ICS 35.030(国际标准分类号)
I65(中国标准文献分类号)

团 体 标 准

T/SCCIA 014 —2024

鸿蒙数据终端管理系统密码应用基本要求

Basic Requirements for Cryptography Application in OpenHarmony Data Terminal Management System.

2024－12－05 发布　　2024－12－05 实施

深圳市商用密码行业协会 发布

目　　次

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由深圳市商用密码行业协会提出并归口。

本文件起草单位：哈尔滨工业大学（深圳）、深圳市证通电子股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、深圳市证通金信科技有限公司、深圳市证开鸿科技有限公司、鼎链数字科技（深圳）有限公司、深圳市马博士网络科技有限公司、深圳开鸿数字产业发展有限公司。

本文件主要起草人：何道敬、程胜春、陈磊、李大为、曾培恒、付庆、龚志勇、胡迎春、苏年乐、马永发、徐江斌、肖飞、王广武、黄励星、王皓、孙碧锋、高山峰。

引　言

本文描述了鸿蒙数据终端管理系统密码应用技术基本要求。

鸿蒙数据终端是采用国产鸿蒙开源操作系统，实现的一类数据终端，作为万物互联时代的新型终端，鸿蒙数据终端采用国产鸿蒙开源操作系统，可应用于金融、政务、教育和医疗等多个领域，其形态包括：各类多功能银行收付款终端、政务大厅自助办事终端、医院自助缴费终端和学校自助打印成绩单终端等。一般由后台终端管理系统对终端统一管理，如接入认证、数据安全传输和固件升级等功能。

终端管理系统的安全，是数据终端安全的重要环节，为提高终端管理系统在终端管理过程中的安全防护能力，需采用密码技术满足终端管理系统在部署环境、网络通信、计算环境和管理系统等方面的安全需求。

本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

鸿蒙数据终端管理系统密码应用基本要求

1 范围

本标准规范了鸿蒙数据终端管理系统的密码应用基本要求，从部署环境安全、网络通信安全、计算环境安全和终端管理系统安全四个技术层面提出了鸿蒙数据终端管理系统的密码应用技术要求，并从管理制度、人员管理、建设运行和应急处置四个方面提出了鸿蒙数据终端管理系统的密码应用管理要求。

本标准适用于指导、规范鸿蒙数据终端管理系统密码应用的规划、建设、运行及测评，也用于指导鸿蒙数据终端管理系统密码应用设计和开发。

2 规范性引用文件

下列文件对于本文件的应用必不可少的。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 37092-2018 信息安全技术 密码模块安全要求

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 43207-2023 信息安全技术 信息系统密码应用设计指南

3 术语和定义

GB/T 37092-2018、GB/T 39786-2021、GB/T 43207-2023 界定的术语和定义适用于本文件。

3.1 数据终端 data terminal

能够接收、处理、存储和传输数据的设备。

3.2 数据终端管理系统 data terminal management system

用于管理和监控数据终端运行、配置和维护的软件系统或平台。

3.3 鸿蒙操作系统 OpenHarmony OS

OpenHarmony 操作系统或基于 OpenHarmony 操作系统的行业发行版系统。

3.4 国产化 national

在产品或服务中采用国内自主研发的技术和标准，以替代过去依赖的进口产品和技术。

4 通用要求

鸿蒙数据终端管理系统应符合以下通用要求：

a）终端管理系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

b）终端管理系统中使用的密码应用技术应遵循密码相关国家标准和行业标准；

c）终端管理系统中使用的密码产品、密码服务应符合法律法规的相关要求；

a） 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

b） 以上采用的密码产品，应达到GB/T 37092-2018二级及以上安全要求。

5 鸿蒙数据终端管理系统模型

鸿蒙数据终端管理系统参考模型见图1。

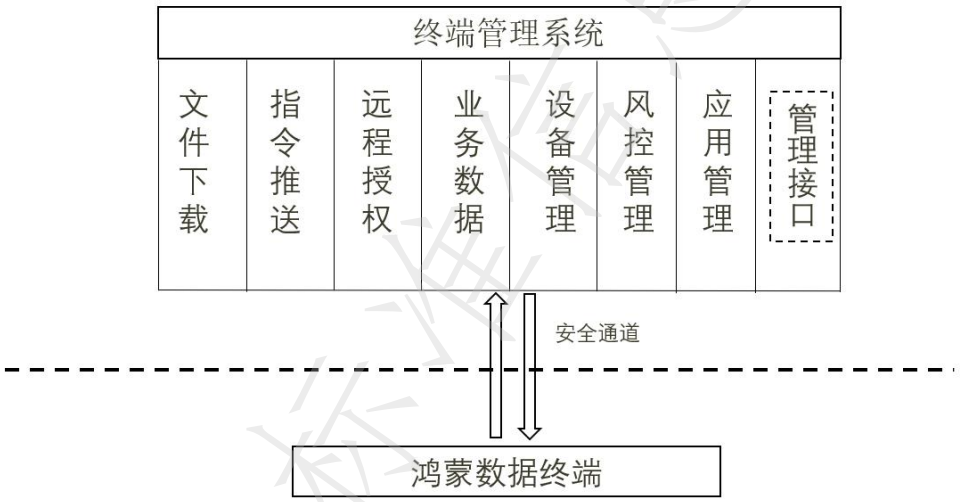

图1 鸿蒙数据终端管理系统逻辑框图

鸿蒙数据终端管理系统使用包括密码在内的各种安全技术来保障业务安全。按照业务过程包括文件下载、指令推送、远程授权、业务数据、设备管理、风控管理、应用管理和管理接口。本标准从部署环境安全、网络通信安全、计算环境安全、终端管理系统安全、管理制度、人员管理、建设运行和应急处置进行针对性设计。

文件下载:鸿蒙数据终端管理系统与终端共同完成包括固件、应用和系统等文件的全量和增量下载，因传输数据大，需通过单独的文件传输通道下载。

指令推送：鸿蒙数据终端管理系统向终端发送应用下载等指令，通过报文传输通道完成指令推送。

远程授权：鸿蒙数据终端管理系统完成远程清除终端的自毁标识、远程关闭终端验签功能和打开指定终端的调试功能等操作。

业务数据：设定的终端心跳间隔数据、终端定位参数、终端系统版本、固件版本等配置信息和用户密码、渠道商信息、设备类型、设备型号、设备信息、系统文件、设备应用、设备动画、设备固件、客户证书等设备信息。

设备管理：鸿蒙数据终端管理系统完成终端在线、自毁和调试模式等状态查询操作，维护终端所属客户和系统版本信息等基础信息。

风控管理：鸿蒙数据终端管理系统设置终端的位置范围，展示终端预警信息，监督终端地理位置，发送终端锁机指令，围栏解绑终端等操作。

应用管理：鸿蒙数据终端管理系统进行终端应用文件上传、应用基本信息管理、应用签名、应用版本校验、版本管理、应用审核、应用上架和下架操作。

管理接口：鸿蒙数据终端管理系统提供给第三方应用的设备管理数据接口(若有)，包含设备在线等数据信息。

6 鸿蒙数据终端管理系统密码安全保护要求

6.1 部署环境安全

鸿蒙数据终端管理系统应部署在满足安全要求的物理机房，机房安全要求包括：

a）应采用密码技术进行物理访问身份鉴别，保证机房进入人员身份的真实性；

b）宜采用密码技术保证机房电子门禁系统进出记录数据的存储完整性；

c）宜采用密码技术保证机房视频监控音像记录数据的存储完整性。

6.2 网络通信安全

鸿蒙数据终端管理系统的网络通信通道，包括终端管理系统与鸿蒙数据终端之间，终端管理系统与系统前端（浏览器、管理 APP 和管理客户端等）之间的通信通道，通信安全要求包括：

a）应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

b）应采用密码技术保证通信过程中数据的完整性；

c）应采用密码技术保证通信过程中重要数据的机密性；

d）宜采用密码技术保证网络边界访问控制信息的完整性；

e）宜采用密码技术实现数据终端接入管理系统的认证，确保接入的设备身份真实性，并记录首次接入信息。

6.3 计算环境安全

鸿蒙数据终端管理系统应部署在国产化服务器（或云平台），采用通过政府有关部门指定的包括但不限于国信息安全测评中心和国家保密科技测评中心等网站上可查看安全可靠测评结果的操作系统、国产数据库系统（如有）满足其运行功能需求，以及采用通过商密认证的密码产品保障其密码应用安全，计算环境安全要求包括：

a）应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；

b）远程管理设备时，应采用密码技术建立安全的信息传输通道；

c）宜采用密码技术保证系统资源访问控制信息的完整性；

d）若涉及重要信息资源安全标记，宜采用密码技术保证设备中的重要信息资源安全标记的完整性；

e）宜采用密码技术保证设备操作日志记录的完整性；

f）宜采用密码技术对关键应用、数据库系统等重要可执行程序进行完整性保护，并对其来源进行真实性验证。

6.4 终端管理系统安全

6.4.1 用户安全

a）应采用密码技术对登录用户进行身份鉴别，保证数据终端管理系统用户身份的真实性；

b）应通过鉴别的真实身份确定对信息内容和系统应用的访问权限，并采用密码技术保证信息系统应用的访问控制信息的完整性。

6.4.2 终端管理接口

鸿蒙终端管理系统若具备对第三方应用提供终端管理接口，满足第三方应用的终端管理要求等功能，

终端管理接口的要求如下：

a）宜采用密码技术，在第三方应用调用服务接口时进行鉴权；

b）应有接口调用的日志记录，并采用密码技术保证日志记录的完整性；

c）宜检查接口的必需参数，包括不限于终端编号、时间戳、令牌和随机数，并采用密码技术实现必需参数的完整性保护。

6.4.3 数据传输安全

鸿蒙数据终端应具备安全通信模块，实现数据终端与终端管理系统的实体身份鉴别和数据传输安全。

a）应采用密码技术对数据终端与终端管理系统之间的通信实体进行身份鉴别，保证通信实体身份的真实性；

b）应采用密码技术保证终端管理系统与数据终端通信过程中重要数据的机密性；

c）终端管理系统在指令推送、远程授权、设备管理和风控管理等功能中发送的控制指令，以及传输数据终端固件时，应采用数字签名机制，实现指令和固件传输的完整性，其中签名公钥通过终端管理系统安全传输至各数据终端并安全存储，同时通过密码技术防止公钥被非授权篡改、替换；

d）鸿蒙数据终端管理系统推送文件下载指令，终端接收到相关指令后，根据具体参数进行全量和增量文件下载，在下载过程中支持文件校验和加密传输。

6.4.4 数据存储安全

鸿蒙数据终端应具备数据保护能力，实现重要数据的存储机密性和完整性。

a）终端管理系统存储的重要数据包括但不限于终端心跳间隔数据等配置信息、用户口令、渠道商信息、设备类型、设备型号、设备信息、系统文件、设备应用、设备动画、设备固件和客户证书等，应采用密码技术实现重要数据存储过程的机密性和完整性保护；

b）应采用密码技术实现终端管理系统日志记录（包括但不限于设备使用情况日志和管理系统日志）的存储完整性保护；

c）宜采用密码技术保证设备中的重要信息资源安全标记（包括但不限于厂商证书、用户证书和设备配置信息）的完整性。

6.4.5 应用管理

终端管理系统为鸿蒙终端提供可信任的终端应用文件（APP）的管理和维护功能。

a）应用程序开发者应使用合规机构颁发的数字证书对应用程序进行签名，应用管理系统对应用程序进行验证后上架，并在分发应用时对应用进行签名，保证应用程序的完整性；

b）应使用密码技术实现应用程序传输的机密性和完整性。

6.4.6 密钥安全

a) 应定期对终端管理系统与数据终端之间传输数据使用的密钥进行更新；

b) 应对终端管理系统的密钥生存周期进行管理，制定符合 GB/T 39786-2021 和 GB/T 43207-2023 等标准要求的密钥管理制度。

7 鸿蒙数据终端管理系统密码管理要求

7.1 管理制度

鸿蒙数据终端管理系统应符合以下管理制度要求：

a）应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
b）应建立相应密钥管理规则；
c）应对管理人员或操作人员执行的日常管理操作建立操作规程；
d）应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
e）应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
f）应具有密码应用操作规程的相关执行记录并妥善保存。

7.2 人员管理

鸿蒙数据终端管理系统应符合以下人员管理要求：
a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
b）应根据密码应用方案建立相应密钥管理规则；
c）应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限：

1）根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；

2）对关键岗位建立多人共管机制；

3）密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；

4）相关设备与系统的管理和使用账号不得多人共用。

5）密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任，并应在任前对其进行背景调查。

d）应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
e）应定期对密码应用安全岗位人员进行考核；
f）应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

7.3 建设运行

鸿蒙数据终端管理系统应符合以下建设运行要求：
a）应依据密码相关标准和密码应用需求，制定密码应用方案；
b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节；
c）应按照应用方案实施建设；
d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
e）在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

7.4 应急处置

鸿蒙数据终端管理系统应符合以下应急处置要求：
a）当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
b）监控和收集与密码应用相关的异常安全状态信息,识别和记录与密码应用相关的入侵行为,对密码应用的安全状态进行监控；
c）当安全状态异常，发生密码应用安全事件时，根据应急策略否启动应急程序，开展应急处置措施，

结合实际情况及时处置；

d）事件发生后，应及时向信息系统主管部门进行报告；

e）事件处置完成后，应及时向主管部门及归属的密码管理部门报告事件发生情况及处置情况。