ICS 33 60
M 36

YD

中华人民共和国通信行业标准

YD/T 1699-2007

移动终端信息安全技术要求

Information Security Technical Specification for Mobile Terminal

2007-09-29 发布　　2008-01-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是移动终端信息安全系列标准之一，该系列标准的结构及名称如下：

1．YD/T1699-2007 移动终端信息安全技术要求；

2．YD/T1700-2007 移动终端信息安全测试方法。

其中，YD/T1700-2007《移动终端信息安全测试方法》是本标准的配套标准。

本标准在制定过程中参考了GB/T 18336《信息技术 安全技术 信息技术安全性评估准则》YD/T 1214-2006《900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术要求：移动台》、YD/T 1215-2006《900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：移动台》和YD/T 1558-2007《2GHz cdma2000数字蜂窝移动通信网设备技术要求：移动台。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：大唐电信科技产业集团、中国移动通信集团公司、信息产业部电信研究院、华为技术有限公司、中兴通讯股份有限公司、中国普天信息产业集团公司

本标准主要起草人：刘迪军、耿　静、孙正红、刘国庆、高建英

移动终端信息安全技术要求

1 范围

本标准规定了移动终端设备的信息安全技术要求，包括总体安全要求、终端硬件的安全要求、终端软件的安全要求、操作系统的安全要求及对安全应用的支持。

本标准适用于二代（包含二代）以上移动通信网的终端设备。本标准不包含EMC、EMI或电气安全等相关的技术要求。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 15843.2	信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制
GB/T 15843.3	信息技术 安全技术 实体鉴别 第3部分：用非对称签名技术的机制
GB/T 15851	信息技术 安全技术 带消息恢复的数字签名方案（idt ISO/IEC 9796）
GB/T 16649.3	识别卡 带触点的集成电路卡 第3部分：电信号和传输协议（idt ISO/IEC 7816-3）
YD/T 1214-2006	900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术要求：移动台
YD/T 1215-2006	900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：移动台
YD/T 1558-2007	2GHz cdma2000数字蜂窝移动通信网设备技术要求：移动台
YD/T 1168-2007	CDMA数字蜂窝移动通信网用户识别模块（UIM）技术要求
ISO 8730	银行业务—消息鉴别要求
3GPP TS 01.61	GPRS加密算法要求
3GPP TS 24.008	移动无线接口层三规范：核心网协议
3GPP TS 31.102	USIM应用特性
3GPP TS 31.111	USIM应用工具箱（USAT）
3GPP TS 34.123-1	用户设备 （UE） 一致性规范；第1部分：协议一致性规范
3GPP2 C.S0035	CDMA卡应用工具箱（CCAT）
ETSI GSM 11.14	数字蜂窝通信系统（第2+阶段）：用户识别模块—移动设备（SIM-ME）接口的SIM应用工具包规范
ETSI TS 102 221	智能卡；UICC—终端接口；物理和逻辑特性
ANSI X9.9	金融机构的消息鉴别
OAM DRM v2.0	数字版权管理标准v2.0

3 术语与定义

下列术语和定义适用于本标准。

3.1

文件 file

文件是在逻辑上具有完整意义的信息的集合，它有一个名称以供识别。

3.2

文件系统 file system

文件系统是操作系统中以文件方式管理移动终端软件资源的软件和被管理的文件和数据结构的集合。

3.3

机密性 confidentiality

信息不提供给或不泄露给未授权方的属性。

3.4

完整性 integrity

信息不被未授权方变更或破坏的属性。

3.5

非否认性 can not be disavowed

指能够保证信息行为人不能否认其信息行为。

3.6

身份认证 user authentication

对用户身份标识的有效性进行验证和测试的过程。

3.7

授权 authorization

在用户身份经过认证后，根据预先设置的安全策略授予用户相应权限的过程。

3.8

授权用户 authorized user

依据安全策略可以执行某项操作的用户。根据实际操作的不同，可对应于本文所定义角色的任何一个。

3.9

访问控制 access control

一种防止资源被未授权用户使用的安全策略。

3.10

安全事件 security event

一种在移动终端资产管理、保护和分配过程中具有直接或潜在危害性的操作或行为。

3.11

角色 role

一组预先确定的规则，用于在用户和移动终端之间建立许可的交互。

3.12

应用 application

指移动终端上用于实现业务功能的文件组或程序。

3.13

数字签名 digital signature

一种非对称加密数据变换，它使得接收方能够验证数据的可靠性和完整性，保护发送和接收的数据不被第三方伪造，同时对于发送方来说，还可用于防止接收方的伪造。

3.14

随机数 random number

一个无法事先预料的时变参数。

3.15

密钥 key

控制密码变换（如加密、解密、密码校验函数计算、签名产生或签名验证）运算的符号序列。

3.16

密钥管理 key management

实施并运用对密钥材料进行产生、登记、认证、注销、分发、安装、存储、归档、撤销、衍生和销毁的服务。

3.17

证书 certification

由认证机构签署的某一实体的不可伪造的公开密钥信息。

3.18

证书管理 certification management

实施并运用证书的颁发、撤销、公布、存档和策略建立/批准等服务。

3.19

终端操作系统 operating system

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

4 缩略语

下列缩略语适用于本标准。

API	Application Program Interface	应用程序接口
AT	Attention	终端设备向终端适配器所发送命令的两个开始字符
DRM	Digital Right Management	数字版权管理
IMEI	International mobile station Equipment Identification	国际移动台设备识别号
IMSI	International Mobile Subscriber Identity	国际移动用户识别号
MAC	Message Authentication Code	消息认证码
MIC	Message Integrity Code	消息完整性码
PIM	Personal Information Management	个人信息管理

PIN1/PIN2	Personal Identity Number	用户身份识别号
RSA		一种可用于加密和数字签名的公钥密码算法，由Rivest、Shamir、Adleman发明

5 总体安全要求

5.1 概述

移动终端作为移动业务对用户的惟一体现形式以及存储用户个人信息的载体，应配合移动网络保证移动业务的安全，实现移动网络与移动终端之间通信通道的安全可靠，同时保证用户个人信息的机密性、完整性。

为了达到以上安全目的，移动终端应提供措施保证系统参数、系统数据、用户数据、密钥信息、证书、应用程序等的完整性、机密性，终端关键器件的完整性、可靠性以及用户身份的真实性。因此在进行移动终端应用开发、设计时应充分考虑和提供一系列安全策略，主要如下：

——应提供措施对系统程序、应用程序、终端关键器件等进行一致性检验；

——应能够基于角色，为用户提供受控和受限的资源及对象的访问、操作权限；

——能够在不同角色用户访问移动终端之前，对用户的身份进行认证，识别用户所对应的角色，然后根据用户的角色对用户进行授权；

——应提供措施对密钥、证书、系统参数、用户数据等进行有效的安全管理，保证存储数据的机密性、完整性、可靠性；

——移动终端应可对各个物理接口进行接入安全控制；

——应保证系统程序、不同的应用程序及其所使用数据在物理及逻辑上的隔离；

——应提供记录安全相关事件的手段，以帮助管理及抵抗潜在攻击；

——移动终端中的关键器件应具有抵抗防篡改等物理攻击的能力，或应使通过此类攻击获得有效信息十分困难，以提高移动终端的自身安全防护能力；

——应具有完善的系统操作权限管理能力；

——应能够安全的接入网络；

——应能够与智能卡安全的进行信息交互；

——应能够识别不同的应用并启用对应的安全策略。

5.2 移动终端的基本构成

移动终端是包括CPU、RAM、非易失性存储器、内存控制器、中断控制器、时钟电路、I/O电路、各种通信接口及相关软件（操作系统、应用软件）、通信协议栈等在内的通信设备。作为独立的物理实体，移动终端由于具有高速的处理器和大容量的存储器，又能够直接和移动网络进行对话，所以很多安全功能和业务应用都可以比较方便的实现。但由于目前移动终端结构比较松散，没有提供措施对内部器件进行统一管理和认证；在操作系统设计上缺乏有效的安全策略；同时移动终端中所存储的数据甚至程序在不同的程度上也是公开或开放的。随着技术和应用的发展，移动终端在进行业务应用时将面临多种安全威胁，如病毒、机密信息的泄露、代码的非法篡改、关键器件的恶意替换等。

5.3 移动终端的安全框架

为了克服移动终端存在的种种漏洞，将安全威胁降低到最小，移动终端应从硬件结构、软件结构入手，制定一系列安全策略保证移动终端以及其承载业务应用安全可靠。

首先，移动终端应提供措施实现移动终端关键器件的完整性认证、系统代码的完整性认证、数据流的安全监控、应用程序的安全服务等，以保证移动终端在工作时，进入一个安全、可信的工作环境。

其次，移动终端还应制定完善的安全控制策略、程序的域隔离策略，以实现用户的身份认证、程序的访问权限控制、程序之间通信的安全可靠以及防止程序在运行过程中出现读取、修改、删除其他程序空间数据的非法攻击。

除了以上功能外，移动终端还应根据数据、文件的敏感性，对其进行分类存储，并对不同级别的数据、文件采取不同的安全措施；同时定义完善的安全审计策略，以帮助发现已发生的安全事件和潜在的安全风险。

5.4 移动终端构成的一致性检验

5.4.1 硬件模块的一致性检验

开机时，移动终端应具有硬件的自检测功能，包括：

1） 硬件是否缺失；

2） 关键部件是否被更换过；

3） 更换的新部件是否合法；

4） 是否出现了未知的硬件设备。

如果检测发现硬件模块出现问题，根据出现问题的不同类型，移动终端应能够采取如下安全措施中的一个或几个：

1） 告警；

2） 记录日志；

3） 关机。

5.4.2 系统软件的一致性检验

移动终端应具有系统软件的自检测功能，包括：

1） 系统软件是否被非法篡改（包括删除、修改和增加）；

2） 系统配置是否被非法篡改。

如果检测发现系统软件出现问题，根据出现问题的不同类型，移动终端应能够采取如下安全措施中的一个或几个：

1） 告警；

2） 记录日志；

3） 关机；

4） 恢复被修改的系统代码；

5） 恢复被修改的系统设置。

5.4.3 应用软件的一致性检验

移动终端应能对应用软件进行一致性检验，包括：

1） 软件代码完整性；

2） 软件配置是否被非法篡改。

如果检测发现应用软件出现问题，根据出现问题的不同类型，移动终端应能够采取如下安全措施中的一个或几个：

1） 告警；

2） 记录日志；

3） 禁止使用；

4） 恢复被修改的配置；

5） 恢复被修改的代码。

5.5 基于角色的身份认证

5.5.1 基于角色的权限划分

角色是一组用户的集合加上一组操作权限的集合，根据移动终端的应用场景，将与移动终端接触的实体划分为四种角色：终端拥有者、业务提供商、终端生产商和终端维修商。终端生产商这一角色所对应的权限只在终端出厂前有效，终端出厂后，终端生产商拥有终端维修商角色所对应的权利。

1.“终端拥有者”角色拥有的权限

1） 使用终端接受移动网络运营商提供的服务，包括拨打/接听电话、发送/接受短消息、发送/接受多媒体短消息等；

2） 使用终端接受业务提供商提供的业务，包括手机银行、数据下载、浏览网络、浏览视频等；

3） 对移动终端系统进行配置，满足用户的个性化需要；

4） 安装/删除/使用应用程序；

5） 读取、创建、修改、删除用户个人数据；

6） 读取系统产生的审计记录、系统日志等。

2.“业务提供商”角色拥有的权限

1） 仅针对所提供的业务，读取、写入、删除、修改移动终端上有关的数据；

2） 仅针对所提供的业务对移动终端进行与业务有关的配置；

3） 仅针对所提供的业务，对移动终端上相关数据加解密。

3.“终端生产商”角色拥有的权限

1） 对移动终端进行出厂配置；

2） 创建特定的系统文件；

3） 加密特定的数据；

4） 预留维修指令。

4.“终端维修商”角色拥有的权限

1） 使用维修指令；

2） 更换移动终端硬件；

3） 为使移动终端正常工作而对终端进行必要的重新配置；

4） 读取、写入、删除、修改与维修移动终端有关的明文数据；

5） 加密、解密与维修移动终端有关的加密数据。

5.5.2 身份认证方式

不同角色用户访问移动终端之前，移动终端应对用户的身份进行认证，识别用户所对应的角色，然后根据用户的角色对用户进行授权。

移动终端的激活可以采用的身份认证方式有口令认证、智能卡认证、生物特征识别及实体鉴别机制4种方式，并根据终端要达到的安全要求，以及不同的角色选用其中的一种或者几种的组合。

5.5.2.1 口令认证

用户登录口令长度不应小于 4 位，而且还应规定一次登录用户能够尝试的口令次数不超过 5 次，以防止强力攻击。如果用户在规定的次数内没有输入正确的口令，移动终端应采用适当的安全措施，例如：关机、锁定，停止用户正在进行的操作，并对此事件进行记录。用户登录口令在移动终端中应以密文或散列值的形式进行存储。

移动终端应提供界面供授权用户对用户登录口令进行更改，但不向用户提供直接读取的权限。

5.5.2.2 智能卡认证

与用户身份认证的相关信息存储在单独的智能卡中。使用时，用户首先要把智能卡插入移动终端，然后移动终端首先与智能卡交互，根据卡中的信息确定用户是否有进行该操作的权限。如果用户有相应的权限，操作正常进行；如果用户没有相应的权限，移动终端可以采用如下安全措施中的一种或者几种：

1） 停止用户正在进行的操作；

2） 告警；

3） 记录日志。

除了智能卡，也可以采用USB Key等能代表身份的具有计算功能的防篡改硬件。智能卡认证方式需要移动终端具有能够插入智能卡、USB Key等设备的物理接口。

5.5.2.3 生物特征认证

生物特征信息应以密文或散列值等形式进行存储。

移动终端应提供界面供授权用户对生物特征信息进行修改，在进行修改操作前需要输入用户口令，该口令可以和用户登陆口令相同，也可以是单独的用户口令。

移动终端不向用户提供读取生物特征信息的权限。

5.5.2.4 实体鉴别机制

实体鉴别机制可有两类，一类以公钥体制为基础，采用数字签名技术，服务提供商或服务使用者使用本身的私钥对消息签名，而验证者使用对方的公钥验证签名，若正确，则确定对方的身份；一类为对称密码体制，服务提供商或服务使用者利用与验证方共享的密钥封装一消息，如验证方能够成功解析出消息或验证消息的正确性，则确认对方的身份，此过程若双向进行，则完成双方的身份的确认。另外，也可通过第三方来实现声称者的确认。

由于各类业务的保障要求，各业务应用实体宜通过实体鉴别后方可交换业务和相关信息，同时考虑到时效性，可根据业务应用实体的不同采用对应的实体鉴别机制，既保证应用系统的安全，又要提高认证的效率。

5.6 访问控制

5.6.1 系统资源的访问控制

本节的系统资源是指 CPU 指令、存储器、通信模块、设备驱动以及系统内核等资源。

用户程序不能直接调用系统资源，如不能直接调用硬件资源、系统指令、通信模块等，所有的系统资源应通过操作系统提供的 API 接口才能进行访问。

对于加载的应用程序，如果没有被授权或没通过认证，则不能调用系统资源。

操作系统不应向用户程序开放访问电信智能卡、修改 IMEI 等数据的程序接口。

一旦发现用户试图访问无权访问的系统资源，根据非法访问的不同情况，移动终端应能够采取如下安全措施中的一个或几个：

1） 告警；

2） 禁止该操作；

3） 记录日志；

4） 系统锁定；

5） 关机。

5.6.2 业务应用的使用控制

可以允许每个业务应用程序定义各自的访问口令。

对于高度安全的应用，还应允许应用程序可以定义自己的访问控制策略。

一旦发现用户试图访问无权访问的应用业务，移动终端应能够采取如下安全措施中的一个或几个：

1） 告警；

2） 禁止该操作；

3） 记录日志；

4） 锁定用户；

5） 关机。

5.7 数据存储和访问安全

5.7.1 数据的存储安全

5.7.1.1 数据的安全分级存储

根据安全级别，移动终端中的数据分为机密数据、敏感数据、私有数据、普通数据。

机密数据是指对移动终端安全、应用安全等起重要作用的数据，比如密钥、口令、IMEI、安全配置信息等。机密数据在存储时要进行加密和完整性校验。

敏感数据是指对移动终端安全、应用安全等起一定作用的数据，如系统数据、证书、审计记录等。敏感数据在存储时要进行完整性校验，并根据数据的重要程度决定是否要进行加密存储。在正常操作时，此类数据只能由操作系统或应用程序进行调用。

私有数据是指和终端使用者有关的个人数据，私有数据在存储时应进行完整性校验，并由用户决定是否需要进行加密存储。此类数据只用终端使用者才能进行读取与修改。

普通数据是指对移动终端安全、应用安全等没有影响的数据，比如一张无关紧要的图片。普通数据的存储没有特殊要求，可以以明文形式存放。

5.7.1.2 机密性要求

移动终端应能对重要数据进行加密。

5.7.1.3 完整性要求

移动终端应能够检测存储在移动终端内的数据是否被篡改，以防止出现非法修改存储数据的逻辑攻击。

5.7.2 数据的访问

移动终端应支持并执行下面的访问控制策略以决定访问的操作是否被允许：

权限管理：定义各种访问数据文件的权限，不同安全属性的数据提供不同访问权限的机密性保护，只有获得相应的访问权限才可以对数据文件进行对应的操作，如读、更新、删除、删除恢复等操作；如果访问超出其规定的权限，移动终端应能及时检测出来，并采取以下措施中的一项或者几项：

1） 阻止该访问操作的继续进行；

2） 告警；

3） 记录日志；

4） 系统锁定。

访问级别：数据访问应该根据需要设置一定的等级权限，以应对不同级别的授权用户，数据访问等级策略一旦确定，将适用于所有的访问操作且不允许进行修改；当检测到有破坏终端内存储数据完整性的操作后，移动终端应采取以下安全措施的一项或或几项：

1） 阻止该操作的进一步执行；

2） 恢复被破坏的数据；

3） 告警；

4） 记录日志；

5） 系统锁定。

文件控制：建立文件结构的过程和指令，包括文件访问条件都应受其访问控制规则的约束。

5.8 安全域隔离

安全域隔离分为物理隔离和逻辑隔离。

物理隔离是指对移动终端中的物理存储空间进行划分，不同的存储空间用于存储不同的数据或代码，具体要求如下：

1） 移动终端操作系统中用于进行基础认证的信息和程序应放于不可更改的存储空间；

2） 系统数据、系统备份数据和用户数据应存储于不同的存储空间；

3） 解密后的机密数据应根据安全级别的不同存储于不同的存储空间。

逻辑隔离主要包括进程隔离、数据的分类存储，具体要求如下：

1） 操作系统应为每个进程的数据和指令分配独立的内存空间，以防止进程间数据的非法访问；

2） 进程间的通信应是在操作系统核控制下进行，操作系统应提供方式对进程的权限进行判断，以决定是否允许其能进行进程间通信；

3） 数据的分类存储见 5.7.1.1。

5.9 安全审计

5.9.1 审计策略

移动终端的安全审计是指对指定操作的错误尝试次数及相关安全事件进行记录、分析的过程。通过分析记录结果，移动终端可判断发生了哪些安全相关活动，并采取预先设定的安全措施。另外检查审计记录结果还可以帮助分析潜在攻击。

移动终端应该具备与以下安全操作相关的审计记录生成、保护等能力以及相应的结果处理能力：

1） 用户认证；

2） 终端构成的一致性认证；

3） 非法访问；

4） 非法数据传输；

5） 程序加载；

6） 程序的安装、删除、更新；

7） 远程控制；

8） 证书的获取、更新、销毁等。

5.9.2 审计记录的生成

移动终端应能够第一时间对相关安全事件生成准确客观的审计记录，以标明或间接反映出安全事件的影响程度或当前终端的状态。

每一条审计记录中至少应该包含的信息有事件发生的事件类型、执行结果（成功或失败）、引起此事件的用户的标志等审计信息。

5.9.3 审计记录的保护

移动终端应保证审计记录存储的完整性。

操作系统应对审计记录进行严格的访问控制，同时提供界面让授权用户访问审计记录。

对于可公开的审计记录，授权用户可以修改或删除，但对于认证剩余次数等审计记录只能由操作系统进行修改、复位等操作。

5.9.4 安全告警

移动终端应该具有根据安全事件的类型，针对那些会对移动终端安全构成威胁的操作不予执行并且进行主动告警的能力。

安全告警的内容应包括安全事件的威胁类型以及相应操作的潜在威胁信息。安全告警事件类型主要包括用户认证、终端构成的一致性认证、数据的非法访问，数据的完整性检验等。

6 移动终端硬件安全要求

6.1 关键器件的安全

6.1.1 器件的物理安全

为了保证移动终端硬件的安全性，它应该满足以下条件：

1） 基带芯片应能抵抗探针探测、光学显微镜探测等物理攻击，或应使通过此类攻击难以获得有效信息；

2） 基带芯片的结构应具有抵抗逻辑操纵或修改的能力，以抵抗软件逻辑攻击；

3） 基带芯片在硬件设计和软件开发上应使其所储存或运算的机密信息不会通过分析电流波形、频率、能量消耗、功率等表征变化而泄露；

4） 移动终端出厂时所有芯片测试模式需禁用。

6.1.2 器件的稳定性

基带芯片应具有高低压检测的功能，以防止攻击者输入特殊电压而使芯片进入非正常工作状态。当基带芯片检测到输入电压超过正常工作电压范围时，应采取相应的安全措施，如停止正常工作、自锁等，保护基带芯片的稳定性。

6.2 物理接口的监控

随着移动终端功能的日益强大，移动终端将会通过多个物理接口与外界进行通信。移动终端应可对从各个物理接口进行接入安全控制。

涉及的接入安全控制要求包括：

1） 访问控制能力；

2） 指令的许可性判定。

为了实现对物理接口的监控，移动终端应该具有以下两种逻辑接口：

1） 数据输入接口：移动终端在此接口可对所有输入数据的合法性进行验证；

2） 数据输出接口：移动终端在此接口可对所有输出数据的合法性进行验证。在自检和存在错误状态时，所有通过数据输出接口的输出数据应该被禁止。

7 移动终端操作系统安全要求

7.1 文件系统

7.1.1 概述

本节主要是描述文件系统中文件的创建、文件的存储、文件的访问、文件的管理等方面的安全要求，不涉及文件系统的组织结构、文件的逻辑结构、文件的命名方式等具体要求。

移动终端中的文件主要包括：系统文件、应用文件和库文件。

— 系统文件是指由操作系统核心和各种系统应用程序和数据组成的文件。

— 应用文件是用户、应用程序创建的文件以及其他与用户有关的个人信息文件，这类文件只能由授权的用户才能使用。

— 库文件是指能供应用程序或系统程序调用的子程序及常用应用程序组成文件。

7.1.2 安全目的

作为操作系统的主要组成部分，文件系统应提供措施保证文件信息的安全存储以及文件的安全访问，以防止未授权用户对文件进行非法删除、修改、复制，对文件、目录的安全属性进行非法更改，对文件的存取路径进行非法更改，并保证文件内容的安全等。

为了达到以上安全目的，文件系统在进行设计时，应满足以下安全策略：

1） 在文件进行创建时，应提供措施设置文件的访问控制权限；

2） 应提供措施保证文件的安全访问。

7.1.3 文件的创建与存储

操作系统应保证只有授权用户才能在移动终端上创建文件。

对于授权用户在移动终端中创建的文件和目录，文件系统应自动设置以下信息并提供修改的用户接口：

1） 有关文件存取控制的信息：文件名、用户名、存取权限、文件类型、文件属性，如读写文件、只读文件等；

2） 有关文件管理的信息：文件建立日期、文件最近修改日期、访问日期、文件的有效期限、文件的大小等。

文件系统还应允许授权用户在创建文件时，为每一个创建的文件设置一个口令，并将该相关信息写在文件头中。

文件系统应提供措施对文件的存储空间进行统一管理，不同类型的文件应存储在不同的物理分区或不同类型的存储设备中，如系统文件存储在 ROM 中，应用文件只能存储在操作系统预先设定的应用文件存储空间。同时还应保证属于不同业务的文件应存储在不同的目录文件下。

系统文件应以隐藏的形式进行存储，同时文件系统还应提供接口并允许授权用户把用户文件设置为隐藏形式，当文件设置为隐藏形式后，只允许授权用户对其属性进行修改。

操作系统还应内置一定的安全算法，并提供安全算法的API接口，以允许授权用户对文件进行加密存储。

7.1.4 文件的访问安全

操作系统只允许授权用户对权限范围内的文件和目录的各种属性，包括隐藏属性、系统属性、只读属性、存档属性等进行修改。

操作系统只允许授权用户对权限范围内的用户目录进行删除操作，对于系统目录，操作系统不向用户提供删除权限。

应充分考虑在对文件进行更新、删除等操作时，由于突然掉电、更新失败等异常对文件可能造成的损坏，以及对应的解决办法。

操作系统应根据用户或者应用程序的权限、文件的安全属性判断文件访问操作的合法性，其具体要求参见 5.6.1 以及 5.7.2。

7.1.5 系统文件的备份

操作系统应划分特定的存储空间用于系统文件的备份，同时操作系统应提供接口，允许用户对系统文件进行备份。

对于备份文件应以隐藏的形式进行存储。

操作系统不向应用程序或用户提供访问系统备份文件的接口，只有当需要进行系统恢复、备份文件更新时，操作系统才对备份文件进行操作。

系统备份文件和系统文件具有相同的安全存储要求。

当系统文件更新后，操作系统应及时的对系统备份文件进行更新操作。

7.1.6 文件管理

文件系统应提供措施对授权用户在权限范围内的目录和文件的删除、文件的移动、文件的复制、文件的更新、文件的控制管理信息等进行有效的管理。

当授权用户对权限范围内的目录进行删除时，操作系统应向用户进行告警，并删除目录文件下面的所有目录和文件，以释放存储空间。

当授权用户对权限范围内的文件进行删除时，操作系统应向用户进行告警，并删除与文件有关的控制管理信息。

当授权用户对文件进行访问或更新时，文件系统应及时更新与文件相关的大小、修改时间、访问时间等管理信息。

当一个文件被复制或移动到一个新的目录里时，这个文件将继承目标目录的权限。

7.2 指令系统

7.2.1 AT 指令

操作系统应禁止向未授权应用程序提供直接调用 AT 指令的公开 API 函数。

操作系统应只允许授权应用程序利用 AT 指令对移动终端进行操作，并与移动网络进行交互。如应用程序可以通过 AT 命令进行呼叫、短信、电话本、数据业务、补充业务等方面的控制。

操作系统应禁止任何应用程序使用 AT 指令对智能卡进行任何操作，如读取电信智能卡中的 IMSI 信

息、修改 PIN1/PIN2 码、对智能卡进行锁定等。

操作系统应只允许授权用户通过串口等外部接口使用 AT 指令对移动终端和电信智能卡进行操作，如用户使用 AT 指令前，应输入用户口令（该口令可以和用户登陆口令相同，也可以是单独的用户口令）等。

操作系统应对使用AT指令的事件进行记录，记录的详细要求及日志文件的安全要求参见7.3.4。

7.2.2 智能卡主动式命令

本节是描述支持 ETSI GSM 11.14《数字蜂窝通信系统（第 2+阶段）：用户识别模块—移动设备（SIM-ME）接口的 SIM 应用工具包规范》、3GPP TS 31.111《USIM 应用工具箱（USAT）》、3GPP2 C.S0035《CDMA 卡应用工具箱（CCAT）》其中之一的全部或部分主动式命令的移动终端所具有的附加安全要求。以下所指移动终端是支持 ETSI GSM 11.14、3GPP TS 31.111、3GPP2 C.S0035 其中之一的全部或部分主动式命令的移动终端。

移动终端操作系统不应向非授权应用程序提供直接调用智能卡主动式命令的接口。

对于支持对电信智能卡进行认证的移动终端，移动终端操作系统只执行已认证的电信智能卡发送的智能卡主动式命令。

当移动终端执行电信智能卡发送的不需要移动终端用户干预的主动式命令时，操作系统应具有向用户进行文字提示等告警的能力。

移动终端操作系统应具有对主动式命令事件进行记录的能力，记录的详细要求及日志文件的安全要求参见7.3.4。

7.2.3 其他用户操作指令

操作系统应只允许授权用户输入查看移动终端的用户操作指令，如只允许授权用户使用查看移动终端 IMEI 号、移动终端软件版本、信号强度、存储器容量、出厂日期、最后修理日期等用户指令。

操作系统应只向授权用户开放可以改变移动终端当前设置的用户操作指令，如把移动终端复位到出厂设置、设置移动终端的工作频率、调节终端传输速率等用户操作指令。

操作系统应禁止开放可以旁路移动终端安全策略的用户操作指令，如不需要用户口令就可以对移动终端解锁、对网络解锁的用户操作指令等。

操作系统应禁止开放对移动终端内存中所存储数据进行修改、删除的用户操作指令，如直接对存放移动终端解锁码的内存字段进行修改、直接清除内存中存储的用户电话号码的用户操作指令等。

操作系统应禁止开放使终端进入调试或工程模式的用户操作指令。

操作系统应具有对用户操作指令使用事件进行记录的能力，记录的详细要求及日志文件的安全要求参见7.3.4。

7.3 系统管理

7.3.1 配置信息管理

移动终端中的配置信息主要包括操作系统、驱动程序、应用程序的设置参数、版本号、生产厂商、安装时间、占用内存空间大小等。

操作系统应通过文件或数据库的形式记录移动终端中的各种配置信息，并对其设置不同的访问控制权限。

当对操作系统、驱动程序、应用程序进行更新后，操作系统应及时的更改其对应的配置信息。

当对驱动程序、应用程序进行删除后，操作系统应及时的删除其对应的配置信息。

当在操作系统中安装新的驱动程序、应用程序后，操作系统应及时的建立其对应的配置信息。

对于操作系统、驱动程序、应用程序的设置参数，应只对授权用户提供读取的权限，但不提供修改、删除的权限。

7.3.2 设备管理

本标准中的设备管理主要包括移动终端中硬件的基本信息（硬件提供商、序列号信息等）管理、内存空间的管理、外接硬件设备的加载与卸载管理等。

操作系统应以文件的形式记录硬件的基本信息、内存空间使用情况等，并对授权用户提供读取的权限，但不提供修改、删除的访问权限。

当移动终端中的硬件被合法更换后，操作系统应能及时更新硬件的基本信息。

操作系统应实时监控内存空间的使用并更新内存空间的使用情况记录，当发现内存空间不足，应能提示用户。

操作系统应能实时检测到外接硬件设备的加载操作，当发现有外接硬件连到移动终端后，应及时提示用户外接硬件设备的加载状态。

操作系统应提供友好的用户界面让用户执行外接设备的卸载操作，当移动终端和外接设备有数据交互时，操作系统应提示用户禁止执行此次卸载操作。

在进行操作系统设计时，应充分考虑当外接设备卸载失败或被突然拔出等异常情况可能对移动终端造成的后果及应对措施，应保证当异常情况发生后，不影响系统的正常运行，或即使发生系统异常或崩溃，重启后，系统可返回到正常运行状态。

7.3.3 软件管理

7.3.3.1 软件的安装管理

移动终端操作系统应确保应用软件安装过程的安全可靠。

移动终端操作系统应保证当应用安装失败或取消后，系统可返回到一个安全状态。

移动终端操作系统应确保安装过程不能旁路操作系统所具有的安全策略，不能影响已有应用的代码、数据、功能和状态等。

在软件安装过程中，移动终端应对软件来源的合法性进行验证，如果软件没有提供证明其合法性的措施，那么移动终端应采取以下措施中的一或几种：

1） 继续安装；

2） 拒绝安装。

如果用户选择了继续安装，安装成功后，该软件应不能运行。

7.3.3.2 软件的更新管理

移动终端操作系统应确保应用程序更新过程的安全可靠。

更新移动终端上的应用不能影响其他应用的完整性，不能旁路移动终端所具有的安全策略，不能为系统引入安全风险。

应充分考虑在更新过程中发生掉电或其他异常时所可能带来的后果，以及对应的解决办法。

7.3.3.3 软件的删除管理

移动终端操作系统应提供一种机制可以删除存储在移动终端中的各种应用软件，以释放移动终端的存储器空间。

移动终端操作系统应确保应用软件删除过程的安全可靠。

删除移动终端上的应用不能影响其他应用的完整性，不能旁路终端所具有的安全策略，不能为系统引入安全风险。

当移动终端上的应用被删除后，应确保应用所拥有的数据同时也被释放掉或不可用。

应充分考虑在删除过程中发生掉电或其他异常时可能带来的后果，以及对应的解决办法。

7.3.3.4 对象的删除管理

本小节的对象为应用程序所指向或创建的数据、实例等。

移动终端操作系统应确保应用软件在删除其所拥有的未被其他应用程序所共享对象过程的安全可靠。

移动终端操作系统在删除指向不再使用或用于其他目的内存区域的对象时，应不能为系统引入新的安全风险或不稳定因素。

终端操作系统应确保应用软件在删除对象时，不能旁路终端所具有的安全策略，如不能删除和其他应用所共享的对象等。

终端操作系统应确保已删除对象不能再被应用程序恶意调用，以避免造成系统异常或崩溃。

7.3.4 日志管理

日志管理包括对系统日志，应用程序安装、更新、删除日志，用户操作过程中的错误日志，历史记录以及与安全事件相关的审计记录等进行管理。操作系统应确保正确、及时的对所发生的事件进行记录，所有的日志至少应包括事件发生的日期、时间、事件发起者、事件类型、事件简单描述信息等内容。

由于日志文件反映了系统的安全状态、用户的使用习惯等信息，操作系统应对日志文件进行加密存储，并只对授权用户提供访问权限。

操作系统应提供界面让授权用户访问日志文件，并允许授权用户对日志文件内容进行全部删除或部分删除。

操作系统应限定每个日志文件的大小，当文件大小达到预先设定的值后，操作系统决定如何进行下一步操作，如存储到外设上，或直接删除等。

操作系统应允许授权用户远程调用日志文件，远程调用命令要求见7.3.5。

7.3.5 远程操作的管理（可选）

远程操作管理包括远程文件内容修改、删除、读取；程应用软件的更新、删除、安装；程锁定与解锁移动终端的某项功能；远程关机、远程功能诊断等。

远程安装、删除、更新应用软件的安全要求同 7.3.3。

移动终端的某项功能被锁定后，在未被解锁前，该功能就不能被执行。

可被远程更新的文件应限定在预先指定的范围内，指定为不可被远程更新的文件应不能被远程文件管理更新。终端操作系统应提供措施对文件的更新属性进行管理。

由于远程操作管理命令一般是通过无线方式进行传播，该命令就有可能被外界所窃听、篡改，甚至被恶意攻击者所分析利用，造成移动终端用户的损失，因此对应特殊的应用应采用较高级别的安全措施，如下：

1） 应对远程操作管理命令的特殊字段进行加密处理，以保证命令的机密性；

2） 应对远程操作管理命令进行校验处理，以防止命令被攻击者所篡改。

有选择地使用源认证、数字签名等安全措施，以进一步保证远程操作管理的安全。

7.4 安全服务

7.4.1 程序加载的控制管理

移动终端在加载程序前，应对终端内剩余空间的统计，记录用户可以实际可以使用的空间大小，如果存储空间不足，就中止程序加载，并提示给用户。

如果在加载过程发生掉电、中断等异常，移动终端应该具有处理加载失败的能力，并删除已经加载到移动终端上的部分程序。

移动终端应只能将加载程序存放在预先定义的应用程序存储空间。

对于被动接收的程序加载过程，移动终端应对程序的来源进行认证。

移动终端应能对已加载程序代码（包括安装代码、可执行代码）的可靠性进行检查，如是否存在引起缓冲区溢出、内存泄漏的指令等。

7.4.2 用户通知

对于移动终端上发生的某些事件，例如证书接收、证书到期、程序运行异常等事件，以及对终端安全构成威胁的某些操作，移动终端应能及时向用户发出通知，由用户决定下一步动作。对于可能构成安全威胁的某些操作，向用户通知的内容应包括安全威胁类型以及相应操作的潜在威胁信息。对于较严重的安全威胁需有手段强化通知，防止系统遭到破坏。

8 移动终端接入安全要求

8.1 接入安全

移动终端通过空中接口和基站子系统接入移动通信网络，2G（GSM/CDMA）、3G（WCDMA/cdma2000/TD-SCDMA）移动通信技术的终端接入技术各有特点、不尽相同，但都对移动终端接入网络的信息安全问题作出了明确和详细的规定。为使本标准所涵盖的移动终端信息安全内容更加全面，本标准将引用2G、3G相关标准中有关接入信息安全的内容作为本标准的要求。

8.2 基本业务与功能

移动终端应能够成功发起紧急呼叫。

移动终端应能够成功始发和接收点对点短消息。

移动终端应能够正确显示主叫号码，并能够正确显示被叫号码。

移动终端应能够正常启用、关闭以下补充业务：

— 主叫号码识别限制；

— 无条件呼叫前转；

— 遇忙呼叫前转；

— 遇无应答呼叫前转；

— 用户不可及呼叫前转；

— 呼叫等待；

— 呼叫保持。

8.3 安全接入相关信令协议

8.3.1 鉴权

移动终端应支持接入移动网络时的鉴权要求，与网络正确交互有关鉴权接入的协议，符合相应的国

际标准或行业标准的要求。

对于 GSM/GPRS 终端、WCDMA 终端、cdma2000 终端，终端接入移动通信网络的鉴权过程应满足相应规范的要求，具体如下：

GSM/GPRS 终端接入鉴权应满足 YD/T 1214-2006《900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术要求：移动台》中第 5.5.3.7 节“安全保密功能”以及 3GPP TS 24.008《移动无线接口层三规范：核心网协议》的要求。

WCDMA 终端接入鉴权应满足 3GPP TS 34.123-1《用户设备（UE）一致性规范；第一部分：协议一致性规范》中 9.1 节“TMSI 分配”，9.2 节“鉴权”，9.3 节“鉴定”的要求。

cdma2000 终端接入鉴权应满足 YD/T 1558-2007《2GHz cdma2000 数字蜂窝移动通信网设备技术要求：移动台》的要求。

8.3.2 数据加密

移动终端应支持接入移动网络的数据加密要求，符合相应的国际标准或行业标准的要求。

对于 GSM/GPRS 终端、WCDMA 终端、cdma2000 终端，终端接入移动通信网络的数据加密应满足相应规范的要求，具体如下：

GSM/GPRS 终端数据加密应满足 YD/T 1214-2006 第 5.5.2 节“分组路由和传输功能的要求”，3GPP TS 24.008 和 3GPP TS 01.61《GPRS 加密算法要求》的要求。

WCDMA 终端数据加密应满足 3GPP TS 34.123-1 中 8.1.7 节“安全模式命令”和 8.1.12 节“完整性保护”的要求。

cdma2000 终端数据加密应满足 YD/T 1558-2007 的要求。

8.3.3 信令完整性保护

WCDMA 终端信令完整性保护应满足 3GPP TS 34.123-1 中 8.1.12 节“完整性保护”的要求。

8.3.4 紧急呼叫

移动终端应支持接入移动网络后相应的紧急呼叫要求，符合相应的国际标准或行业标准的要求。对于 GSM/GPRS 终端、WCDMA 终端、cdma2000 终端，终端接入移动通信网络后应支持紧急呼叫，满足相应规范的要求，具体如下：

GSM/GPRS 终端紧急呼叫应满足 YD/T 1214-2006 中 5.2.1 节“电信业务”的要求。

WCDMA 终端紧急呼叫应满足 3GPP TS 34.123-1 中 13 章“常规测试”有关紧急呼叫的要求。

cdma2000终端紧急呼叫应满足YD/T 1558-2007的要求。

9 移动终端与卡间的数据传输

对于机卡分离的移动终端，其卡接口的电信号和传输协议应满足 GB/T 16649.3《识别卡 带触点的集成电路卡 第 3 部分：电信号和传输协议》（idt ISO/IEC 7816-3）的要求。对于 GSM/GPRS 终端、WCDMA 终端、TD-SCDMA 终端、cdma2000 终端，其卡接口不仅要满足 GB/T 16649.3（idt ISO/IEC 7816-3）的要求，还应满足相应规范的要求，具体如下：

GSM/GPRS 终端卡接口应满足 YD/T 1215-2006《900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：移动台》中第 7.2 节“SIM/ME 接口”的要求。

WCDMA 终端、TD-SCDMA 终端卡接口应满足 ETSI TS 102 221《智能卡；UICC—终端接口；物理和逻辑》和 3GPP TS 31.102《USIM 应用特性》的要求。

cdma2000 终端卡接口应满足 YD/T 1168-2007《CDMA 数字蜂窝移动通信网用户识别模块（UIM）技术要求》的要求。

移动终端应只执行和响应相应规范中所规定的指令，并按照要求对指令的格式、参数等进行检查。

移动终端在与电信智能卡交互过程中，应保证送出数据的完整性，并对读入的具有完整性需求的数据进行完整性校验。当读入数据因为数据错误等原因而不能通过数据完整性校验时，移动终端应按照规范的要求采取相应的动作。

移动终端应禁止把移动终端中存储的密钥、配置信息、保密数据等传输到卡中。

对于支持对电信智能卡进行认证的移动终端，应只接受来自合法电信智能卡传输的数据和指令。

10 移动终端对业务应用的安全支持

10.1 安全组件的概念

移动终端上可以承载多种业务，同时终端应保证各种业务的安全性，安全组件即是移动终端对所承载的各类业务的安全支持，通过各种安全组件的灵活使用可以为业务应用提供不同类别的安全服务，同时安全组件使系统和业务的安全性具有一定的能见度和可配置性。

保障移动终端上所承载业务的安全需要从以下几个安全属性考虑：机密性、完整性、鉴权和非否定性，因此保障业务的安全至少应包含数据加解密、数据完整性、身份认证、签名与验证等几类安全组件。DRM、PIM 组件是保障特定业务安全的一类安全组件。

各类安全组件功能的实现独立于移动终端系统，具有开放、通用的应用接口，供上层业务灵活使用，同时支持多业务的并发使用。

安全组件可以通过软件或硬件的形式实现，但使用规范的应用接口。

10.2 安全组件应用的策略

根据所承载业务不同的安全需求和安全应用策略灵活使用安全组件，开机时应提供移动终端对安全组件的完整性检验。对于以硬件方式实现的安全组件，开机时还应提供对安全组件的鉴别。

10.3 安全组件的类别

10.3.1 数据加解密

该组件为移动终端的机密数据、敏感数据的传递、储存提供有效保护。该组件实现了对称密码体制和非对密码体制的多种算法的加解密功能，根据输入参数选择具体的算法，对指定的数据进行加密或解密运算，并将结果提交使用者。

10.3.2 数据完整性

该组件为移动终端所承载的应用业务提供数据完整性服务，业务数据、敏感数据在传送、储存之前受到完整性保护，同时提供业务数据、敏感数据在接收、读取后的数据完整性验证，防止用户的业务数据和敏感数据受到未授权用户的修改或破坏，而接收或读取者却未能检测。该组件可与数据加解密组件配合应用，既保证业务数据的完整性又保障数据的机密性。对于不同的业务应用提供其对应的完整性支持，具体实现可参见 ANSI X9.9《金融机构的消息鉴别》、ISO 8730《银行业务—消息鉴别要求》及 GB/T 15851《信息技术 安全技术 带消息恢复的数字签名方案》（idt ISO/IEC 9796）。

该组件支持封装、完整性校验值、消息认证码（MAC）、消息完整性码（MIC）和散列函数等方法来保护数据的完整性，具体采用的方法可根据引擎参数进行选择。

10.3.3 身份认证

该组件以多种方式对移动终端以及其承载的业务提供身份识别服务。

10.3.3.1 用户口令字

用户口令字作为身份认证的一种方式，应能根据业务的安全要求而具有相应的防攻击强度，安全要求越高，用户口令字应该越长。该组件应能为用户提供一次性口令字验证和非一次性口令验证。并提供试探连续次数限制功能，在达到最大尝试次数后，此组件将拒绝对该用户的服务。

该组件允许用户更改口令字，并通过加密存储或采用域隔离等方式保证用户口令字在终端内存储的安全性。具体实现参见 5.8“安全域隔离”。

10.3.3.2 认证协议

认证协议作为身份认证的一种方式，是通过交互的方式实现对移动终端上应用业务通信双方的身份进行认证的，该组件可提供通信双方的单向或双向认证，对认证交互过程中所需要的随机数由随机数产生组件提供，以保证随机数的质量，该组件应保证业务通信双方严格按照认证协议规定的流程执行。

该组件的实现可参见 GB/T15843.2《信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制》和 GB/T15843.3《信息技术 安全技术 实体鉴别 第 3 部分：用非对称签名技术的机制》。

10.3.4 数字签名

该组件可以为移动终端所承载的业务提供不可否认性方面的安全支持，以避免通过终端实现的业务完成后不承担后果。

为了支持业务的不可否认性，该组件能：

1） 确保通过安全的途径获取/更换所用的签名密钥和验证密钥；

2） 确保签名密钥和验证密钥在终端中存储的安全性；

3） 提供多种数字签名业务，但使用统一的签名算法接口与验证算法接口。

该组件的实现可参见 GB/T15843.3《信息技术、安全技术实体鉴别 第 3 部分：采用非对称签名技术的机制》。

10.3.5 随机数组件

该组件为上层业务提供随机数支持，可以根据上层应用对随机数属性的描述产生相应的随机数，并选用频数、扑克、游程、自相关、序偶五类方法（可根据对随机数的要求可采用一种或多种）对随机数的随机性进行检验，以保证随机数的质量，为移动终端承载的各种业务的安全提供随机数保障。

10.3.6 密钥管理

该组件为移动终端承载的各种业务应用所需的密钥进行管理，对密钥产生、密钥协商、密钥存储、密钥使用/更换、密钥销毁等各环节进行管理，确保密钥在整个生命周期内的安全，目的是保护秘密密钥或私有密钥免受未经授权的获取、修改和替换，保护公开密钥免受未经授权的修改和替换。

1） 密钥产生

所有密钥的产生均使用经国家密码管理机构的审批的随机数发生器或伪随机数发生器，并且对所产生的密钥进行检测以排除可能的弱密钥；对于公钥密码体制，采用经国家密码管理机构批准的密钥生成算法。

2） 密钥存储

对存储的密钥进行完整性保护，以明文方式存储的密钥均有防护措施，以防被非授权应用获取；经加密后存放的密钥，其保护算法和安全防护机制是安全可靠的，并与对其加密所用的密钥分离存放。具

体可参见 5 .7.1.1 “数据的安全分级存储”。

3） 密钥使用

密钥在使用时均对其进行正确性、完整性检测，同时各种密钥的使用完全遵循其规定的用途，并在一定的防护措施下使用密钥。

4） 密钥更换

在移动终端上支持各类业务的密钥需要在其有效期前更换，当密钥可能被泄露时需停止使用。密钥不应长期使用，应根据业务需求定期更换；在密钥生命期结束或认为密钥出现安全隐患的情况下，应更换密钥并提示用户，以保障业务的安全性。

5） 密钥销毁

当不再需要提供安全服务的业务终止或移动终端失窃等特殊情况下，如终止移动支付、撤销信息定制服务等，移动终端能够提供密钥销毁的功能。密钥销毁应简便、快速、彻底；密钥销毁机制应当有效，并确保已经销毁的密钥无法完全或部分恢复。

10.3.7 证书管理

该组件对各种业务所需的证书进行管理，包括：

1） 通过可靠的技术手段（外设接口、通信口、无线接口）获取与业务/使用者身份捆绑的个人证书和可信任的第三方证书；

2） 能够对证书的合法性进行检验；

3） 能将证书存放在安全区域或以密文方式存储来保证其安全性；

4） 能通过外设接口、通信口、无线接口上利用安全协议更换证书；

5） 能保证个人证书、可信任的第三方证书的安全销毁。

10.3.8 DRM

DRM 组件的实施使移动终端能支持受 DRM 技术保护的内容的使用。

DRM 组件具有如下功能：

1） 有获取受 DRM 技术保护的内容使用许可证的方法；

2） 能够严格执行许可证中规定用户对受 DRM 保护内容使用的权利与限制；

3） 能安全保存授权机构发布的使用许可证；

4） 能够识别授权机构发布的使用许可证的失效。

DRM 组件的实现可以参考 OMA—DRM v2.0 标准中对 DRM 代理的要求。

10.3.9 PIM

PIM 组件提供对终端上承载的用户个人信息管理业务的安全支持。用户可以在此组件的支持下安全地进行收发邮件管理、个人账务管理、网络信息管理、计划任务管理、分组管理、日程提醒等操作。

该组件具有如下功能：

1） 保证用户信息在数据传输过程中的安全；

2） 保证用户信息在移动终端上的安全存储。