ICS 35.240
CCS L 70/84

团　　体　　标　　准

T/ZISIA 0101-2025

通用操作系统商用密码子系统安全轮廓

Security profile for commercial cipher subsystem of general purpose operating system

2025-04-20 发布　　2025-04-20 实施

中关村网络安全与信息化产业联盟　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。

本文件由中关村网络安全与信息化产业联盟提出并归口。

本文件起草单位：中关村网络安全与信息化产业联盟、麒麟软件有限公司、中科方德软件有限公司、阿里云计算有限公司、兴唐通信科技有限公司、蚂蚁科技集团股份有限公司、北京天威诚信电子商务服务有限公司、江南信安（北京）科技有限公司、北京吉大正元信息技术有限公司、北京三博安科技有限公司、神州网络信息技术有限公司。

本文件主要起草人：王震、张大朋、岳佳圆、郭亮、胡昆、龚文、刘赢、冯建茹、时圣亮、李世奇、张天佳、姚长远、王辉、钱程、杨洋、张成龙、郭智慧、王尧、李延昭、胡冰、白锦龙、汪海洋、徐剑南、杨子峰、王彤、何道君、王立臣、吕明、王克、胡金山、罗捷、李彬安、刘海涛、林璟锵、王强、黄建忠。

引　言

密码是保障网络与信息安全的核心技术和基础支撑，通过加密保护和安全认证两大核心功能，为信息系统的机密性、完整性、真实性和不可否认性提供可靠的安全保障。

作为计算机系统基础软件，现代操作系统广泛运用密码技术以保护系统自身安全，系统安全启动、用户身份鉴别、代码签名/验证、数据加密保护等，都依赖密码技术。可以说，没有密码技术支撑保护，就没有操作系统安全，网络信息系统安全也难以保证。

目前，国内操作系统普遍使用国外密码算法和密码资源，商用密码算法的使用缺乏顶层规划和标准规范，存在密码使用不规范、不正确、不安全，密钥、证书等敏感数据保护不严格，密码资源调用接口不统一，第三方密码产品适配难等问题。

为解决上述问题，本文件将操作系统内各种密码功能组件逻辑上作为一个特殊的密码模块进行规范，依据国家有关标准，提出操作系统密码子系统的安全功能要求、安全保障要求及评估方法，为密码子系统实现、使用和操作系统密码安全应用提供指导。

通用操作系统商用密码子系统安全轮廓

1. 范围

本文件规定了通用操作系统商用密码子系统的安全功能要求和安全保障要求。

本文件适用于指导操作系统商用密码子系统的开发、使用、管理和检测。

2. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 17964-2021 信息安全技术 分组密码算法的工作模式

GB/T 20272-2019 信息安全技术 操作系统安全技术要求

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918 （所有部分）信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 33133 （所有部分）信息安全技术 祖冲之序列密码算法

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

GM/T 0044 （所有部分）SM9 标识密码算法

GM/T 0062-2018 密码产品随机数检测要求

GM/T 0091 基于口令的密钥派生规范

GM/T 0092 基于SM2算法的证书申请语法规范

GM/T 0129 SSH密码协议规范

GM/Z 4001-2013 密码术语

3. 术语和定义

GB/T 25069、GM/Z 4001-2013界定的以及下列术语和定义适用于本文件。

3.1

引导加载器 boot loader

计算机启动过程中运行的一段程序，负责初始化计算机硬件设备、检测可启动的操作系统、将操作系统内核加载到内存并将系统控制权传递给操作系统内核，从而使操作系统能够正常启动和运行。

3.2

启动垫片 boot shim

一种在操作系统启动过程中的过渡阶段运行的软件，它位于BIOS/UEFI和操作系统内核之间，以增强系统安全性，方便在同一台计算机上安装和启动多个操作系统。

3.3

证书 certificate

关于实体的一种数据，该数据由认证机构的私钥或秘密密钥签发，并无法伪造。

[来源：GB/T 37092-2018，3.1]

3.4

证书认证机构 certification authority（CA）

对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。

[来源：GM/Z 4001-2013，2.145]

3.5

密码模块 cryptographic module

实现密码运算功能的、相对独立的软件、硬件、固件或其组合。

[来源：GM/Z 4001-2013，2.53]

3.6

数据加密密钥 data encryption key（DEK）

用于对数据进行加密或解密的密钥。

3.7

有限状态模型 finite state model（FSM）

序列机的一种数学模型，该模型包含输入事件的有限集合、输出事件的有限集合、状态的有限集合、将状态和输入映射到状态的函数（状态转移函数）以及初始状态的说明。

3.8

多因素鉴别 multi-factor authentication

至少具有两个独立鉴别因素的鉴别。

注：独立的鉴别因素类别包括：已知某物，拥有某物，以及具有某属性。

[来源：GB/T 37092-2018，3.10]

3.9

密钥加密密钥 key encryption key（KEK）

用于对密钥进行加密或解密的密钥。

[来源：GM/Z 4001-2013，2.78]

3.10

操作系统容器 operating system containers

一种虚拟化技术，允许在单个操作系统内核上运行多个独立的用户空间实例。这些实例被称为容器（containers）。每个容器包含其自己的文件系统、进程空间、网络接口和 IPC（进程间通信）资源，但共享宿主操作系统的内核。这使得容器比传统虚拟机更加轻量级，因为它们不需要包含完整的操作系统内核。

3.11

根密钥 root key（RK）

用于生成派生密钥的密钥。

[来源：GB/T 25069-2022，3.204]

3.12

安全启动 secure boot

一种确保计算机只运行可信软件的安全功能，主要目的是防止能够感染操作系统引导加载程序和系统固件的恶意软件。其工作原理是验证每个阶段的引导加载程序和操作系统内核是否具有有效的数字签名。

3.13

SM2算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。

[来源：GM/Z 4001-2013，2.118]

3.14

SM3算法 SM3 algorithm

一种密码杂凑算法，其输出为256比特。

[来源：GM/Z 4001-2013，2.119]

3.15

SM4算法 SM4 algorithm

一种分组密码算法，分组长度为128比特，密钥长度为128比特。

[来源：GM/Z 4001-2013，2.120]

3.16

SM9密码算法 SM9 algorithm

一种基于身份标识的非对称密码算法。

[来源：GM/Z 4001-2013，2.122]

3.17

祖冲之序列密码算法 ZUC stream cipher algorithm
一种序列密码算法。
[来源：GM/Z 4001—2013，2.154]

4. 符号和缩略语

下列缩略语适用于本文件。
API：应用程序接口（Application Program Interface）
CA：证书认证机构（Certification Authority）
DEK：数据加密密钥（Data Encryption Key）
FSM：有限状态模型（Finite State Model）
HMAC：基于杂凑的消息鉴别码（Hash-Based Message Authentication Code）
KEK：密钥加密密钥（Key Encryption Key）
OS：操作系统（Operation System）
RK：根密钥（Root Key）
SSH：安全交互（Secure Shell）
TCM：可信密码模块（Trusted Cryptography Module）
TPM：可信平台模块（Trusted Platform Module）

5. 概述

5.1 安全威胁

5.1.1 针对密码系统的安全威胁

5.1.1.1 密钥攻击

攻击者可能突破操作系统访问控制措施，获取密钥、密钥材料，以及与密钥相关的中间计算结果，或者利用密钥生成、建立、存储、使用、销毁等缺陷恢复或部分恢复密钥，从而破解密码系统。

5.1.1.2 密码组件攻击

攻击者可能通过对操作系统的本地攻击、物理攻击等手段，对软硬件密码组件进行控制、修改，或者绕过密码组件调用机制，导致密码系统保护功能失效。

5.1.1.3 证书攻击

攻击者可能通过欺骗、盗窃、篡改等手段攻击操作系统数字证书的存储、管理和使用，从而影响操作系统使用者身份的可信度、数据的可信度及关键数据的完整性、机密性。

5.1.2 针对操作系统的安全威胁

5.1.2.1 网络攻击

攻击者在远程通过网络通道对操作系统进行攻击窃取系统信息、改变主机状态、修改程序代码、监视网络通信数据。

5.1.2.2 本地攻击

攻击者可通过篡改操作系统上运行的应用程序或利用软件供应链方式使得计算机安装恶意程序对主机实施攻击，从而窃取操作系统数据、瘫痪主机软硬件系统等。

5.1.2.3 物理攻击

攻击者可能在有限的时间内直接接触计算机硬件设备（如磁盘、内存、CPU等），从而尝试访问其中的操作系统数据。

5.2 安全目的

5.2.1 概述

为防止5.1所述安全威胁，建立操作系统商用密码子系统（简称商密子系统），实现保护OS密码算法及密钥安全、保护OS通信安全、保护OS存储安全、保护OS软件安全等目的。

5.2.2 算法及密钥安全

为防止5.1.1.1密钥攻击、5.1.1.2密码组件以及5.1.1.3证书攻击安全威胁，确保操作系统使用的密码算法符合商用密码法规要求，确保密钥、证书正确使用及安全，操作系统商用密码子系统提供商用密码算法、独立的密码资源、规范的数据加解密应用及商用密码子系统管理及安全保护功能。

5.2.3 通信安全

为防止5.1.2.1网络攻击威胁，商密子系统提供操作系统远程通信加密功能，为操作系统与远程用户建立可信信道。

5.2.4 存储安全

为防止5.1.2.3物理攻击威胁，确保在操作系统存储介质失控情况下存储数据的安全，商密子系统提供静态数据加密保护功能。

5.2.5 软件安全

为防止5.1.1.2密码组件攻击及5.1.2.2本地攻击威胁，商密子系统为操作系统提供用户身份鉴别、软件签名/验证机制，确保操作系统及商密子系统软件完整性、责任可追溯性，降低软件供应链安全威胁。

5.3 商密子系统边界

商密子系统是在通用操作系统（简称操作系统或OS，包括服务器操作系统、桌面终端操作系统和移动智能终端操作系统）上运行的软硬件组件的集合，主要承担需要由操作系统执行的内核态和用户态商用密码操作（简称商密应用），同时也可为应用软件提供商密功能调用。商密应用通过内核态和用户态OS商密API进行商密功能调用。

商密子系统赖以运行的操作系统是商密子系统的宿主操作系统。商密子系统与宿主操作系统其他部分之间的边界逻辑上可视为一种密码模块边界。图1中虚线框表示OS商密子系统边界。

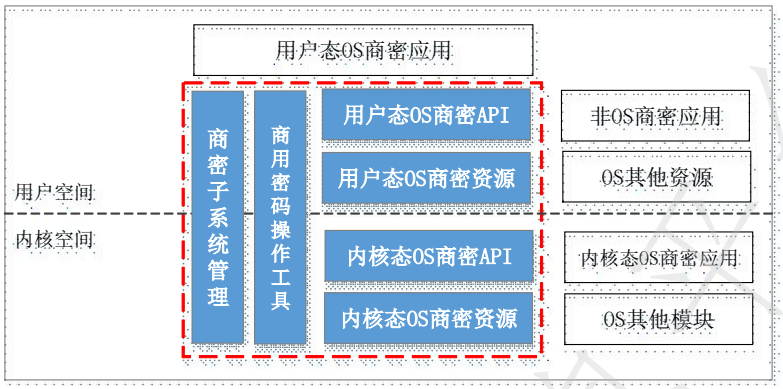

图1 OS商密子系统边界

OS商密子系统一般包括内核态和用户态OS商密资源、内核态和用户态OS商密API、商密子系统管理以及商用密码操作工具等组件。

内核态和用户态OS商密资源包括：软硬件密码模块（如密码算法库、密码机、智能密码钥匙、TPM/TCM、CPU等）及其驱动程序、中间件等。OS商密资源为OS（或应用软件）提供密码学基本功能，如数据加/解密、数据签名/验证、数据杂凑、密钥生成、密码协议等。

注：内核态和用户态使用的密码资源可以是同一密码资源，也可以是不同的密码资源。

内核态和用户态OS商密API：分别为内核态、用户态OS商密应用提供商用密码调用标准化接口以及商密资源挂接接口。

商密子系统管理：完成OS商密子系统数据、密码资源管理及系统配置等功能。

商用密码操作工具：包括密码操作命令行、工具包等。

5.4 假定

宿主操作系统应保证商密子系统有效运行和安全，并提供必要的安全支持。本文件假定宿主操作系统具有：

——访问控制、用户账户保护、软件运行安全保护等基本安全措施，保证商密子系统管理员具有独立使用和管理商密子系统的能力。

——安全隔离保护机制，保证商密子系统具有相对隔离的运行环境。

5.5 文件约定

本文件的每一个要求采用“**【要求xx-yy】**”格式编号，xx表示本要求所在的章节号，yy表示本要求在xx章节中的序号。

附录A给出每个要求的“**说明**”及“**评估**”。“**说明**”是对满足本要求的含义、条件和实施方法的展开和补充。因此**“说明”**是“【要求**xx-yy**】”的组成部分。如一个要求不需要说明，可没有“说明”项。“**评估**”给出本要求的评估检测事项及方法。

6. 安全功能要求

6.1 密码资源

【要求6.1-01】商密子系统应包含独立的软/硬件商密资源。

【要求6.1-02】商密子系统使用的所有商密资源应经商用密码认证机构认证。

【要求6.1-03】商密子系统应具有适配密码资源标准化机制。

6.2 密码算法

6.2.1 加密算法

【要求6.2-01】商密子系统应按照指定（核准）的商密算法提供数据加密/解密功能，指定（核准）的算法至少包括SM4算法（GB/T 32907）和祖冲之序列密码算法（GB/T 33133）之一。

【要求6.2-02】商密子系统应提供SM2公钥加密算法功能，并满足GB/T 32918.4 SM2椭圆曲线公钥密码算法 公钥加密算法的规范要求。

6.2.2 数字签名算法

【要求6.2-03】商密子系统应按照指定（核准）的商密算法执行数字签名/验证操作，数字签名算法至少是SM2算法（GB/T 32918.2）和SM9算法（GM/T 0044）之一。

6.2.3 杂凑算法

【要求6.2-04】商密子系统应按照SM3算法（GB/T 32905）提供消息摘要功能。

6.2.4 带密钥的杂凑算法

【要求6.2-05】商密子系统应采用基于SM3杂凑算法的HMAC算法。

6.2.5 随机数生成

【要求6.2-06】商密子系统应提供随机数生成功能。生成的随机数应符合GM/T 0062-2018检测要求。

6.3 密码管理

6.3.1 密钥管理

操作系统商密子系统使用的密钥数据包括但不限于：对称算法密钥、非对称算法密钥、随机数生成器生成数据、密钥生成的中间数据；按密钥用途可分为根密钥（RK）、数据加密密钥（DEK）、密钥加密密钥（KEK）等。这些密钥用于操作系统静态数据加密、通信加密、软件签名/验证、身份验证等过程。

【要求6.3-01】密钥生成。商密子系统应具有密钥生成功能，并符合GB/T 37092-2018敏感安全参数管理条款要求。

【要求6.3-02】 密钥建立。商密子系统应具有密钥建立功能，并符合SM2密钥交换协议（GB/T 32918.3）或SM9密钥交换协议（GM/T 0044.3）规范。

【要求6.3-03】密钥保护——密钥链。商密子系统应建立密钥链机制保护数据加密密钥。

【要求6.3-04】密钥保护——密钥存储。商密子系统应对密钥链实施存储保护。

【要求6.3-05】密钥销毁。当商密子系统密钥数据需要销毁时应按照以下方法实施销毁：

——对于易失性存储器，使用以下方式之一对密钥数据存储器进行擦除：

a) 撤掉电源；

b) 用系统提供的随机数生成器生成的伪随机数或单值0（或1）刷新存储器。

——对于非易失性存储器，调用底层平台接口用系统提供的随机数生成器生成的伪随机数或单值0（或1）刷新非易失性存储器。

6.3.2 证书管理

【要求6.3-06】商密子系统应具有宿主操作系统数字证书管理功能。

6.4 密码服务

6.4.1 密码接口

【要求6.4-01】商密子系统应具有以下密码接口方式：

——内核态、用户态OS商密API。用于内核及用户态商密应用操作调用。

——内核态、用户态OS商密资源挂接接口。用于商密子系统挂接内核态、用户态OS商密资源。

6.4.2 用户身份鉴别

【要求6.4-02】商密子系统应为宿主操作系统提供基于商密数字签名的OS用户身份鉴别机制。

6.4.3 存储数据加密

【要求6.4-03】商密子系统应为宿主操作系统提供用户文件/目录商密加密功能。

【要求6.4-04】商密子系统可为宿主操作系统提供磁盘加密功能。

【要求6.4-05】商密子系统应为宿主操作系统提供用户敏感信息加密保护功能。

6.4.4 通信数据保护

【要求6.4-06】商密子系统应为宿主操作系统内核网络安全通信协议提供商密数据保护功能。

6.4.5 应用软件包签名/验证

【要求6.4-07】商密子系统应为宿主操作系统提供应用软件包数字签名/验证机制。

6.4.6 内核代码签名/验证

【要求6.4-08】商密子系统应支持宿主操作系统驱动程序数字签名/验证功能。

【要求6.4-09】商密子系统应支持宿主操作系统内核程序完整性、数字签名/验证功能。

6.4.7 安全启动

【要求6.4-10】商密子系统应为宿主操作系统安全启动提供程序代码签名/验证密码支撑。

【要求6.4-11】商密子系统应为宿主操作系统启动阶段的可信计算提供密码支持。

6.4.8 自启动

【要求6.4-12】商密子系统应具备自启动功能。

6.4.9 软件/固件加载

【要求6.4-13】商密子系统宜具有加载外部软件/固件的能力。

6.4.10 安全操作系统密码功能支撑

商密子系统为GB/T 20272相关安全要求提供密码功能支撑。

6.5 商密子系统安全

6.5.1 管理员

【要求6.5-01】商密子系统应支持商密子系统主管角色设置，只有商密子系统主管能对商密子系统实施相关管理操作。

注：商密子系统主管简称商密主管。

6.5.2 系统管理

【要求6.5-02】商密主管应对商密子系统进行管理。

【要求6.5-03】商密子系统管理操作可通过命令行或管理面板方式实施。

6.5.3 身份鉴别

【要求6.5-04】商密子系统应具备鉴别机制以对商密主管进行身份鉴别，防止非商密主管对商密子系统进行控制。

6.5.4 数据保护

【要求6.5-05】商密子系统应对相关数据实施保护。

【要求6.5-06】商密子系统应支持访问控制功能，防止商密子系统相关数据被非法修改、读取。

【要求6.5-07】商密子系统应具备对其敏感数据实施加密保护功能。

6.5.5 系统隔离

【要求6.5-08】商密密码子系统相关资源应与非商密子系统实行隔离。

【要求6.5-09】商密子系统管理进程应与系统其他进程实行隔离，商密子系统管理进程优先权高于其他进程，应保证商密子系统管理进程与操作员交互数据安全。

6.5.6 可信信道

【要求6.5-10】商密子系统应使用网络安全通信协议与授权的实体之间建立可信信道，进行相关安全通信。

6.5.7 旁路

【要求6.5-11】如果商密子系统具有旁路功能，应设置该功能开启/关闭状态，并应由商密主管开启和关闭。

6.5.8 安全日志

【要求6.5-12】商密子系统应能够生成包括但不限于以下事件审计记录：

a） 商密主管身份鉴别（成功/失败）；

b） 敏感数据文件访问（创建、访问、删除、修改、修改权限的尝试成功和不成功）；

c） 审计和记录数据访问（成功/失败）；

d） 系统自检（成功/失败）；

e） 系统重新启动和关闭（成功/失败）；

f） 其他特别定义的可审计事件。

6.5.9 自检

【要求6.5-13】商密子系统应具备运行前自测试和条件自测试能力。

6.5.10 软件/固件安全

【要求6.5-14】商密子系统所有的软件和固件应经过安全检测。

6.5.11 可信更新

【要求6.5-16】如果商密子系统具有加载外部软件/固件的能力，加载时应对外部软件/固件进行签名验证。

6.5.12 有限状态模型FSM

【要求6.5-17】商密子系统应建立有限状态模型，并在不同状态下运行。

7. 安全保障要求

7.1 开发

7.1.1 功能规范文档

【要求7.1-01】商密子系统开发者应提供商密子系统功能规范文档。

7.2 指导性文档

7.2.1 用户操作指南

【要求7.2-01】商密子系统开发者应提供商密子系统用户操作指南文档。

7.2.2 准备程序

【要求 7.2-02】商密子系统开发者应提供商密子系统及评估准备程序。

7.3 生命周期支持

7.3.1 系统标签

【要求7.3-01】商密子系统应具有唯一性标签。

7.3.2 配置管理覆盖

【要求7.3-02】商密子系统开发者应提供系统配置列表。

7.3.3 及时安全更新

【要求7.3-03】商密子系统开发者应在功能规范文档中说明如何及时进行安全更新。

7.4 日常管理

7.4.1 管理制度

【要求7.4-01】使用商密子系统应建立执行以下管理制度：

——商密主管、操作员管理制度和操作规程；

——密钥（证书）管理；

——重要数据备份及应急处置；

——软硬件密码资源及介质管理等制度；

——商密子系统配置管理规定。

7.4.2 人员管理

【要求7.4-02】宿主操作系统使用商密子系统应符合以下人员管理要求：

——设置商密主管和操作员岗位；

——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；

——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；

——定期对相关人员进行考核。

7.4.3 应急处置

【要求7.4-03】宿主操作系统使用商密子系统应建立应急处置机制。

7.5 一致性测试

【要求7.5-01】对商密子系统进行一致性测试。

7.6 脆弱性评估

【要求 7.6-01】应对商密子系统进行脆弱性评估。

附 录 A
（规范性附录）
商密子系统要求条款说明及评估

A.1 安全功能要求

A.1.1 密码资源

【要求6.1-01】商码子系统应包含独立的软硬件商密资源。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1. 文档审查

审查评估文档，确认是否有关于密码子系统包含软硬件密码资源的描述。确认密码资源的架构、数据流向和接口定义等。

2. 功能测试：

验证在多样化的硬件和软件环境中部署密码子系统，其功能的正确性和性能的稳定性。

模拟系统升级和环境变化，测试密码子系统的自适应能力和对配置更改的响应。

【要求6.1-02】商密子系统使用的所有商密资源应经商用密码认证机构认证。

说明：

为实现5.2.2安全目的提出本要求。

评估：

检查评估文档，确认商密子系统使用的密码模块经商用密码认证机构认证。

【要求6.1-03】商密子系统应具有适配密码资源标准化机制。

说明：

为实现5.2.2安全目的提出本要求。

为有效挂接多厂家、多形态的密码资源，应建立适应操作系统环境的密码资源连接机制。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统标准化适配密码资源机制的描述。

2. 功能测试

确认商密子系统是否具有密码资源连接机制，用于标准化适配多厂家、多形态的密码资源。

测试密码资源连接机制的适配性，尝试连接不同厂家、不同形态的密码资源，并验证其连接稳定性和可靠性。

检查密码资源连接机制是否遵循标准化接口规范。

进行密码资源的功能测试，验证密码资源连接机制能够正确调用密码资源提供的功能，包括加密、解密、数字签名等操作。

测试密码资源连接机制的兼容性，验证其与不同厂家、不同形态的密码资源之间的兼容性。确保密码资源连接机制能够适配各种类型的密码资源。

A.1.2 密码算法

A.1.2.1 加密算法

【要求6.2-01】商密子系统应按照指定（核准）的商密算法提供数据加密/解密功能，指定（核准）的算法至少包括SM4算法（GB/T 32907）和祖冲之序列密码算法（GB/T 33133）之一。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1. 文档审查

检查评估文档，确认是否有商密子系统支持SM4、祖冲之序列密码算法的说明。

查看商密子系统配置文件，确认是否有相关配置项允许或强制使用这些算法。

2. 功能测试

SM4算法测试：

使用SM4算法对一组数据进行加密，然后解密，验证加密前后数据的一致性。

使用标准测试实例（如GB/T 32907附录或GB/T 17964-2021附录中提供的示例）进行测试，确保算法实现正确。

祖冲之序列密码算法测试：

使用祖冲之序列密码算法对一组数据进行加密，然后解密，验证加密前后数据的一致性。

使用标准测试实例（如GB/T 33133.1附录C中提供的计算实例）进行测试，确保算法实现正确。

3. 第三方认证

确认商密子系统SM4算法和祖冲之序列密码算法是否由经商用密码认证机构认证的密码模块提供。

【要求6.2-02】商密子系统应提供SM2公钥加密算法功能，并满足GB/T 32918.4 SM2椭圆曲线公钥密码算法 公钥加密算法的规范要求。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1.文档审查

审查评估文档，确认是否有关于商密子系统提供SM2公钥加密算法功能的说明。

2.功能测试

使用操作系统提供的API或工具执行SM2公钥加密算法的数据，检验过程是否符合GB/T 32918.4。

3.第三方认证

确认商密子系统SM2公钥加密算法是否由经过检测认证的商用密码模块提供。

A.1.2.2 数字签名算法

【要求6.2-03】商密子系统应按照指定（核准）的商密算法执行数字签名/验证操作，数字签名算法至少是SM2算法（GB/T 32918.2）和SM9算法（GM/T 0044）之一。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1. 文档审查

查看评估文档，确认商密子系统是否有关于商密子系统支持 SM2 或 SM9 数字签名算法的说明。

2. 功能测试

——SM2 算法测试

密钥生成：

使用商密子系统的 API 或工具本地生成 SM2 数字签名算法的公钥和私钥对。

验证生成的密钥对是否符合 SM2 算法标准 GB/T 32918.2。

签名操作：

使用生成的私钥对一组已知数据进行数字签名。

签名验证：

使用生成的公钥对签名结果进行验证。确认验证结果是否正确，即签名是否被成功验证。

——SM9 算法测试

密钥生成：

使用商密子系统的 API 或工具本地生成 SM9 算法的签名主私钥、主公钥，使用指定用户 ID，生成用户签名私钥。

验证生成的主私钥、主公钥及用户签名私钥是否符合 SM9 算法标准 GM/T 0044.2。

签名操作：

使用生成的指定用户 ID 所对应的用户签名私钥对一组已知数据进行数字签名。

签名验证：

使用生成的签名主公钥及指定用户 ID 对签名结果应用 SM9 算法进行验证。确认验证结果是否正确。

3. 符合性检测

确认操作系统SM2和MS9算法是否由经商用密码认证机构认证的密码模块提供。

A.1.2.3 杂凑算法

【要求6.2-04】商密子系统应按照SM3算法（GB/T 32905）提供消息摘要功能。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1. 文档审查

审查评估文档，确认是否有商密子系统提供SM3算法消息摘要功能的说明。

2. 功能检测

使用操作系统提供的API或工具执行SM3算法计算消息摘要，检测计算过程是否符合SM3算法标准GB/T 32905。

3. 第三方认证

确认商密子系统SM3算法是否由经过检测认证的商用密码模块提供。

A.1.2.4 带密钥的杂凑算法

【要求6.2-05】商密子系统应采用基于SM3杂凑算法的HMAC算法。

说明：

为实现5.2.2安全目的提出本要求。

HMAC是基于密钥杂凑算法生成的消息认证码（MAC）。在HTTPS、TLS、SSH、IPSec等协议中HMAC用于数字签名、消息认证码生成、安全密钥交换等。

评估：

1.文档审查

审查评估文档，确认是否有商密子系统采用SM4算法计算HMAC的说明。

2.功能检测

检测商密子系统HMAC生成算法是否基于SM3算法，检测计算过程是否符合HAMC-SM3算法标准GM/T 0091-2020。

A.1.2.5 随机数生成

【要求6.2-06】商密子系统应提供随机数生成功能。生成的随机数是否符合GM/T 0062-2018检测要求。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统提供的随机数生成功能的说明。

2.功能检测

使用操作系统提供的API或工具执行生成随机数，使用随机数检测工具所生成的随机数是否符合GM/T 0062-2018检测要求。

A.1.3 密码管理

A.1.3.1 密钥管理

【要求6.3-01】密钥生成——商密子系统应具有密钥生成功能，并符合GB/T 37092-2018敏感安全参数管理条款要求。

说明：

为实现5.2.2安全目的提出本要求。

评估：

审查相关文档，查看是否有关于商密子系统具有密钥生成功能的说明。确认密钥生成是否符合GB/T 37092-2018敏感安全参数管理条款要求。

【要求6.3-02】密钥建立。商密子系统应具有密钥建立功能，并符合SM2密钥交换协议（GB/T 32918.3）或SM9密钥交换协议（GM/T 0044.3）规范。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统密钥建立功能的说明。

2.功能检测

按照GB/T 32918.3附录A验证示例验证商密子系统密钥建立符合SM2密钥交换协议。

按照GM/T 0044.3验证商密子系统密钥建立符合SM9密钥交换协议。

【要求6.3-03】密钥保护——密钥链。商密子系统应建立密钥链机制保护数据加密密钥。

说明：

为实现5.2.2安全目的提出本要求。

密钥链机制：

——数据加密密钥（DEK）对系统静态数据进行加密；

——密钥加密密钥（KEK）对DEK进行加密保护；

——宿主操作系统根密钥（RK）与用户口令（或个人生物信息）联合派生KEK。

DEK生成满足【要求6.3-01】，KEK派生符合GM/T 0091规范，RK由随机数生成器产生。

KEK对DEK加密应采用【要求6.2-01】要求的算法，由商密子系统密码资源库（或密码模块）执行。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统应建立密钥链机制保护数据加密密钥的说明。

2.功能检测

——RK检测

检查RK生成的规范和算法是否符合GM/T 0091标准。

——KEK检测

检测KEK是否由商密主管口令（或个人生物信息）派生，或与RK组合派生，且生成过程符合GM/T 0091规范。

确认KEK的加密保护是否采用【要求6.2-01】要求的算法，且加密过程在商密子系统密码资源库（或密码模块）中进行。

通过审计和模拟访问控制测试，确认KEK的存储安全性和访问控制的有效性。

——DEK检测

检测DEK生成是否满足【要求6.3-01】。

检测DEK是否由KEK加密保护，且加密算法符合商密子系统要求。

通过审计和模拟操作，检查DEK的使用和管理是否遵循安全策略，包括生命周期管理、更新和撤销等。

【要求6.3-04】密钥保护——密钥存储。商密子系统应对密钥链实施存储保护。

说明：

为实现5.2.2安全目的提出本要求。

RK宜存储在受保护的硬件中，运行时与操作系统其他任务隔离，只能被商密子系统进程读取。KEK存储在用户证书存储库中，DEK用KEK加密后存储在用户应用系统选择的位置。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统对静态数据加密密钥实施存储保护的说明。

2.功能检测

检查RK是否存储在受保护的硬件介质中，如USB设备、硬件安全模块（HSM）或TPM等。

模拟访问控制测试，确认只有商密子系统进程能够访问RK。

检测KEK（密钥加密密钥）是否存储在证书存储库中，该存储库应具备访问控制和加密保护。

检查DEK（数据加密密钥）是否使用KEK加密后存储。

验证只有授权的用户或服务能够访问主密钥RK和密钥加密密钥KEK。这包括对存储位置的物理访问控制和对证书存储库的访问控制。

审计和日志：检查是否有详细的访问日志和审计记录，用于追踪密钥的访问和使用情况。

【要求6.3-05】密钥销毁。当商密子系统密钥数据需要销毁时应按照以下方法实施销毁：

——对于易失性存储器，使用以下方式之一对密钥数据存储器进行擦除：撤掉电源、用系统提供的随机数生成器生成的伪随机数或单值0（或1）刷新存储器。

——对于非易失性存储器，调用底层平台接口用系统提供的随机数生成器生成的伪随机数或单值0（或1）刷新非易失性存储器。

说明：

为实现5.2.2安全目的提出本要求。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统密钥数据销毁方法的说明。

2.功能检测

验证是否可以通过撤掉电源的方式擦除易失性存储器中的密钥数据。

使用系统提供的随机数生成器生成的伪随机数或单值 0（或 1）测试是否有效擦除存储器中的密钥数据。

验证是否可以调用底层平台接口使用伪随机数或单值 0（或 1）刷新非易失性存储器。

在销毁操作完成后，进行存储器数据恢复尝试，验证密钥数据是否已被完全销毁。

A.1.3.2 证书管理

【要求6.3-06】商密子系统应具有宿主操作系统数字证书管理功能。

说明：

为实现5.2.2安全目的提出本要求。

宿主操作系统证书分内核证书和应用证书。内核证书用于内核模块（包括安全启动）的数字签名/验证，应用证书用于应用软件的数字签名/验证。内核证书由商密主管管理，应用证书可由其他用户管理。

商密子系统提供的操作系统数字证书管理包括但不限于以下功能：

a) 生成SM2算法公私钥，生成自签名证书、签署证书申请、创建证书链、证书导入、导出、验证等，证书申请符合GM/T 0092规范要求，证书格式应符合GB/T 20518规范的要求；
b) 管理引导加载器、驱动程序、内核程序、应用软件包签名证书；
c) 管理可信权威机构；
d) 通过证书策略设置定义信任根证书、撤销列表检查、证书链验证等规则；
e) 建立证书存储库集中存放宿主操作系统证书，可使用硬件存储区存放私钥。

评估：

1.文档审查

审查评估文档，确认是否有关于商密子系统具有宿主操作系统数字证书管理功能的描述。

2. 功能测试

验证用户能否成功生成 SM2算法（或SM9算法）公私钥，并生成自签名证书。

测试用户是否能成功签署证书申请。

验证用户是否能够创建证书链。

测试证书的导入、导出功能，并验证导入的证书是否有效。

验证证书申请是否符合GM/T 0092规范要求。

检查证书格式是否符合 GB/T 20518 规范要求。

检查用户是否能够管理启动垫片、驱动程序、引导加载器、内核程序、应用软件包签名证书。

测试用户是否能够管理可信权威机构。

检查用户是否能够通过证书策略设置来定义信任根证书、撤销列表检查、证书链验证规则。

验证是否集中存放宿主操作系统证书。

检查是否设立硬件存储区存放私钥，如USB设备、硬件安全模块（HSM）或TPM等。

A.1.4 密码服务

A.1.4.1 密码接口

【要求6.4-01】商密子系统应具有以下密码接口方式：

——内核态、用户态OS商密API。用于内核及用户态商密应用操作调用。

——内核态、用户态OS商密资源挂接接口。用于商密子系统挂接内核态、用户态OS商密资源。

说明：

为实现5.2.2安全目的提出本要求。

商密子系统内核态、用户态OS商密API，以及内核态、用户态OS商密资源挂接接口应为标准化接口，内核态标准接口应兼容操作系统原生密码调用接口。

评估

1. 文档审查

审查评估文档，确认是否有关于商密子系统应具有内核态、用户态OS商密API，以及内核态、用户态OS商密资源挂接接口的描述。

2. 功能测试

测试是否可通过商密子系统内核态、用户态OS商密API标准接口进行内核态和用户态商密应用操作调用。验证接口是否符合相关标准。

测试是否可通过商密子系统内核态、用户态OS商密资源挂接标准接口挂接、调用OS商密资源。验证接口的兼容性，以确保能够与不同类型的OS商密资源实现无缝连接。

检查内核态OS商密API标准接口和OS商密资源挂接接口是否兼容操作系统原生密码调用接口。

A.1.4.2 用户身份鉴别

【要求6.4-02】商密子系统应为宿主操作系统提供基于商密数字签名的OS用户身份鉴别机制。

说明：

为实现5.2.4及5.2.5安全目的提出本要求。

数字签名鉴别机制符合GB/T 15843.3。数字签名鉴别应使用【要求6.2-03】提供的密码算法（SM2算法或SM9算法）。

如果采用SM2算法，用户证书应由宿主操作系统运行组织负责颁发，颁发证书的CA可以是宿主操作系统运行组织自建并维护的CA，也可以是宿主操作系统组织机构指定的第三方CA，证书格式符合GB/T 20518规范。证书验证时应对证书链进行验证，确保证书链的所有证书都是受信任CA颁发的证书。自行建设并维护的CA，应确保根私钥的安全。

如采用SM9算法，用户签名私钥由宿主操作系统运行组织建立的密钥管理系统（KMS）分发。

当宿主操作系统用户采用SSH协议远程登录系统时，商密子系统为SSH提供数字签名身份鉴别机制。

数字签名身份鉴别机制一般使用外部智能卡、USB智能密码钥匙等硬件介质存放用户鉴别密钥（证书）。

商密子系统使用【要求6.3-06】提供的方法对用户证书进行管理。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统为宿主操作系统提供基于数字签名的用户身份鉴别机制的描述。

2. 功能测试

确认商密子系统提供的数字签名用户身份鉴别机制是否符合GB/T 15843.3标准的要求。

确认数字签名算法是否采用商密子系统提供的密码算法（SM2算法、SM9算法）进行用户身份鉴别。

检查证书格式是否符合GB/T 20518规范，包括证书的结构、字段和内容。

确认系统在证书验证时是否对证书链进行验证，以确保证书链中的所有证书都是受信任的CA证书。

测试证书链验证功能，确保系统能够正确处理和验证证书链中的所有证书。

确认如果采用SM9算法，用户签名私钥是否由宿主操作系统运行组织建立的密钥管理系统（KMS）进行分发。

确认商密子系统使用【要求6.3-06】提供的方法对用户证书进行管理。

A.1.4.3 存储数据加密

【要求6.4-03】商密子系统应为宿主操作系统提供用户文件/目录商密加密功能。

说明：

为实现5.2.4安全目的提出本要求。

文件/目录商密加密机制应采用【要求6.2-01】提供的算法。

加密的文件/目录可以单个文件或文件集（或卷、容器等），只有在用户身份验证后才允许访问加密的文件/目录。

使用数据加密密钥（DEK）对文件进行加密。DEK密钥由【要求6.3-01】提供的方法产生，每个文件（或一组文件）使用唯一的DEK。

相关密钥保护和销毁应按照【要求6.3-03】、【要求6.3-04】和【要求6.3-05】方法执行。

在解密/加密操作完成后，解密/加密时创建的所有原始明文数据在易失性和非易失性存储器中应被删除。

文件/目录加密用户身份鉴别可采用【要求6.3-01】提供的方法实施。

不在非易失性存储器中存储明文密钥。

商密子系统应至少能够执行以下文件加密管理功能：配置加密功能、更改身份验证因素、对数据进行加密擦除、配置所需的失败验证尝试次数等管理。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统应为宿主操作系统提供文件/目录加密机制的说明。

2. 功能测试

确认商密子系统能够提供文件/目录加密机制，包括单个文件或文件集的加密，以及只有在用户身份验证后才允许访问加密文件/目录。

检验文件/目录商密加密机制是否采用【要求6.2-01】提供的算法。

验证DEK密钥由【要求6.3-01】方法产生，对每个文件（或一组文件）使用唯一的DEK。

验证密钥保护和销毁是否按照【要求6.3-03】、【要求6.3-04】和【要求6.3-05】方法执行。

确认在解密/加密操作完成后，解密/加密时创建的所有原始明文数据在易失性和非易失性存储器中被销毁。

确认文件/目录加密用户身份鉴别采用【要求6.4-02】方法实施。

验证不在非易失性存储器中存储明文密钥，以防止未经授权的访问。

确认商密子系统能够执行所需的管理功能，包括配置加密功能、更改身份验证因素、对数据进行加密擦除、配置失败验证尝试次数等。

【要求6.4-04】商密子系统可为宿主操作系统提供磁盘加密功能。

说明：

为实现5.2.4安全目的提出本要求。

商密子系统在操作系统内核启动后，加载用户空间的应用程序或服务前对用户需要保护的磁盘空间进行加密设置。操作系统完全启动后商密子系统磁盘加密机制对指定的磁盘数据（不包括系统主引导记录）进行无需用户干预的加解密操作（写入加密，读出解密），只有授权用户才允许访问磁盘数据。

一个磁盘使用唯一一个DEK加解密，每次加解密使用不同的DEK。DEK由【要求6.3-01】提供的方法产生。

相关密钥保护和销毁应按照【要求6.3-03】、【要求6.3-04】和【要求6.3-05】方法执行。

商密子系统除执行磁盘加解密操作，还承担密钥生成、更新、归档、恢复、保护，以及销毁等管理功能。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统为宿主操作系统提供磁盘加密机制的说明。

2. 功能测试

验证商密子系统能够在操作系统内核启动后正确加载，并在用户空间的应用程序或服务启动前对指定的磁盘空间进行加密设置。

检查加解密操作，确认商密子系统在操作系统完全启动后对指定磁盘数据执行无需用户干预的加解密操作，验证写入数据时的加密和读取数据时的解密操作是否正常进行。

尝试从加密的磁盘中恢复数据，评估加密的效果。

验证访问控制机制，确认只有授权用户可以访问经商密子系统加密的磁盘数据。

检查商密子系统是否为一个磁盘使用唯一的DEK进行加解密操作。

验证DEK的生成是否符合【要求6.3-01】中提供的方法。

验证密钥销毁是否按照【要求6.3-03】、【要求6.3-04】和【要求6.3-05】方法执行。

确认商密子系统能够执行磁盘相关密钥生成、更新、归档、恢复、保护和销毁等管理功能。

【要求6.4-05】商密子系统应为宿主操作系统提供用户敏感信息加密保护功能。

说明：

为实现5.2.4安全目的提出本要求。

宿主操作系统敏感信息至少包括：

——用户账户信息，包括用户名、用户口令、用户生物信息等；

——SSH密钥，包括公私钥对；

——访问控制信息，包括用户或组对文件或目录的访问权限、ACL（访问控制列表）等；

——应用程序凭据，包括API密钥（应用程序访问第三方服务的唯一标识符）、令牌（用于身份验证和授权的短时有效字符串）等；

——用户申请保护的其他文件。

使用数据加密密钥（DEK）对用户敏感数据进行加密，DEK密钥由【要求6.3-01】提供的方法产生，每一组数据使用唯一的DEK。

相关密钥保护和销毁应按照【要求6.3-03】、【要求6.3-04】和【要求6.3-05】方法执行。

在解密/加密操作完成后，解密/加密时创建的所有原始明文数据在易失性和非易失性存储器中应被删除。

如果用户敏感信息以文件的形式存放，则使用【要求6.4-03】方法实施加密。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统为宿主操作系统提供用户敏感信息加密保护功能的说明。

2. 功能测试

确认商密子系统能够提供用户敏感信息加密机制，只有合法用户才能解密数据。

检验数据加密机制是否采用【要求6.2-01】提供的算法。

验证DEK密钥由【要求6.3-01】方法产生，对每一组数据使用唯一的DEK进行加密。

验证密钥保护和销毁是否按照【要求6.3-03】、【要求6.3-04】和【要求6.3-05】方法执行。

确认在解密/加密操作完成后，解密/加密时创建的所有原始明文数据在易失性和非易失性存储器中被销毁。

验证不在非易失性存储器中存储明文密钥，以防止未经授权的访问。

A.1.4.4 通信数据保护

【要求6.4-06】商密子系统应为宿主操作系统网络安全通信协议提供商密数据保护功能。

说明：

本要求为实现 5.2.3 安全目的而提出。

宿主操作系统网络安全通信数据协议包括但不限于：

——SSH，用于操作系统安全远程登录访问。应符合GM/T 0129。

——KTLS，主要用于客户端和服务器之间的安全通信，如浏览器通信协议HTTPS。应符合GB/T 38636。

网络安全通信协议数据加密应采用【要求6.2-01】提供的算法。

网络安全通信协议的密钥的生成、建立、保护、销毁及证书管理应符合【要求6.3-01】、【要求6.3-02】、【要求6.3-03】、【要求6.3-04】、【要求6.3-05】及【要求6.3-06】。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统为宿主操作系统内核网络安全通信协议提供商密数据加密功能的说明。

2. 功能测试

使用网络抓包工具捕获数据包，验证商密子系统是否支持操作系统内核网络安全通信协议，如SSH和KTLS。

检测网络安全通信协议数据加密是否采用【要求6.2-01】提供的算法。

测试网络安全通信协议在传输过程中实现适当的密钥交换和加密保护。

验证商密子系统支持的协议（如SSH和KTLS）是否符合GM/T 0129和GB/T 38636。

检测网络安全通信协议的密钥的生成、建立、保护、销毁及证书管理是否符合【要求6.3-01】、【要求6.3-02】、【要求6.3-03】、【要求6.3-04】、【要求6.3-05】及【要求6.3-06】。

审查商密子系统的安全配置，包括加密算法的选择、密钥管理、访问控制等，确保系统配置符合最佳安全实践。

A.1.4.5 应用软件包签名/验证

【要求6.4-07】商密子系统应为宿主操作系统提供应用软件包数字签名/验证机制。

说明：

本要求为实现5.2.5安全目的而提出。

应用软件包安装数字签名验证机制是保证软件供应链安全的重要方法，可防止应用软件被非法篡改，也提供了应用软件来源的可追溯性。

商密子系统对应用软件包数字签名/验证应使用【要求6.2-03】提供的密码算法（SM2算法或SM9算法）。

应用软件包数字签名应遵循软件代码签名相关标准，保证应用软件签名的兼容性、互操作性。

宿主操作系统安装应用软件时商密子系统使用可信权威机构分发的公钥（证书）对软件包进行数字签名验证，并根据签名验证结果决定是否安装该应用软件。

一个应用软件包可由多个软件责任主体进行签名，软件责任主体包括软件开发者、发行者、检测机构等。签名主体公私钥（证书）应由可信权威机构分发，实施实名签名，确保软件责任可追溯。各签名主体的公私钥（证书）可由不同可信权威机构分发。

商密子系统可对一个应用软件包实施不同软件责任主体签名/验证。

应用软件安装签名验证时商密子系统应验证可信权威机构分发的公钥（证书）是否有效，确保公钥（证书）是指定的可信权威机构分发，在有效期内且未被吊销。

可信权威机构分发应用软件所有签名者公私钥（证书）应由操作系统厂商授权分发。可信权威机构可以是不同的组织，也可以是同一个组织。为降低宿主操作系统公私钥（证书）管理复杂度，可授权一个（或几个）可信权威机构负责分发软件各责任主体的签名公私钥（证书）。

商密子系统应为应用软件包数字签名提供工具。如签名密钥生成、软件包签名、签名密钥（证书）请求及管理等。

商密子系统使用【要求6.3-06】提供的方法对应用软件包签名证书进行管理。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统为宿主操作系统提供应用软件包数字签名/验证机制的说明。

2. 功能检测

确认商密子系统提供的应用软件包数字签名/验证机制是否使用【要求 6.2-03】提供的密码算法（SM2 算法或SM9 算法）。

审核应用软件包数字签名是否遵循软件代码签名相关标准。

验证应用软件签名者的公私钥（证书）是否由可信权威机构分发，确保软件包签名实名化。

验证商密子系统对一个应用软件包实施不同软件责任主体签名/验证正确性。

确认商密子系统在应用软件安装签名验证时是否是可信权威机构分发的公钥（证书）的有效性。

对可信权威机构分发的证书链进行验证，验证应用软件数字签名公钥（证书）是否由授权的可信权威机构分发。

安装一个没有数字签名和一个有签名的应用软件，验证没有签名的软件安装失败，有签名的软件安装成功。

使用无效公钥（证书）和有效公钥（证书）分别对应用软件进行签名验证，验证无效公钥（证书）的应用软件安装失败，有效公钥（证书）的安装成功。

确认商密子系统使用【要求6.3-06】提供的方法对应用软件包签名证书进行管理。

A.1.4.6 内核代码签名/验证

【要求6.4-08】商密子系统应支持宿主操作系统驱动程序数字签名/验证功能。

说明：

本要求为实现5.2.5安全目的而提出。

驱动程序（内核模块）包括字符设备驱动程序和块设备驱动程序，如键盘、鼠标、硬盘驱动程序等。每个驱动程序须经数字签名。当OS安全启动时对内核驱动程序进行数字签名验证，验证不通过不能加载运行。某些驱动程序在OS安全启动前进行签名验证不在本文件要求范围。安全启动要求见**【要求6.4-10】。**

商密子系统对驱动程序数字签名/验证应使用【要求6.2-03】提供的密码算法（SM2算法或SM9算法）。

商密子系统应为操作系统驱动程序数字签名/验证提供工具。如签名密钥生成、代码包签名、签名密钥（证书）请求及管理等。

一个驱动程序可由多个责任主体进行签名，软件责任主体包括软件开发者、发行者、检测机构等。签名主体公私钥（证书）应由可信权威机构分发。各签名主体的公私钥（证书）可由不同可信权威机构分发。

驱动程序由宿主操作系统加载运行时，商密子系统使用可信权威机构分发的公钥（证书）进行数字签名验证，签名验证不通过不能加载运行。

分发驱动程序所有签名者公私钥（证书）的可信权威机构应由操作系统厂商授权。可信权威机构可以是同一个组织，也可以是不同的组织。为提高驱动程序的兼容性、互操作性、安全检测标准的一致性

以及签名公私钥（证书）的管理效率，操作系统厂商可授权一个可信权威机构分发开发者、发行者、检测机构的签名公私钥（证书）。

商密子系统使用【要求6.3-06】提供的方法对内核代码签名证书进行管理。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统应支持宿主操作系统驱动程序商密数字签名/验证功能的说明。

2.功能检测

确认商密子系统提供的驱动程序数字签名/验证机制是否使用【要求 6.2-03】提供的SM2 算法或SM9算法。

确认驱动程序签名者的公私钥（证书）是否由可信权威机构分发。

测试数字签名验证功能，确保系统能够正确验证驱动程序的签名，并根据验证结果决定是否允许代码执行。

确认商密子系统在驱动程序加载签名验证时是否是可信权威机构分发的公钥（证书）的有效性。

对可信权威机构分发的证书链进行验证，验证驱动程序数字签名公钥（证书）是否由授权的可信权威机构分发。

安装一个没有数字签名和一个有签名的驱动程序，验证没有签名的内核代码加载失败，有签名的内核代码加载成功。

使用无效公钥（证书）和有效公钥（证书）分别对驱动程序进行签名验证，验证无效公钥（证书）的驱动程序加载失败，有效公钥（证书）的加载成功。

确认商密子系统使用【要求6.3-06】提供的方法对驱动程序签名证书进行管理。

【要求6.4-09】商密子系统应支持宿主操作系统内核程序完整性、数字签名/验证功能。

说明：

本要求为实现5.2.5安全目的而提出。

内核程序是非驱动程序的内核代码，当内核程序加载时操作系统对其进行杂凑值或数字签名进行验证，并根据安全策略决定是否运行。

商密子系统内核程序杂凑计算应使用【要求6.2-04】提供的算法（SM3算法），数字签名/验证应使用【要求6.2-03】提供的密码算法（SM2算法或SM9算法）。

商密子系统应为操作系统内核程序杂凑计算、数字签名提供工具。如杂凑值生成、签名密钥生成、代码包签名、签名密钥（证书）请求及管理等。

一个内核程序可由多个责任主体进行签名，软件责任主体包括软件开发者、发行者、检测机构等。签名主体公私钥（证书）应由可信权威机构分发。各签名主体的公私钥（证书）可由不同可信权威机构分发。

内核程序加载时商密子系统使用可信权威机构分发的公钥（证书）进行数字签名验证，验证不通过不能加载运行。

内核程序签名验证时商密子系统应验证可信权威机构分发的公钥（证书）是否有效，确保公钥（证书）是指定的可信权威机构分发，并且没有作废。

分发内核程序所有签名者公私钥（证书）的可信权威机构应由操作系统厂商授权。可信权威机构可以是同一个组织，也可以是不同的组织。为提高内核代码的兼容性、互操作性、安全检测标准的一致性以及签名公私钥（证书）的管理效率，操作系统厂商可授权一个可信权威机构分发开发者、发行者、检测机构的签名公私钥（证书）。

商密子系统使用【要求6.3-06】提供的方法对内核程序签名证书进行管理。

评估：

1.文档审查

审查相关文档，查看是否有关于商密子系统应支持宿主操作系统内核程序完整性、数字签名/验证功能的说明。

2.功能检测

确认商密子系统提供的内核程序完整性验证是否使用【要求 6.2-04】提供的SM3 算法。

确认商密子系统提供的内核程序数字签名/验证是否使用【要求 6.2-03】提供的SM2 算法或SM9 算法。

确认内核程序签名者的公私钥（证书）是否由可信权威机构分发。

测试数字签名验证功能，确保系统能够正确验证内核程序的签名，根据验证结果决定是否允许代码执行。

确认商密子系统在内核程序加载签名验证时是否验证可信权威机构分发的公钥（证书）的有效性。

对可信权威机构分发的证书链进行验证，验证内核程序数字签名公钥（证书）是否由授权的可信权威机构分发。

安装一个没有数字签名和一个有签名的内核程序，验证没有签名的内核程序加载失败，有签名的内核程序加载成功。

使用无效公钥（证书）和有效公钥（证书）分别对内核程序件进行签名验证，验证无效公钥（证书）的内核程序加载失败，有效公钥（证书）的加载成功。

确认商密子系统使用【要求6.3-06】提供的方法对内核程序签名证书进行管理。

A.1.4.7 安全启动

【要求6.4-10】商密子系统应为宿主操作系统安全启动提供程序代码签名/验证密码支撑。

说明：

本要求为实现5.2.5安全目的而提出。

计算机安全启动机制大致分为两个阶段：硬件启动和操作系统启动。硬件启动阶段不属于本文件规范内容。

操作系统安全启动过程：

第一步，启动垫片验证操作系统引导加载器数字签名；

第二步，引导加载器验证操作系统内核代码数字签名；

第三步，操作系统内核运行。

对启动垫片和部分驱动程序（内核模块）签名验证由硬件启动过程负责。

注：有的驱动程序数字签名在引导加载器启动后验证。

商密子系统可使用硬件密码模块支撑宿主操作系统安全启动。

商密子系统为宿主操作系统安全启动提供密码支撑包括：

使用【要求6.2-03】提供的方法对引导加载器和驱动程序（内核模块）进行签名和验证。

使用【要求6.3-06】提供的方法对引导加载器和驱动程序（内核模块）签名证书进行管理。

商密子系统对引导加载器和驱动程序（内核模块）进行签名使用的公私钥（证书）由宿主操作系统厂商指定（授权）的可信权威机构签发，以保证操作系统底层资源及内核代码供应链安全责任可追溯。启动垫片和部分驱动程序（内核模块）的签名公钥（证书）存储在硬件启动资源中，用于硬件启动时验证启动垫片和部分驱动程序（内核模块）签名。引导加载器及部分驱动程序（内核模块）签名公钥（证书）存储在操作系统可控的资源中，用于操作系统启动时验证引导加载器及部分驱动程序（内核模块）的签名。

评估：

1. 文档审查

检查评估文档，查看是否有关于商密子系统为宿主操作系统安全启动提供密码支撑的说明。

2.功能测试

使用【要求6.2-03】提供的方法对引导加载器和驱动程序（内核模块）进行签名和验证。

使用【要求6.3-06】提供的方法对引导加载器和驱动程序（内核模块）签名证书进行管理。

进行启动流程的测试，包括签名验证、完整性验证等步骤的模拟和验证，确保商密子系统提供的密码支撑能够有效地保护系统安全启动。

【要求6.4-11】商密子系统应为宿主操作系统启动阶段的可信计算提供密码支持。

说明：

本要求为实现5.2.5安全目的而提出。

商密子系统只负责宿主操作系统引导加载器启动后的可信计算支撑。可信计算机制可调用商密子系统密码接口实现对OS启动时的可信计算功能。启动垫片及部分驱动程序（内核模块）可信计算验证由硬件启动过程负责。

注：宿主操作系统引导加载器启动后的可信计算机制参见GB/T 37935。

评估：

1. 文档审查

检查评估文档，查看是否有关于商密子系统应为宿主操作系统启动阶段的可信计算提供密码支撑的说明。

2.功能测试

检查商密子系统能否支持宿主操作系统启动阶段的可信计算。

使用【要求6.2-04】提供的方法，验证商密子系统是否对驱动程序（内核模块）进行杂凑值生成和验证。

A.1.4.8 自启动

【要求6.4-12】商密子系统应具备自启动功能。

说明：

本要求为实现5.2.2安全目的而提出。

商密子系统应无需操作员请求，其内核部分优先于宿主操作系统内核其他部分启动，以完成操作系统启动所需的密码操作，如内核代码完整性度量及签名验证等。

自启动密码服务能力由商密主管配置，该配置可以在商密子系统重置、重启之后保留下来。

评估：

1. 文档审查

检查评估文档，查看是否有关于商密子系统应具备自启动功能的说明。

2.功能测试

验证商密子系统能够优先于宿主操作系统内核其他部分启动，无需操作员干预或请求。

确保商密子系统能够生成启动日志并记录自启动过程中的关键事件和状态。

进行系统集成测试，验证商密子系统的自启动功能不会影响宿主操作系统的正常运行，完成所需要的密码操作，并且能够与其他系统组件良好协同工作。

测试自启动失败时的应急处理机制，确保商密子系统能够在自启动失败时进行适当的处理和恢复。

A.1.4.9 软件/固件加载

【要求6.4-13】商密子系统宜具有加载外部软件/固件的能力。

说明：

本要求为实现5.2.2安全目的而提出。

如果商密子系统具有加载外部软件或固件的能力，那么在软件/固件加载之前经过审验机构审验。加载时禁止密码应用操作，直到软件/固件加载完成。应修改商密子系统版本信息。

评估：

1. 文档审查

检查评估文档，查看是否有关于商密子系统可具有加载外部软件/固件的能力的说明。

2.功能测试

审验外部软件/固件，确保商密子系统具有加载外部软件或固件的能力之前，这些外部软件/固件必须经过审验机构的审验。

检测加载外部软件或固件之前，商密子系统应禁止密码应用操作。

监控加载外部软件/固件过程，确保加载过程中的操作符合规范并且没有异常行为。

检验在外部软件或固件加载完成后，商密子系统恢复密码应用操作。

检查在加载外部软件或固件后，是否修改商密子系统版本信息。

加载日志记录，记录加载外部软件或固件的过程和相关操作，生成加载日志以便日后审查和追踪。

A.1.4.10安全操作系统密码支撑

【要求6.4-14】商密子系统应为GB/T20272相关密码应用要求提供支撑。

说明：见附录B。

A.1.5 商密子系统安全

A.1.5.1 概述

【要求6.5-01】~【要求6.5-17】是为实现5.2.2安全目的而提出。

A.1.5.2 管理员

【要求6.5-01】商密子系统应支持商密子系统主管角色设置，只有商密子系统主管能对商密子系统实施相关管理操作。

注：商密子系统主管简称商密主管。

说明：

商密主管负责执行商密子系统相关管理，例如，商密子系统初始化、自测试、配置设置、敏感数据以及审计管理等。相关管理项目由【要求6.5-02】给出。商密主管可建立、授权系统操作员。

评估：

1.文档审查

审查相关文档，查看是否有关于商密主管角色的详细描述，包括角色定义、权限范围、操作流程等的说明。

2.功能测试

创建一个普通用户账号和一个商密主管账号。尝试使用普通用户账号访问商密子系统的管理功能，应被系统拒绝。使用商密主管账号进行管理操作，应能够成功执行。检查系统日志，确认只有商密主管账号的操作被记录。

尝试使用非商密主管账号进行管理操作，如创建、修改、删除商密数据等，确认系统是否拒绝这些操作，并给出相应的权限不足提示。使用商密主管账号进行上述操作，确认操作是否成功。

在系统中切换到非商密主管角色，尝试执行商密子系统的管理操作，确认系统是否拒绝操作，并给出权限不足的提示。使用商密主管账号执行一系列管理操作，查看系统日志，确认是否记录了这些操作的时间、操作类型、操作结果等信息。

模拟异常情况，如断电、网络中断等，在异常情况恢复后，检查商密子系统的状态，确认是否只有商密主管可以执行管理操作。

A.1.5.3 系统管理

【要求6.5-02】商密主管应对商密子系统进行管理。

说明：

商密主管至少对表1给出的项目进行管理。

表1 商密子系统管理项目

管理项目	说明
商密主管用户、操作员凭证管理	管理商密主管、操作员登录凭证，包括用户名、口令、密钥等。
商密主管、操作员鉴别设置	设定商密主管、操作员鉴别机制，如双因素认证、生物识别等。
商密子系统配置	设定商密子系统启动参数。
密钥管理	公私钥、数据加密密钥（DEK）、密钥加密密钥（KEK）导入、导出、更新、删除等。
证书管理	管理数字证书，包括证书的导入、导出和删除操作。
文件、磁盘加密设置	对商密子系统相关文件和磁盘进行加密设置。
通信加密设置	对商密子系统对外通信进行加密设置。
内核代码签名	对宿主操作系统内核代码进行签名。
内核代码杂凑值生成	对内核代码杂凑值生成以支撑可信计算。
敏感数据存储保护设置	对商密子系统敏感数据进行特殊保护进行设置，如存储位置、加密存储、访问控制等。
日志策略设置	设定对商密子系统审计策略，记录和监控系统的操作行为。
密码资源管理	安装、升级、测试密码资源库。
密码调用接口管理	管理密码调用接口，确保系统各部分在需要时能够正确、安全地调用密码资源。
启用/禁用外部接口	控制外部接口的启用和禁用，防止未授权访问和攻击。
其他必要的管理	包括但不限于系统备份与恢复、系统监控等，确保系统的整体安全和稳定运行。

评估：

表2给出【要求6.4-02】评估方法。

表2【要求6.4-02】评估方法

管理项目	评估检测方法

商密主管用户凭证管理	1.文档审查 审查评估文档，确认是否有关于商密主管用户凭证管理功能的描述。 2.功能测试 检查用户凭证的存储方式是否安全（如加密存储）。 验证用户凭证的复杂度和定期更新策略。 进行模拟攻击测试，检查凭证的安全性。
商密主管鉴别设置	1.文档审查 审查评估文档，确认是否有关于商密主管鉴别设置功能的描述。 2.功能测试 检查口令、生物、数字签名等鉴别机制的实施情况。 进行模拟登录测试，验证鉴别机制的有效性。
密钥管理	1.文档审查 审查评估文档，确认是否有关于商密子系统密钥管理功能的描述。 2.功能测试 进行密钥操作测试，验证密钥导入、导出和删除操作的正确性和安全性。
证书管理	1.文档审查 审查评估文档，确认是否有关于商密子系统证书管理设置功能的描述。 2.功能测试 检查证书管理的流程和权限控制。 进行证书操作测试，验证证书的导入、导出和删除操作的正确性和安全性。
文件、磁盘加密设置	1.文档审查 审查评估文档，确认是否有关于商密子系统相关文件、磁盘加密设置功能的描述。 2.功能测试 检查文件和磁盘的加密算法和密钥管理策略。 进行数据恢复测试，验证加密数据的完整性和可恢复性。
通信加密设置	1.文档审查 审查评估文档，确认是否有关于商密子系统与外部通信加密设置功能的描述。 2.功能测试 检查通信加密协议（如TLS/SSL）的配置和实施情况。 进行网络抓包测试，验证通信数据的加密状态。
敏感数据存储保护设置	1.文档审查 审查评估文档，确认是否有关于商密子系统敏感数据存储保护设置功能的描述。

	2.功能测试 检查敏感数据的存储方式和访问控制策略。 进行数据访问测试，验证敏感数据的保护措施是否有效。
日志策略设置	1.文档审查 审查评估文档，确认是否有关于商密子系统日志策略设置功能的描述。 2.功能测试 检查审计日志的记录内容和存储方式。 进行操作模拟测试，验证审计日志的记录准确性和完整性。
密码资源库管理	1.文档审查 审查评估文档，确认是否有关于商密子系统密码资源库管理功能的描述。 2.功能测试 检查密码资源库的安装和配置情况。 进行密码资源库自测试和升级测试，验证密码资源库的正确性和安全性。
密码调用接口管理	1.文档审查 审查评估文档，确认是否有关于商密子系统密码调用接口管理功能的描述。 2.功能测试 检查密码调用接口的权限控制和日志记录。 进行接口调用测试，验证密码调用接口的安全性和正确性。
启用/禁用外部接口	1.文档审查 审查评估文档，确认是否有关于商密子系统启用/禁用外部接口功能的描述。 2.功能测试 检查外部接口的启用和禁用流程。 进行接口访问测试，验证外部接口的控制措施是否有效。
其他必要的管理	1.文档审查 审查评估文档，确认是否有关于商密子系统其他必要的管理功能的描述。 2.功能测试 检查相应管理措施的实施情况。 进行综合测试，验证系统的整体安全和稳定运行。

【要求6.5-03】商密子系统管理操作可通过命令行或管理面板方式实施。

评估：

1. 文档审查

检查商密子系统的设计文档、用户手册和管理指南，确认是否包含通过命令或管理面板进行管理的相关说明。

2. 功能测试

测试命令行管理功能：

可以使用系统自带的命令行工具或第三方命令行工具，通过命令行界面输入管理命令，观察命令执行结果，确认是否能够成功执行管理操作。

测试管理面板功能：

通过管理面板界面进行操作，观察操作结果，确认是否能够成功执行管理操作。

3. 安全性测试

对命令或管理面板进行渗透测试，尝试未授权访问或执行非法操作。

检查是否有适当的安全措施，如访问控制、操作审计等。

确认系统在遭受攻击时的恢复能力。

A.1.5.4 身份鉴别

【要求6.5-04】商密子系统应具备鉴别机制以对商密主管进行身份鉴别，防止非商密主管对商密子系统进行控制。

说明：

商密主管对商密子系统进行管理操作前应对商密主管进行身份鉴别。

可采用口令（或生物信息）、多因素等鉴别机制。

第一次访问商密子系统时，商密子系统中无商密主管鉴别数据，应使用其他被授权的方法（例如，过程控制，使用出厂设置或默认的鉴别数据）进行访问控制和初始化鉴别。

评估：

1. 文档审查

审查评估文档，确认商密子系统是否有商密主管身份鉴别机制的描述。

2. 功能测试

测试商密主管是否使用口令（或生物信息）、证书方式方可登录商密子系统。

模拟系统登录过程，确保登录界面提示正确，在登录者输入错误口令和证书时的响应。

检查系统是否记录了所有鉴别的尝试和结果。

A.1.5.5 数据保护

【要求6.5-05】商密子系统应对相关数据实施保护。

说明：

商密子系统至少满足表3给出的相关数据保护要求。

表3 商密子系统相关数据及保护要求

数据种类	说明	保护要求		
		访问控制	机密性	完整性
密码资源	密码模块程序。	禁止非法修改		保护
硬件密码资源驱动程序	负责与硬件密码模块（如智能卡、硬件安全模块等）进行通信的密码资源驱动程序。	禁止非法修改		保护
商密子系统敏感数据	存放在密码资源之外的数据：数据加密密钥（DEK）、密钥加	禁止非法读取、修改。	加密存储	保护

	密密钥（KEK）、根密钥（RK）、证书，内核代码杂凑值等； 商密主管用户凭证：包括用户名、口令、生物识别信息以及它们的杂凑值等。			
商密子系统可执行文件	密码服务程序：执行数据加密和解密、密钥管理等功能的密码调用接口API中间件。 管理程序：执行商密子系统管理项目。 安全审计工具：用于监控和记录系统的安全活动的程序。	禁止非法修改		保护
商密子系统日志	记录系统操作、事件、错误和安全审计信息，用于事后分析和合规审计。	禁止非法读取、修改		保护
密码配置文件	加密算法配置：选择使用的加密算法及其参数。 安全策略：定义系统级别的安全策略和规则。 密钥存储位置：指定密钥和证书的存储位置。	禁止非法修改		保护
其他重要数据	备份和恢复数据。 合规性文件：如安全策略、操作手册、培训材料等，确保系统操作符合相关法规和标准。	禁止非法修改		

【要求6.5-06】商密子系统应支持访问控制功能，防止商密子系统相关数据被非法修改、读取。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统支持访问控制功能，防止商密子系统相关数据被非法修改、读取的描述。

2. 功能测试

——检查操作系统访问控制策略

使用命令或工具查看操作系统的访问控制列表（ACL）或安全策略配置，确认是否有专门为商密主管用户设置的角色和权限，是否已设置适当的访问控制策略。

——检查密码资源库访问控制

使用命令或工具检查密码资源库的文件/目录权限，确认非商密主管用户无法修改密码资源库，以及密码资源库修改权限是否仅限于商密主管用户。

——检查硬件密码资源驱动程序访问控制

使用命令或工具查看操作系统的设备管理器或驱动管理工具，检查驱动程序的访问权限，尝试以非商密主管用户的身份修改驱动程序，确认硬件密码资源驱动程序的修改权限是否仅限于商密主管用户。

——检查商密子系统敏感数据访问控制

使用命令或工具检查存储商密子系统重要敏感数据（文件或数据库）的访问权限，尝试以非商密主管用户的身份修改、读取这些数据，确认数据的修改、读取权限是否仅限于商密主管用户。

——检查商密子系统可执行文件访问控制

使用命令或工具检查商密子系统可执行文件的文件权限，尝试以非商密主管用户的身份修改这些文件，确认商密子系统的可执行文件的修改权限是否仅限于商密主管用户。

——检查商密子系统日志访问控制

使用命令或工具检查日志文件的文件权限，尝试以非商密主管用户的身份修改、读取日志文件，确认商密子系统的日志文件的修改、读取权限是否仅限于商密主管用户。

——检查密码配置文件访问控制

使用命令或工具检查商密子系统配置文件的文件权限，尝试以非商密主管用户的身份修改配置文件，确认配置文件的修改权限是否仅限于商密主管用户。

——检查其他重要数据访问控制

使用命令或工具检查商密子系统所有相关文件的访问权限，尝试以非商密主管用户的身份修改这些文件，确认这些重要数据的修改权限是否仅限于商密主管用户。

【要求6.5-07】商密子系统应具备对其敏感数据实施加密保护功能。

说明：

对商密子系统敏感数据加密应使用商密子系统密码资源库（或密码模块）实施，采用SM4算法，数据加密密钥（DEK）生成满足【要求6.3-01】，DEK需由密钥加密密钥（KEK）加密保护，KEK由商密主管口令（或个人生物信息）派生，也可由商密主管口令（或个人生物信息）与操作系统根密钥（RK）组合派生。RK由随机数生成器产生，并存储在硬件中，运行时与操作系统其他任务隔离，只能被商密子系统进程读取。KEK按照GM/T 0091规范派生。

评估：

1. 文档审查

审查评估文档，确认是否有关于对其敏感数据实施加密保护功能的描述。

2. 功能测试

——算法正确性检测

审查系统相关代码，确认对商密子系统敏感数据进行 SM4 算法加密，确保没有使用其他不安全的加密算法。

使用正确的 SM4 算法、一个 DEK 对一个敏感数据明文 A 进行加密，再测试被评估的商密子系统用同一个 DEK 对 A 进行加密，比较两个加密结果，若结果一致满足要求，否则不满足。

——DEK 生成

采用【要求 6.3-01】的评估方法，验证 DEK 生成是否符合要求。

——DEK保护

检查代码实现，确认DEK使用KEK 进行加密保护。

使用正确的SM4算法、一个KEK对一个DEK进行加密，再测试被评估的商密子系统用同一个KEK对A进行加密，比较两个加密结果，若结果一致满足要求，否则不满足。

——KEK派生

检查KEK派生代码，确认其符合GM/T 0091规范。

使用符合GM/T 0091规范的密钥派生工具、一组派生输入B（主管口令或个人生物信息、RK）生成一个KEK，再测试被评估的商密子系统，用B派生KEK′，比较KEK和KEK′，若结果一致满足要求，否则不满足。

——RK管理

检查相关代码确认RK使用随机数生成器。

采用6.3.1【要求6.3-01】的评估方法，验证RK生成是否符合要求。

检测RK是否存储在硬件中。

验证在操作系统运行时RK是否只能被商密子系统进程读取。

A.1.5.6 系统隔离

【要求6.5-08】商密密码子系统相关资源应与非商密子系统实行隔离。

说明：商密码子系统内核态的隔离资源包括商密资源、文件系统、网络资源等。可采用虚拟机技术或容器机制实现资源隔离。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密密码子系统相关资源应与非商密子系统实现隔离的描述。

2.功能检测

如果使用虚拟机技术，验证商密子系统的虚拟机是否配置了独立的CPU核心、内存和存储资源，且这些资源与非商密子系统的虚拟机不共享。

检查操作系统是否为商密密码子系统配置了独立的用户账户和组策略，确保与非商密子系统用户隔离。

验证商密子系统的文件系统是否与非商密子系统的文件系统分离，可以通过不同的挂载点或文件系统分区来实现。

检查商密资源模块是否安装在一个独立的库中，且该库的访问权限仅限于商密密码子系统。

如果使用容器技术，验证商密子系统是否运行在独立的容器中，且该容器与非商密子系统的容器网络和存储空间隔离。

检查容器的安全配置，包括网络策略、存储权限和进程权限，确保容器内资源不会泄露到容器外。

检查商密子系统是否配置了独立的网络接口和子网，确保其网络流量与非商密子系统的网络流量不交叉。

验证防火墙规则是否正确配置，以阻止商密子系统和非商密子系统之间的不必要通信。

检查是否有明确的用户权限控制，确保只有授权用户可以访问商密子系统的资源。

验证系统是否记录了对商密子系统资源的所有访问尝试，包括成功和失败的尝试。

检查系统配置和日志，确保隔离措施得到执行。

实施实时监控，以检测任何违反隔离策略的行为。

【要求6.5-09】商密子系统管理进程应与系统其他进程实行隔离，商密子系统管理进程优先权高于其他进程，应保证商密子系统管理进程与操作员交互数据安全。

说明：

可采用操作系统容器（或沙箱）机制对商密子系统管理进程进行隔离，在一般操作系统进程隔离机制基础上实现进一步进程隔离。如进程ID、主机名和域名、进程间通信资源（如信号量、消息队列和共享内存）、网络接口和路由表、文件系统挂载点以及用户和组ID等隔离机制。

评估：

1.文档审查

审查系统设计文档，确认是否有关于商密子系统管理进程隔离策略、进程优先级及可信通道实现的表述。

2.功能检测

使用系统监控工具（如top, ps, strace等），检查管理进程的运行环境是否独立。

确认是否有操作系统级别的隔离机制，如虚拟机、容器技术或进程空间隔离。

使用命令和工具验证：每个容器有独立的进程ID空间、每个容器有独立的网络栈、每个容器有独立的文件系统视图、容器资源（CPU、内存、I/O）等限制配置、容器之间文件系统隔离性、容器内的文件权限和用户权限配置、容器之间的网络隔离性等。

使用网络监控工具，对管理进程与操作员交互通道进行渗透测试，检测交互数据是否安全。

利用内存检测工具扫描系统运行时的内存使用情况，验证内存保护机制。

执行代码注入测试，检查系统是否能够检测并阻止恶意代码的执行。

检查容器日志，确保没有异常行为和安全漏洞。

A.1.5.7 可信信道

【要求6.5-10】商密子系统应使用网络安全通信协议与授权的实体之间建立可信信道，进行相关安全通信。

说明：网络安全通信协议可选择 TLS、DTLS、IPSEC、SSH、TLCP 等。授权的实体可能包括密码管理中心、CA 机构、商密子系统管理等远程系统管理员，以进行商密子系统远程密钥分发、证书认证、证书更新、商密子系统远程更新等操作。可信信道的逻辑接口应与其他逻辑接口实现逻辑隔离；可信信道应采用身份鉴别机制进行双方通信，并满足【要求 6.4-06】。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统应使用网络安全通信协议与授权的实体之间建立可信通道功能的描述。

2.功能检测

配置操作系统，使商密子系统与授权的实体进行通信，监控网络传输，确保根据要求选择的网络安全通信协议（TLS、DTLS、IPSEC、SSH、TLCP）建立可信通道，确定通道数据不以明文形式发送。

A.1.5.8 旁路

【要求6.5-11】如果商密子系统具有旁路功能，应设置该功能开启/关闭状态，并应由商密主管开启和关闭。

说明：为了某些需要商密子系统可以实现旁路功能，即指某些系统功能被绕过或不执行。系统应设置旁路开启/关闭状态。关闭时，表明商密子系统保持正常的使用功能，开启时，表明商密子系统部分功能不能执行。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统具有旁路功能的描述。

2. 功能检测

对旁路功能进行功能测试，验证在开启和关闭状态下系统的行为是否符合预期，确保在开启状态下旁路功能正常运行，而在关闭状态下功能被禁用。

检查商密子系统的配置文件或设置界面，查看是否存在旁路功能的开关选项，确保旁路功能的开启/关闭状态可以在系统设置中进行调整。确保只有商密主管或具有相应权限的人员可以更改旁路功能的状态。

检查系统日志记录，查看旁路功能的开启/关闭操作是否被记录。确保系统能够记录并追踪旁路功能状态的变化，以便进行审计和监控。

A.1.5.9 安全日志

【要求6.5-12】商密子系统应能够生成包括但不限于以下事件审计记录：

a） 商密主管身份鉴别（成功/失败）；

b） 敏感数据文件访问（创建、访问、删除、修改、修改权限的尝试成功和不成功）；

c） 审计和记录数据访问（成功/失败）；

d） 系统自检（成功/失败）；

e） 系统重新启动和关闭（成功/失败）；

f） 其他特别定义的可审计事件。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统应能够生成事件审计记录的描述。

2. 功能检测

检查商密子系统的配置，确认是否已配置生成要求的事件审计记录，包括商密主管身份鉴别、敏感数据文件访问、数据访问审计、系统自检、系统重新启动和关闭等事件。

检查生成的事件审计记录的格式和内容，确保记录包含必要的信息，如时间戳、事件类型、触发事件的用户、事件描述等。

进行事件触发测试，模拟商密主管身份鉴别、敏感数据文件访问、系统自检、系统重新启动和关闭等事件，验证系统是否生成相应的审计记录，确保系统能够准确记录各种事件，并能够区分成功和失败的操作。

A.1.5.10自检

【要求6.5-13】商密子系统应具备运行前自测试和条件自测试能力。

说明：运行前自测试是在宿主操作系统启动商密子系统后未输出任何数据之前（处于“加电”状态）执行。条件自测试是在商密子系统处于“运行”状态时执行。

商密子系统应对自身进行完整性验证，并指示密码资源库（软硬件密码模块）执行自测试。如果自测试失败，系统应进入“故障”状态。在“故障”状态下，商密子系统不执行任何密码操作。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统应具备运行前自测试和条件自测试能力的描述。

2. 功能检测

确认商密子系统是否具备在宿主操作系统启动后未输出任何数据之前执行自测试的能力。

确认商密子系统是否能够在“运行”状态时执行条件自测试。

确认商密子系统是否能够对自身进行完整性验证。

确认商密子系统是否能够指示密码资源库（软硬件密码模块）执行自测试。

测试密码资源库自测试功能，验证其能够检测密码资源库的正常运行状态。

模拟自测试失败的情况，验证系统是否能够正确进入“故障”状态。

确认在“故障”状态下商密子系统不执行任何密码操作，以防止系统在异常状态下继续运行可能导致的安全风险。

检查系统是否记录自测试的执行结果和日志信息，包括成功和失败的情况。

A.1.5.11软件/固件安全

【要求6.5-14】商密子系统所有的软件和固件应经过安全检测。

说明：

对商密子系统软件和固件进行安全检测，包括源码审计和二进制分析。

评估：

审查是否有商密子系统所有软件和固件经过安全检测的证据。

【要求6.5-15】商密子系统所有的软件和固件应由开发者（提供者）、第三方权威机构数字签名。安装、运行由宿主操作系统进行签名验证。

说明：

模块的软件和固件部件只包含可运行形式的代码，不包括源代码、目标代码或实时编译的代码。

对商密子系统软件和固件数字签名按照【要求6.2-03】商密算法执行签名/验证操作，数字签名算法至少是SM2算法（GB/T 32918.2）和SM9算法（GM/T 0044）之一。使用的公私钥应由可信权威机构分发。软件/固件开发者、发行者、检测机构等多个责任主体可对一个软件/固件进行签名。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统所有的软件和固件应由开发者（提供者）数字签名的描述。

2. 功能检测

检查系统是否具有软件和固件开发者（提供者）数字签名公钥（证书），使用该公钥确认商密子系统所有的软件和固件是否经过开发者（提供者）进行签名验证。

检查宿主操作系统的软件签名验证流程，测试安装和运营商密子系统时的数字签名验证过程，确保系统能够有效执行签名验证。

检查商密子系统软件和固件数字签名所使用的公私钥是否由可信权威机构签名分发。

检查操作台是否记录软件和固件的数字签名验证结果和日志信息。

A.1.5.12可信更新

【要求6.5-16】如果商密子系统具有加载外部软件/固件的能力，加载时应对外部软件/固件进行签名验证。

说明：

外部软件/固件是指现商密子系统边界之外的软件或固件，软件/固件内容在【要求6.4-13】中给出。在加载之前，加载的软件/固件要进行审验，如果加载的是商密资源，那么新加载的商密资源需要由检测机构重新检测。

软件/固件数字签名符合【要求6.4-08】。

在运行加载的代码之前应执行【要求6.5-13】中规定的软件/固件条件自测试。

软件/固件加载后修改商密子系统版本信息。

评估：

1. 文档审查

审查评估文档，确认是否有关于对加载的外部软件/固件进行签名验证的描述。

2. 功能检测

安装一个没有数字签名和一个有签名的更新软件/固件，验证没有签名的安装失败，有签名的安装成功。

使用无效公钥（证书）和有效公钥（证书）分别对更新的软件/固件进行签名验证，验证无效公钥

（证书）的安装失败，有效公钥（证书）的安装成功。

对可信权威机构分发的证书链进行验证，验证软件/固件数字签名公钥（证书）是否由希望的可信权威机构分发。

A.1.5.13有限状态模型（FSM）

【要求6.5-17】商密子系统应建立有限状态模型（FSM）并在不同状态下运行。

说明：

有限状态模型SFM由状态转移图、状态转移表和状态描述构成。

商密子系统的FSM至少包括以下状态；

开启/关闭状态：此时系统处于停止运行状态；

初始化状态：在系统转换到密码服务密码状态前，执行初始化所处的状态；

商密主管状态：执行密码主管服务的状态（例如，密码初始化、安全管理和密钥管理）。除商密主管以外，任何其他角色被禁止转换成商密主管状态；

敏感数据管理状态：将系统输入、输出敏感数据时所处的状态；

用户状态（若实现了用户角色）：授权用户获得安全服务、执行密码操作或执行其他核准的功能所处的状态；

密码服务状态：执行核准的密码功能时所处的状态；

自测试状态：系统正在执行自测试时所处的状态；

故障状态：当系统遇到故障（错误）状况（例如，自测试失败）时所处的状态；

旁路状态：此状态下系统不以正常的规程进行工作，如在系统维护、故障分析时；

升级状态：系统正在进行软件/固件更新状态。

评估：

1. 文档审查

审查评估文档，确认是否有关于商密子系统应建立有限状态模型，并在不同状态下运行的描述。

2. 功能检测

核实模块的运行与有限状态图和描述一致。

执行商密子系统，使其进入各状态，检验每个状态是否具有不同的标识。

A.2 安全保障要求

A.2.1. 开发

A.2.1.1.功能规范文档

【要求7.1-01】商密子系统开发者应提供商密子系统功能规范文档。

说明：

功能规范文档应描述：

密码子系统的功能；

密码子系统功能的安全域；

密码子系统设计与全部实现的一致性；

所有商密子系统接口的目的和使用方法，包括调用权限及相关参数。API文件应说明每个可用的功能适用于哪些产品和版本；

商密子系统自身功能要求与为外提供支持的功能要求的接口目的和使用方法。

评估：

确认功能规范文档所提供的信息满足开发者提供证据内容和形式的要求。

确定功能规范文档是第6节密码功能要求准确、完整例证说明。

按照密码子系统的功能描述、功能规范说明、设计文档等要求，检查与密码子系统实际开发是否一致。

A.2.2. 指导性文档

A.2.2.1.用户操作指南

【要求7.2-01】商密子系统开发者应提供商密子系统用户操作指南文档。

说明：

用户操作指南不必包含在单个文档中。对商密主管、用户和应用程序开发人员的指导可以在文档或网页中显示。在适当的情况下，指导文档以可扩展的配置检查表描述格式（XCCDF）表示，以支持安全评估自动化。

用户操作指南应对商密子系统每个角色（商密主管、用户及开发者）进行描述：

——在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息。

——怎样以安全的方式使用商密子系统提供的可用接口。

——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。

——与需要执行的用户可访问功能相关安全事件，包括改变安全功能要求所控制实体的安全特性。

——为了充分实现商密子系统安全目的所执行的安全策略。

用户操作指南应确定商密子系统所有可能的操作模式（包括故障或操作错误后的操作）、其后果以及对维护安全操作的影响。

用户操作指南应标示【要求6.5-16】商密子系统运行的所有状态，以及状态与安全运行的关系。

评估：

用户操作指南的部分内容通过第 6 章中的功能要求项目进行验证。

确认所提供的信息满足提供证据内容和形式的所有要求。

确认用户操作指南提供以下信息：

——本地安装的程序列表和相关版本号。

——与商密子系统评估相关联的密码资源说明，向宿主操作系统密子商密主管员说明本商密子系统的评估不包括其他密码资源。

——通过验证数字签名进行商密子系统更新。

A.2.2.2.准备程序

【要求7.2-02】商密子系统开发者应提供商密子系统及评估准备程序。

说明：

开发人员应关注评估活动，以确定有关准备程序的所需内容。

准备程序应描述按照开发人员的交付程序，安全接受交付的商密子系统所需的所有步骤。

准备程序应描述商密子系统安装以及宿主操作系统的运行环境安全准备所需的所有步骤。

评估：

检查为宿主操作系统提供的指南是否充分描述了安全目的中的所有平台。

确认提供的信息满足证据的内容和形式的所有要求。

运用准备过程确认商密子系统能为操作做好安全准备。

A.2.3. 生命周期支持

A.2.3.1. 系统标签

【要求7.3-01】商密子系统应具有唯一性标签。

说明：

建立商密子系统产品标签，以便用户区别同一商家不同产品或版本。

评估：

检查相关文档确认商密子系统具有一个标识符（如产品名称/版本号）。

A.2.3.2. 配置管理覆盖

【要求7.3-02】商密子系统开发者应提供系统配置列表。

说明：

配置列表应包括下列内容：商密子系统自身配置以及安全保障要求所要求的评估证据。

评估：

确认所提供的信息满足评估证据的内容和形式的所有要求。

确认确保商密子系统有明确标签，并在用户操作指南中保持一致。

A.2.3.3. 及时安全更新

【要求7.3-03】商密子系统开发者应在功能规范文档中说明如何及时进行安全更新。

说明：

开发人员应提供如何更新用户系统以及时解决安全问题的信息。包括从报告/发现安全缺陷到更新发布期间向公众提供更新的过程。

系统更新包括密码资源、密码API、商密子系统管理模块等软件/固件，流程包括每个部署机制（如，本地更新、远程更新）。

应给出漏洞公开披露和公开商密子系统可以安全更新之间的时间窗口，以天为单位。

应包括商密子系统安全问题报告的机制。

评估：

应确认所提供的信息满足评估证据的内容和形式的所有要求。

验证功能规范文档是否包含开发人员用于创建和部署安全更新的及时安全更新过程的描述。

验证是否涉及商密子系统、固件和捆绑的应用程序。

除商密子系统开发人员流程外，任何载体或其他第三方流程也在描述中得到了说明。

验证是否描述了部署安全更新的每个机制。

验证对于更新过程每个机制，列出漏洞公开披露和商密子系统修补该漏洞的安全更新之间的时间。

核实是否包括报告商密子系统安全问题的机制（包括电子邮件地址或网站），包括一种保护报告的方法，如使用加密电子邮件或网站的可信通道。

A.2.4. 日常管理

A.2.4.1. 管理制度

【要求7.4-01】使用商密子系统应建立执行以下管理制度：

——商密主管、操作员管理制度和操作规程；
——密钥（证书）管理；
——重要数据备份及应急处置；
——软硬件密码资源及介质管理等制度；
——商密子系统配置管理规定。

说明：

在重要信息系统使用商密子系统时，应定期对相关管理制度和操作规程进行审定、修订；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。

应具有密码应用操作规程的相关执行记录并妥善保存。

评估：

查阅文档和记录：查阅商密管理制度文档，确认职责分工和操作流程；查阅密钥管理文档，确认密钥生成、分发、存储、销毁等流程；查阅数据备份策略、备份记录、应急处置预案、应急演练记录；查阅软硬件密码资源管理文档，确认采购、安装、维护、报废等流程；查阅商密子系统配置管理规定，确认系统配置是否能保障系统安全正确运行。

访谈相关人员：了解相关人员对管理制度的理解程度和实际执行情况。

现场观察：观察实际操作过程，确保管理制度的实际执行符合要求。

A.2.4.2. 人员管理

【要求7.4-02】宿主操作系统使用商密子系统应符合以下人员管理要求：

——设置商密主管和操作员岗位；
——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；
——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；
——定期对相关人员进行考核。

评估：

检查岗位设置：确认是否设置了商密主管和操作员岗位。确保岗位设置和人员管理符合规定。

审查文档和记录：查阅相关的管理制度、培训记录、考核记录等文档。

访谈相关人员：通过访谈了解相关人员对密码相关法律法规和管理制度的了解程度，以及他们接受培训的情况。确保培训内容涵盖必要的专业知识。

A.2.4.3. 应急处置

【要求7.4-03】宿主操作系统使用商密子系统应建立应急处置机制。

说明：

应制定商用密码应用应急策略，做好应急资源准备，当商用密码应用安全事件发生时，应立即启动应急处置措施；向信息系统主管部门及归属的密码管理部门报告事件发生及处置情况。

A.2.5. 一致性测试

【要求7.5-01】对商密子系统进行一致性测试。

说明：

测试是为了确认规范文档中描述的功能以及提供的管理（包括配置和操作），确认在第6章中规定的要求得到满足。评估者生成一份测试报告，记录测试计划和结果。

评估：

确认所提供的信息满足对评估内容和提交证据的所有要求。

测试密码安全功能要求一个子集，确认密码安全功能按要求运行。

A.2.6. 脆弱性评估

【要求 7.6-01】应对商密子系统进行脆弱性评估。

评估：

从公共领域来源进行搜索公开漏洞，以识别商密子系统中潜在漏洞。

根据识别出的潜在漏洞进行渗透测试，以确定商密子系统是否能够抵抗具有基本潜在攻击能力的攻击者所进行的攻击。

附 录 B
（资料性附录）
商密子系统支撑GB/T 20272-2019 密码技术相关要求

表 B.1 列出商密子系统对 GB/T 20272-2019 密码技术相关要求的支撑。

表 B.1 商密子系统对 GB/T 20272-2019 密码技术相关要求支撑表

GB/T20272-2019密码技术相关要求	第二级	第三级	第四级	第五级	商密子系统支撑要求
身份鉴别		✱ 数字证书鉴别等相结合的方式。	—	—	【要求6.4-02】
标记和强制访问控制		✱ 实现跨网络的操作系统间用户数据保密性和完整性保护。	—	—	【要求6.4-06】
数据保密性	✱ a）应提供文件加密功能，用户可对指定的文件和目录进行加密保护；b）支持采用硬件形式对密钥进行保护。	＋ 应提供文件系统加密功能，对存储在加密文件系统中的文件和目录，进行透明加解密。	＋ 应对密钥提供基于硬件信任根的可信存储支持。	—	【要求6.4-03】 【要求6.4-04】 【要求6.4-05】
可信路径			✱ 在本地用户和远程用户进行初始登录和/或鉴别时，操作系统应在它与用户之间建立一条安全的通信路径。此路径对其端点进行了可信标识，并能保护鉴别通信数据免	—	【要求 6.4-06】 【要求 6.5-10】

			遭修改、泄露。		
可信信道			✱ 应在操作系统和另一个可信操作系统之间提供一条通信信道，此信道在逻辑上与其他通信信道隔离，对其端点进行了可信标识，并能保护通信数据免遭修改、泄露。	—	【要求 6.4-06】 【要求 6.5-10】
网络安全保护	✱ 对网络传输数据应能进行加密与完整性保护。	＋ 支持基于系统身份、系统运行状态的双向网络可信接入认证。	＋ 应对网络访问进行控制，只有被授权的且通过可信度量的进程才能访问网络。	—	【要求6.4-06】
可信度量	✱ a）在操作系统启动时应对操作系统内核进行完整性度量；b）在可执行程序启动时应进行完整性度量；c）应对完整性度量基准值进行安全存储，防止其被篡改。	＋ 支持硬件可信芯片作为信任根。	—	—	【要求6.4-08】 【要求6.4-09】 【要求6.4-10】 【要求6.4-11】
注：“✱”表示具有该项要求，“＋”表示本级增加的要求，“—”表示同前级要求。					

参 考 文 献

[1] GB/T 20272-2019 信息安全技术 操作系统安全技术要求
[2] GB/T 18336-2024 网络安全技术 信息技术安全评估准则
[3] GB/T 30270-2024 网络安全技术 信息技术安全评估方法
[4] GB/T 36322 信息安全技术 密码设备应用接口规范
[5] GB/T 37935-2019 信息安全技术 可信计算规范 可信软件基
[6] GB/T 39786 信息安全技术 信息系统密码应用基本要求
[7] GB/T 43578 信息安全技术 通用密码服务接口规范
[8] GM/T 0028-2024 密码模块安全要求
[9] Protection Profile for General Purpose Operating Systems. National Information Assurance Partnership. 2022-09-27.Version:4.3
[10] Mobile Device Fundamentals. National Information Assurance Partnership.2022-09-12.Version:3.3
[11] PP-Module for File Encryption. National Information Assurance Partnership.2019-07-25.Version:1.0