_CMC.2.3C 配置管理系统应唯一标识 TOE 所包含的所有配置项。

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。

8.4.2 TOE 配置管理覆盖部分（ALC_CMS.2）

依赖：无。

开发者行为元素：

ALC_CMS.2.1D 开发者应提供一个 TOE 配置列表。

内容和形式元素：

ALC_CMS.2.1C 配置列表应包含下列内容：TOE 自身；安全保证要求所要求的评估证据；和构成 TOE 的各个部分。

ALC_CMS.2.2C 配置列表应唯一标识配置项。

ALC_CMS.2.3C 对每个与 TSF 相关的项，配置列表应标明此项的开发者。

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。

8.4.3 交付过程（ALC_DEL.1）

依赖：无。

开发者行为元素：

ALC_DEL.1.1D 开发者应把 TOE 或其部分交付用户的过程文档化，并提交。

ALC_DEL.1.2D 开发者应使用交付过程。

内容和形式元素：

ALC_DEL.1.1C 交付文档应描述，在向消费者颁发 TOE 版本时，用以维护其安全性所必需的全部过程。

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。

8.5 安全目标评估

8.5.1 遵从声明（ASE_CCL.1）

依赖：ASE_INT.1：ST 引言；

ASE_ECD.1：扩展组件定义；

ASE_REQ.1：安全要求的陈述。

开发者行为元素：

ASE_CCL.1.1D 开发者应提供遵从声明。

ASE_CCL.1.2D 开发者应提供对遵从声明的解释。

内容和形式元素：

ASE_CCL.1.1C 遵从声明应说明 ST 及 TOE 所遵从的标准。

ASE_CCL.1.2C 遵从声明应论证 TOE 类型与其遵从的标准中的 TOE 类型是一致的。

ASE_CCL.1.3C 遵从声明应论证安全问题定义与其遵从的标准中的安全问题定义是一致的。

ASE_CCL.1.4C 遵从声明应论证安全目的与其遵从的标准中的安全目的是一致的。

ASE_CCL.1.5C 遵从声明应论证其安全要求与其遵从的标准中的安全要求是一致的。

评估者行为元素：

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

8.5.2 ST 引言（ASE_INT.1）

依赖：无。

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 实例、TOE 实例、TOE 概述及 TOE 描述。

ASE_INT.1.2C ST 实例应唯一标识 ST。

ASE_INT.1.3C TOE 实例应唯一标识 TOE。

ASE_INT.1.4C TOE 概述应简述 TOE 用途和主要安全特征。

ASE_INT.1.5C TOE 概述应标识 TOE 类型。

ASE_INT.1.6C TOE 概述应标识不属于 TOE 但 TOE 需要的任何硬件、软件及固件。

ASE_INT.1.7C TOE 描述应陈述 TOE 的物理范围。

ASE_INT.1.8C TOE 的描述应陈述 TOE 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 实例、TOE 概述及 TOE 描述之间的一致性。

8.5.3 扩展组件定义（ASE_ECD.1）

依赖：无。

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定义。

内容和形式元素：

ASE_ECD.1.1C 安全要求的陈述应标明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组件。

ASE_ECD.1.3C 扩展组件定义应描述每一个扩展组件与标准现有的组件、族、类的关系。

ASE_ECD.1.4C 扩展组件定义应使用标准现有组件、族、类及方法作为表达形式。

ASE_ECD.1.5C 扩展组件应由可度量的和客观的组件组成，以便于论证是否遵从这些组件。

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 评估者应确认已有组件无法明确表示扩展组件。

8.5.4 安全目的（ASE_OBJ.2）

依赖：ASE_SPD.1 安全问题定义

开发者行为元素：

ASE_OBJ.2.1D 开发者应陈述安全目的。

ASE_OBJ.2.2D 开发者应提供安全目的原理。

内容和形式元素：

ASE_OBJ.2.1C 安全目的应描述 TOE 的安全目的和操作环境的安全目的。

ASE_OBJ.2.2C 安全目的原理应追溯每一个 TOE 的安全目的所对应的威胁和要求实施的组织安全策略。

ASE_OBJ.2.3C 安全目的原理应追溯每一个操作环境的安全目的所对应的威胁和要求实施的组织

安全策略，及其支持的假设。

ASE_OBJ.2.4C 安全目的原理应证明安全目的应对了所有的威胁。

ASE_OBJ.2.5C 安全目的原理应证明安全目的实施了所有的组织安全策略。

ASE_OBJ.2.6C 安全目的原理应证明操作环境的安全目的支持了所有的假设。

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。

8.5.5 安全要求的导出（ASE_REQ.2）

依赖：ASE_OBJ.2 安全目标；

ASE_ECD.1 扩展组件定义。

开发者行为元素：

ASE_REQ.2.1D 开发者应陈述安全要求。

ASE_REQ.2.2D 开发者应提供安全要求原理。

内容和形式元素：

ASE_REQ.2.1C 安全要求应描述安全功能要求和安全保证要求。

ASE_REQ.2.2C 应定义用于安全功能要求和安全保证要求中的所有主体、客体、操作、安全属性、外部实体及其他项目。

ASE_REQ.2.3C 安全要求陈述应标明安全要求的所有操作。

ASE_REQ.2.4C 应正确实施所有操作。

ASE_REQ.2.5C 每一个安全要求的依赖应满足，或在安全要求原理中说明不满足的理由。

ASE_REQ.2.6C 安全要求原理应追溯每一安全要求到所对应的 TOE 的安全目的。

ASE_REQ.2.7C 安全要求原理应论证安全要求组件实现了所有的 TOE 安全目的。

ASE_REQ.2.8C 安全要求原理应解释选择安全保证要求组件的原因。

ASE_REQ.2.9C 安全要求的陈述应是内部一致的。

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。

8.5.6 安全问题定义（ASE_SPD.1）

依赖：无。

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 所有威胁应按照威胁主体、资产及攻击行为进行描述。

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有关 TOE 操作环境的假设。

评估者行为元素：

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

8.5.7 TOE 概要规范（ASE_TSS.1）

依赖：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。

开发者行为规范：

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 TOE 如何满足每一个安全功能要求。

评估者行为元素：

ASE_TSS.1.1E 评估者应能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 概述和 TOE 描述一致。

8.6 测试

8.6.1 覆盖证据（ATE_COV.1）

依赖：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证据。

内容和形式元素：

ATE_COV.1.1C 测试覆盖证据应展示测试文件中的测试与功能规范的 TSFIs 之间的对应关系。

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内容和形式的所有要求。

8.6.2 功能测试（ATE_FUN.1）

依赖：ATE_COV.1：证据覆盖。

开发者行为元素：

ATE_FUN.1.1D 开发者应测试 TSF 并形成结果文档。

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、预期测试结果和实际测试结果。

ATE_FUN.1.2C 测试计划应标明所开展的测试并描述每个测试的测试场景。这些场景应包括对其他测试结果的次序依赖。

ATE_FUN.1.3C 预期测试结果应给出成功执行测试的预期输出。

ATE_FUN.1.4C 实际测试结果应与预期测试结果一致。

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的内容和形式的所有要求。

8.6.3 独立测试-用例（ATE_IND.2）

依赖：ADV_FSP.2：安全执行功能规范；

AGD_OPE.1：用户操作指南；

AGD_PRE.1：准备过程；

ATE_FUN.1：功能测试；

ATE_COV.1：证据覆盖。

开发者行为元素：

ATE_IND.2.1D 开发者应提供 TOE 用于测试。

内容和形式元素：

ATE_IND.2.1C TOE 应适于测试。

ATE_IND.2.2C 开发者应提供开发者进行 TSF 功能测试的等同资源。

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 评估者应执行一个测试文件中的测试用例以检验开发者的测试结果。

ATE_IND.2.3E 评估者应测试一个 TSF 的子集，确认 TSF 以指定的方式工作。

8.7 脆弱性评估

8.7.1 脆弱性分析(AVA_VAN.2)

依赖：ADV_ARC.1：安全架构描述；

ADV_FSP.2：安全执行功能规范；

ADV_TDS.1：基本设计；

AGD_OPE.1：用户操作指南；

AGD_PRE.1：准备过程。

开发者行为元素：

AVA_VAN.2.1D 开发者应提供 TOE 用于测试。

内容和形式元素：

AVA_VAN.2.1C TOE 应适于测试。

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 评估者应执行公共域资源搜索以辨识 TOE 中的脆弱性。

AVA_VAN.2.3E 评估者应通过使用用户指南、功能规范、TOE 设计和安全架构描述，执行独立的 TOE 脆弱性分析以辨识 TOE 中潜藏的脆弱性。

AVA_VAN.2.4E 基于已经辨识的潜在脆弱性，评估者应构造穿透性测试以确定 TOE 能抵抗具备基础攻击潜能的攻击者发起的攻击。

9 原理

9.1 安全目的原理表

表 3、表 4 分别描述了安全威胁和组织安全策略所对应的安全目的。

表 3 威胁与安全目的

序号	威　胁	安全目的
1	用户数据丢失(T.LOSS_THEFT) 由于丢失或被盗，可能导致用户数据损失	用户数据备份(O.USERDATA_BACKUP) 移动终端操作系统应提供用户数据备份机制
2	非授权人员访问(T.UNAUTHORIZED_ENTRY) 非授权人员试图访问移动终端上的用户数据和系统敏感资源，例如在手机丢失或被盗的情况下非授权人员访问移动终端	鉴别(O.USER_AUTHENTICATION) 鉴别用户、应用软件的身份； 会话锁定(O.SESSION_LOCK) 移动终端操作系统应能在不活动时间达到规定值时锁定会话。同时也应支持由用户发起的会话锁定。重新激活终端应经过用户的再次鉴别

表 3（续）

序号	威　胁	安全目的
3	用户配置错误（T. USER _ CONFIGRATION _ ERROR） 不具备安全意识或安全意识薄弱的用户通过不正确地配置 TOE，使移动终端安全受到威胁	管理（O.MANAGE） 向管理员提供管理移动终端操作系统安全的功能，并限制非授权用户使用此项功能
4	危及 TSF 安全（T.TSF_COMPROMISE） 恶意用户、进程可能查看、更改或删除 TSF 数据或可执行代码，危及 TSF 的安全	域隔离（O.DOMAIN_ISOLATION ） 提供域隔离机制，保护自身及资源不受到外部冲突、篡改或破坏
5	非授权网络流量（T.UNAUTHORIZED_ NETTRAFFIC） 未授权外部 IT 实体向 TOE 发送网络数据或接收经由 TOE 路由的网络数据	网络信息流控制（O. NETWORK _ FLOW _ CONTROL） 移动终端操作系统需依据信息流控制策略与远程 IT 实体通信 （IP 网络信息流控制 SFP、安全管理信息流控制 SFP）
6	授权人员用户的恶意行为（T. ACCESS _ MALICIOUS） 授权用户利用权限进行非法操作，比如：维修人员在设备维护期间窃取用户隐私、安装恶意软件，或进行其他违背持有者意愿的行为	管理员角色（O.ADMINISTRATOR_ROLE） 设置管理员角色以隔离管理员行为
7	恶意软件（T.MALICIOUS_SOFTWARE） 恶意软件可能通过伪装成授权应用或进程非授权访问用户数据和系统敏感资源，比如，木马或病毒	设备访问（O.DEVICE_ACCESS） 用户、进程、主体应通过授权方式访问用户数据及系统敏感资源（设备访问控制 SFP）； 应用软件限制（O.APPLICATION_RESTRICT） 在应用软件安装、运行时，对应用软件进行限制 （应用软件限制 SFP，设备访问控制 SFP）
8	数据备份（T.DATA_BACKUP） 攻击者可能在备份数据传送过程中窃取或破坏用户数据	备份数据保护（O.BACKUP_DATA_PROTECT） 移动终端操作系统应在备份数据输出前对数据进行保密性和完整性保护
9	设备管理（T.DEVICE_MANAGEMENT） 攻击者可能在设备管理过程中篡改、破坏管理数据、配置数据和系统更新数据	设备管理（O. DEVICE_MANAGEMENT） 移动终端操作系统应保护设备管理过程中传送的管理数据、配置数据和系统更新数据

表 4　组织安全策略与安全目的

序号	组织安全策略	安全目的
1	按需授予（P.NEED_TO_KNOW） 限制授权用户及主体访问能力的原则是按需给予	设备访问（O.DEVICE_ACCESS） 用户、进程、主体应通过授权方式访问用户数据及系统敏感资源（设备访问控制 SFP）； 管理员角色（O.ADMINISTRATOR_ROLE） 设置管理员角色以隔离管理员行为

表 4（续）

序号	组织安全策略	安全目的
2	访问授权管理(P.ACCESS_ AUTHORIZATION_MANAGE) 移动终端操作系统应向用户提供访问授权管理能力	管理(O.MANAGE) 向管理员提供管理移动终端操作系统安全的功能，并限制非授权用户使用此项功能； 管理员角色(O.ADMINISTRATOR_ROLE) 设置管理员角色以隔离管理员行为
3	明确提示(P. VISIBLE_PROMPT) 当访问与安全、法律有关的用户数据和系统敏感资源时，移动终端操作系统应能够向用户提供明确的提示	设备访问(O.DEVICE_ACCESS) 用户、进程、主体应通过授权方式访问用户数据及系统敏感资源(设备访问控制 SFP)； 应用软件限制(O.APPLICATION_RESTRICT) 在应用软件安装、运行时，对应用软件进行限制(应用软件限制 SFP)
4	标识和鉴别(P.I_AND_A) 移动终端的用户、应用软件、进程、主体、客体都应被分配唯一的标识，并在执行访问和实施动作之前加以鉴别	鉴别(O.USER_AUTHENTICATION) 鉴别用户、应用软件的身份； 标识(O.USER_IDENTIFICATION) 给用户、应用软件分配唯一的标识
5	追溯(P.TRACE) 主体行为可以被追溯	审计产生(O.AUDIT_GENERATION) 移动终端操作系统具备检测与安全有关事件的能力，并产生审计记录； 审计保护(O.AUDIT_PROTECTION) 保护审计信息； 审计调阅(O.AUDIT_REVIEW) 具备选择性审阅审计信息的能力，并向管理员报告安全违规
6	密码(P.CRYPTOGRAPHY) 移动终端操作系统安全功能应得到密码技术的支持，密码算法应符合国家和行业的信息技术安全标准或规范	密码服务(O.CRYPTOGRAPHIC_SERVICES) 移动终端操作系统应为安全功能的实施提供密码服务
7	网络连接(P.NETWORK) 移动终端操作系统用户通过互联网访问远程可信 IT 实体(应用软件商店、运营商服务器、设备管理系统、邮件服务器)时应能够建立安全连接	网络连接(O.NETWORK) 移动终端操作系统需与远程实体通信建立安全连接 (网络信息流控制 SFP、安全管理信息流控制 SFP)

9.2 安全要求原理表

表 5 描述了针对每一个安全目的所对应的安全功能要求或安全保证要求，以说明安全目的得到正确实施。

表 5　安全要求原理表

序号	安全目的	安全功能要求(SFRs)
1	用户数据备份(O.USERDATA_BACKUP) 移动终端操作系统应提供用户数据备份机制	TOE 通过[FDP_ETC.1(UD)]、[FDP_ETC.2(UD)]向用户提供用户数据输出到 TOE 外的功能，通过[FDP_ITC.1(UD)]、[FDP_ITC.2(UD)]提供用户数据由 TOE 外输入的功能
2	鉴别(O.USER_AUTHENTICATION) 鉴别用户、应用软件的身份	TSF 应确保只有授权人员用户和授权的应用软件基于用户属性(FIA_ATD.1)访问 TOE 或 TOE 的敏感资源。用户和应用软件须经标识鉴别过程实现访问(FIA_UAU.1、FIA_UAU.5、FIA_UAU.6、FIA_UAU.7)；TSF 应具备抵御暴力攻击的能力(FIA_AFL.1、FIA_SOS.1)
3	会话锁定(O.SESSION_LOCK) 移动终端操作系统应能在不活动时间达到规定值时锁定会话。同时也应支持由用户发起的会话锁定。重新激活终端应经过用户的再次鉴别	TOE 应通过 TSF 原发(FTA_SSL.1)、用户原发(FTA_SSL.2)锁定用户会话以限制非授权用户对 TOE 的访问； TOE 应根据安全属性拒绝用户会话建立(FTA_TSE.1)，TSF 应基于访问方法限制管理员和审计管理员会话的安全属性范围(FTA_LSA.1)
4	管理(O.MANAGE) 向管理员提供管理移动终端操作系统安全的功能，并限制非授权用户使用此项功能	(FMT_SMF.1)定义了 TOE 安全管理接口的划分。通过(FMT_MOF.1)确定管理员和审计管理员能够实施的安全功能行为的管理；通过(FMT_MSA.1)、(FMT_MSA.2)、(FMT_MSA.3)对执行应用程序限制策略、设备访问控制策略、网络信息流控制策略、安全管理信息流控制所依赖的安全属性进行管理；通过(FMT_MTD.1)、(FMT_MTD.2)、(FMT_MTD.3)对审计数据及其他 TSF 数据进行管理；通过安全属性撤销(FMT_REV.1)向用户提供撤销应用软件安全属性的能力；管理权限通过(FMT_SMR.1)进行分割
5	域隔离(O.DOMAIN_ISOLATION) 提供域隔离机制，保护自身及资源不受到外部冲突、篡改或破坏	TSF 应具备自检能力(FPT_TST.1)，确保密码模块、TSF 可执行代码的完整性。应为审计、用户数据保护等安全功能提供可靠的时间戳(FPT_STM.1)；通过安全架构描述(ADV_ARC.1)保证自身及资源不受到外部冲突、篡改或破坏
6	网络信息流控制(O.NETWORK_FLOW_CONTROL) 移动终端操作系统需依据信息流控制策略与远程 IT 实体通信	网络信息流控制机制[FDP_IFC.1(NIC)]和安全管理信息流控制机制[FDP_IFC.1(MIC)]控制移动终端与远程网络实体间的网络信息流，采用由 FDP_IFF.1(NIC)和 FDP_IFF.1(MIC)定义的规则对网络信息流实施控制
7	管理员角色(O.ADMINISTRATOR_ROLE) 设置管理员角色以隔离管理员行为	(FMT_SMR.1)定义了 TOE 安全角色
8	设备访问(O.DEVICE_ACCESS) 用户、进程、主体应通过授权方式访问用户数据及系统敏感资源(设备访问控制 SFP)	[FDP_ACC.1(DA)]定义了 TOE 的设备访问控制 SFP 的控制范围，[FDP_ACF.1(DA)]定义了 TSF 实施设备访问控制 SFP 的规则；访问用户数据及系统敏感资源的权限与用户身份关联(FIA_USB.1)

表 5（续）

序号	安全目的	安全功能要求(SFRs)
9	应用软件限制（O. APPLICATION _ RESTRICT) 在应用软件安装、运行时，对应用软件进行限制	[FDP_ACC.1(AP)]定义了 TOE 应用软件限制 SFP 的控制范围，[FDP_ACF.1(AP)]定义了 TSF 实施应用软件限制 SFP 的规则； [FDP_ITC.1(AP)]和[FDP_ITC.2(AP)]定义了应用软件输入时应受到的限制
10	备份数据保护（O. BACKUP _ DATA _ PROTECT) 移动终端操作系统应在备份数据输出前对数据进行保密性和完整性保护	(FDP_UCT.1)保证备份数据输出的保密性，(FDP_UIT.1)保证备份数据输出的完整性
11	设备管理(O. DEVICE_MANAGEMENT) 移动终端操作系统应保护设备管理过程中传送的管理数据、配置数据和系统更新数据	用(FPT_ITC.1)、(FPT_ITI.1)、(FPT_TDC.1)实现 TOE 与外部实体间管理数据、配置数据的交互及系统数据的更新
12	标识(O.USER_IDENTIFICATION) 给用户、应用软件分配唯一的标识	应用程序应被 TSF 标识(FIA_UID.1)
13	审计产生(O.AUDIT_GENERATION) 移动终端操作系统具备检测与安全有关事件的能力，并产生审计记录	TOE 应产生审计数据(FAU_GEN.1)，并与用户身份关联(FAU_GEN.2)
14	审计调阅(O.AUDIT_REVIEW) 具备选择性审阅审计信息的能力，并向管理员报告安全违规	TOE 应提供审计查阅(FAU_SAR.1)及有限审计查阅(FAU_SAR.2)
15	审计保护(O.AUDIT_PROTECTION) 保护审计信息	TOE 应保护审计迹存储(FAU_STG.1)
16	密码服务(O.CRYPTOGRAPHIC_ SERVICES) 移动终端操作系统应为安全功能的实施提供密码服务	(FCS_CBR_EXT.1)确定了 TOE 密码支持的基本要求，(FCS_COA_EXT.1)定义了向 TOE 的安全功能应提供的密码操作
17	网络连接(O.NETWORK) 移动终端操作系统需与远程实体通信建立安全连接	TOE 与远程实体进行安全的网络通信前应进行双向鉴别(FIA_UAU.5)，通过(FPT_ITC.1)、(FPT_ITI.1)、(FPT_TDC.1)与远程实体进行 TSF 数据的交互，通过(FDP_ITC.2)、(FDP_UCT.1)、(FDP_UIT.1)与远程实体进行用户数据交互，以实现与远程实体建立安全连接

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—2006 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 15408-1:2009 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型(Information technology—Security techniques—Evaluation criteria for IT security—Part 1:Introduction and general model)

中 华 人 民 共 和 国
国 家 标 准
移动通信智能终端操作系统安全技术要求
（EAL2 级）
GB/T 30284—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3 字数 78 千字
2014 年 5 月第一版 2014 年 5 月第一次印刷
*
书号：155066·1-49174 定价 42.00 元

GB/T 30284-2013

打印日期：2014年6月10日 F001