# 商用密码应用与维护

# 职业技能等级标准

标准代码：510097

（2021年2.0版）

中盈创信（北京）科技有限公司 制定

2021 年 12 月　发布

# 目　次

# 前　　言

本标准按照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。

本标准起草单位：中盈创信（北京）科技有限公司、中国电子商会、浪潮云信息技术股份公司、重庆电子工程职业学院、常州信息职业技术学院、中科磐云（北京）科技有限公司。

本标准主要起草人：孙昕炜、周明、武春岭、陈振宇、张晖、周恒、齐光鹏、方亚东、赵志刚、颜亮、鲁先志、王磊、胡兵、李贺华、张靖、唐继勇、黄宇航、白超异、孙雨春。

## 1 范围

本标准规定了商用密码应用与维护职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于商用密码应用与维护职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

## 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，其最新版本适用于本文件。

国家、行业有关标准如下：

GM/Z 4001-2013 密码术语

GM/Z 0054-2018 信息系统密码应用基本要求

GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》

GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》

GB/T 38625-2020《信息安全技术　密码模块安全检测要求》

GB/T 38629-2020《信息安全技术　签名验签服务器技术规范》

GB/T 38635.1-2020《信息安全技术　SM9 标识密码算法 第 1 部分：总则》

GB/T 38635.2-2020《信息安全技术　SM9 标识密码算法 第 2 部分：算法》

GB/T 38636-2020《信息安全技术　传输层密码协议（TLCP）》

GB/T 38647.1-2020《信息技术　安全技术 匿名数字签名 第 1 部分：总则》

GB/T 38647.2-2020《信息技术　安全技术 匿名数字签名 第 2 部分：采用群组公钥的机制》

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0051 密码设备管理 对称密钥管理规范

GM/T 0052 密码设备管理 VPN 设备监察管理规范

GM/T 0053 密码设备管理 远程监控与合规性检验接口数据规范

## 3 术语和定义

GM/Z 4001-2013等界定的以及下列术语和定义适用于本标准。

3.1

**加密 encryption**

是指采用特定变换的方法，将原来可读的信息变成不能识别的符号序列。

3.2

**商用密码 commercial encryption**

商用密码是指对不涉及国家秘密的信息与网络进行加密保护或者安全认证所使用的密码。

3.3

**商用密码产品 commercial encryption products**

商用密码产品是指由国家密码管理机构批准许可的单位生产、销售和使用的，用于保护信息安全，维护公民、组织和国家安全和利益的信息安全产品。

3.4

**加密保护 encryption protection**

加密保护是指采用特定变换的方法，将原来可读的信息变成不能识别的符号序列。简单地说，加密保护就是将明文变成密文。

3.5

**安全认证 security certification**

安全认证是指采用特定变换的方法，确认信息是否被篡改，包括增加或删除、是否来自可靠信息源，以及确认行为是否真实。简单地说，安全认证就是确认主体和信息的真实可靠性。

3.6

**数字签名 digital signature**

数字签名是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明，是非对称密钥加密技术与数字摘要技术的应用。

## 4 适用院校专业

### 4.1 参照原版专业目录

中等职业学校：计算机应用、网络信息安全、计算机网络技术、网站建设与管理、软件与信息服务、移动应用技术与服务、网络安防系统安装与维护、计算机与数码产品维修、通信技术、通信运营服务、电子商务、跨境电子商务、电子与信息技术、物联网技术应用等相关专业。

高等职业学校：信息安全与管理、计算机信息管理、大数据技术与应用、人工智能技术服务、工业网络技术、移动应用开发、计算机网络技术、计算机应用技术、软件技术、软件与信息服务、电子商务技术、电子商务、跨境电子商务、云计算技术与应用、移动互联应用技术、通信技术、光通信技术、移动通信技术、通信系统运行管理、物联网工程技术等相关专业。

高等职业教育本科学校：计算机应用工程、网络工程、软件工程、大数据技术与应用、信息安全与管理、区块链技术与应用、通信工程、电子信息工程、物联网工程、跨境电子商务、电子商务、工业机器人技术、自动化技术与应用等相关专业。

应用型本科学校：保密技术、计算机科学与技术、软件工程、网络工程、信息安全、物联网工程、智能科学与技术、电子与计算机工程、数据科学与大数据技术、网络空间安全、区块链工程、人工智能、工业智能、智能装备与系统、通信工程、电子信息工程、信息工程、电子商务、跨境电子商务、机器人工程、自动化、电气工程及其自动化等相关专业。

### 4.2 参照新版职业教育专业目录

中等职业学校：计算机应用、网络信息安全、计算机网络技术、网站建设与管理、软件与信息服务、大数据技术应用、移动应用技术与服务、网络安防系统安装与维护、计算机与数码设备维修、现代通信技术应用、通信运营服务、电子商务、跨境电子商务、电子信息技术、物联网技术应用等相关专业。

高等职业学校：密码技术应用、信息安全技术应用、大数据技术、人工智能技术应用、工业互联网技术、区块链技术应用、移动应用开发、计算机网络技术、计算机应用技术、软件技术、电子商务、跨境电子商务、云计算技术应用、移动互联应用技术、现代通信技术、现代移动通信技术、通信软件技术、通信系统运行管理、智能互联网络技术等相关专业。

高等职业教育本科学校：计算机应用工程、网络工程技术、软件工程技术、大数据工程技术、云计算技术、信息安全与管理、人工智能工程技术、工业互联网技术、区块链技术、现代通信工程、电子信息工程技术、物联网工程技术、跨境电子商务、电子商务、机器人技术、自动化技术与应用、工业互联网工程等相关专业。

应用型本科学校：密码科学与技术、保密技术、计算机科学与技术、软件工程技术、网络工程技术、信息安全与管理、物联网工程技术、智能科学与技术、电子与计算工程、数据科学与大数据技术、网络空间安全、区块链工程、人工智能、人工智能工程技术、工业智能、智能装备与系统、现代通信工程、电子信息工程技术、物联网工程技术、信息工程、电子商务、跨境电子商务、机器人工程、自动化、电气工程及自动化等相关专业。

## 5 面向职业岗位（群）

【商用密码应用与维护】（初级）：主要针对企事业单位密码应用需求，面向网络与信息安全管理员、信息通信网络运行管理员等从事密码和密钥的维护管理工作的岗位（群），针对企业密码应用需求，保障信息系统正常运行以及业务数据安全，防止由于商用密码相关应用设置不当导致的信息泄露和损失。

【商用密码应用与维护】（中级）：主要针对企事业单位密码维护管理需求，面向信息安全工程技术人员、信息系统运行维护工程技术人员等岗位（群），能够根据企业的数据安全需求灵活配置和使用企业网络中的商用密码安全产品，能够对重要数据链路和相关应用进行合理的加密保护配置，及时发现安全保密隐患并妥善处理。

【商用密码应用与维护】（高级）：主要针对企事业单位信息管理工程技术人员、信息系统分析工程技术人员等岗位（群），能够深入解读国家等级保护和商用密码安全的相关标准要求，熟悉各类安全产品功能和特点，能够主持完成不同类型不同规模的企业商用密码安全应用现状检测和评估，并提出有针对性的解决方案和规划设计。

## 6 职业技能要求

### 6.1 职业技能等级划分

商用密码应用与维护职业技能等级分为三个等级：初级、中级、高级。三个级别依次递进，高级别涵盖低级别技能要求。

【商用密码应用与维护】（初级）：根据企业密码管理相关制度的要求，执行商业密码应用相关的日常业务操作，对各类商用密码设备器材进行合理选型和使用，并对常用的软硬件业务系统、信息通道进行合理加密配置和日常运行维护。

【商用密码应用与维护】（中级）：根据密码技术国家标准，指导信息安全管理员选配合适的密码技术和安全体系架构，根据企业商用密码保护的相关要求，将加密系统、保密制度灵活部署实施到企业生产环境中，负责安全设备的日常管理和维护，针对设备保密运行情况和商用密码应用的制度运行情况，对发现的软硬件系统、管理制度提出整改意见，并在审批后实施。

【商用密码应用与维护】（高级）：根据国家等级保护和商用密码安全的要求，分析不同企业应用和数据安全需求，撰写规范的企业信息系统安全需求分析报告，能够设计完成满足国家标准的商用密码系统建设方案，制定完善可行的商用密码管理制度，能够按照商用密码系统的等级保护要求，主持测评不同规模和类型的企业网络商用密码系统，对商用密码应用实施情况进行合理评级。

### 6.2 职业技能等级标准描述

表 1 商用密码应用与维护职业技能等级要求（初级）

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| 1.密码设备维修及数据恢复 | 1.1 密码设备芯片级维修 | 1.1.1 能够参考设备技术文件拆装常见密码设备主板，完成设备修复，恢复设备原有功能。<br>1.1.2 能够参考设备技术文件更换常见密码设备的存储模块，完成存储模块的重新设置。<br>1.1.3 能够根据维修工作的具体要求合理选用芯片维修工具，并进行工具使用前后的校准校验和保养。<br>1.1.4 能够根据存储介质技术文件分析存储介质的控制电路和工作原理，合理判断故障，并修复故障电路。 |
| | 1.2 密码系统数据软恢复 | 1.2.1 能够使用 WinHex、Diskgenius 等磁盘编辑器完成存储介质的故障修复，恢复所指定的数据文件内容。 |
| | 1.3 密码系统数据专业设备恢复 | 1.3.1 能够使用主流数据恢复设备，对各类密码系统的故障数据进行有效恢复和重置，恢复系统的正常功能。 |
| 2. 加密产品应用 | 2.1 应用层加密技术使用 | 2.1.1 能够根据应用需求合理选择使用 DES、3DES、AES、SM4 等对称加密算法，实现应用层加密。<br>2.1.2 能够根据不同应用通信接口的要求合理选择使用 SSL、SSH、SOCKS、HTTPS、S-MIME 等安全协议，实现应用连接的信息安全保护。<br>2.1.3 能够根据邮件系统的整体配置要求配置实现邮件客户端加密，实现邮件客户端的正常加密通信。<br>2.1.4 能够在不同类型操作系统上，合理配置实现 SSL VPN 客户端，实现网络连接链路加密和客户端接入 VPN 网络。 |
| | 2.2 主机层加密技术使用 | 2.2.1 能够根据不同操作系统的具体操作要求，选择操作系统文件加密方法并实施，实现系统文件保密要求。<br>2.2.2 能够根据不同操作系统的具体操作要求，选择操作系统磁盘加密方法并实施，实现系统磁盘的加密解密功能。<br>2.2.3 能够根据不同系统设置情况，判断加密文件的可能加密方案，选择加密文件数据恢复的方法并实施，还原加密文件当中的数据内容。<br>2.2.4 能够按照典型口令密码强度要求的实施策略要求，针对主流操作系统的登录口令策略进行有效的设置和实施，使得系统密码口令安全级别符合对应安全策略级别的具体要求。 |

| | | |
|---|---|---|
| | 2.3 网络层加密技术使用 | 2.3.1 能够不同网络通信方式的要求，合理选择 PPP、PPTP、L2TP、IPSec 相关隧道协议并实施，建立加密通信网络通道。<br>2.3.2 能够根据操作系统和网络通信方式的特定要求，配置实现不同隧道协议的 VPN 客户端，实现客户端接入 VPN 网络。<br>2.3.3 能够根据加密操作规范要求，配置实现三层交换机、路由器、防火墙等设备账户口令加密存储，并在对应网络设备上实施。 |
| | 2.4 物理层加密产品使用 | 2.4.1 能够根据应用要求，合理选择和使用加密狗、U 盾等加密产品，实现应用软件的合理加密。<br>2.4.2 能够区分各类射频卡、接触式芯片卡等使用的密码技术，并在各类加密环节当中合理应用。 |
| 3.认证产品应用 | 3.1 信息系统中认证“人”的身份 | 3.1.1 能够根据信息系统的保密要求，合理部署和使用口令认证技术，实现网络和系统加密。<br>3.1.2 能够根据信息系统的保密要求，部署和使用 USB Key 认证技术，实现 USB Key 认证方式的系统加密。<br>3.1.3 能够根据信息系统的保密要求，部署和使用基于生物特征认证技术的加密方案。 |
| | 3.2 信息系统中认证“主机”的身份 | 3.2.1 能够基于可信第三方认证协议和双方认证协议实现对主机的认证，完成主机认证体系搭建。<br>3.2.2 能够基于公钥密码体制的认证协议实现对主机认证。<br>3.2.3 能够基于单向认证协议和双向认证协议实现对主机的认证。 |
| | 3.3 数字签名技术产品应用 | 3.3.1 能够根据实际选择密码生成算法、标记算法、验证算法，搭建数字签名体系。<br>3.3.2 能够根据系统加密要求，实现 PKI 技术架构，完成系统加密。<br>3.3.3 能够选择使用哈希算法和基于非对称密钥加密体制的数字签名技术，应用于系统加密过程。<br>3.3.4 能够根据电子签名体系要求，完成搭建并实现电子签名体系。<br>3.3.5 能够根据加密系统规划要求，实现电子签名的合法性验证过程，完成系统电子签名验证体系。 |

表 2 商用密码应用与维护职业技能等级要求（中级）

| 工作领域 | 工作任务 | 职业技能要求 |
|---|---|---|

| | | |
|---|---|---|
| 1.加密系统配置 | 1.1 应用层加密技术配置 | 1.1.1 能够根据系统加密要求，在应用层配置实现 DV SSL，实现通信连接。<br>1.1.2 能够根据系统加密要求，在应用层配置实现 OV SSL，实现通信连接。<br>1.1.3 能够根据系统加密要求，在应用层配置实现 EV SSL，实现通信连接。<br>1.1.4 能够根据邮件系统搭建要求，在电子邮件系统配置实现 PGP 个人邮件加密，完成加密邮件正常收发解读。<br>1.1.5 能够根据邮件系统搭建要求，在电子邮件系统配置实现 PGP 企业级邮件加密，完成加密以后见正常收发解读。<br>1.1.6 能够在应用层开展商用密码检测认证体系工作。<br>1.1.7 能够理解《中华人民共和国密码法》《中华人民共和国电子签名法》《商用密码管理条例》等相关法规和标准内涵，能够完成所要求的“合规性”内部工作审查步骤。 |
| | 1.2 主机层加密技术配置 | 1.2.1 能够根据操作系统要求，配置实现操作系统文件加密。<br>1.2.2 能够根据操作系统要求，配置实现操作系统磁盘加密。<br>1.2.3 能够根据加密文件的加密配置方案要求，配置实现加密文件数据恢复。<br>1.2.4 能够根据不同操作系统的实际情况，实现操作系统密码破解，恢复操作系统的各类账户设置。 |
| | 1.3 网络层加密技术配置 | 1.3.1 能够根据通信网络加密要求，配置实现各种隧道协议的 VPN 安全访问，实现加密网络连接。<br>1.3.2 能够根据通信网络结构体系和加密体系要求,配置实现多点 IPSec VPN 的实现与 NAT 地址转换，实现加密网络连接。<br>1.3.3 能够根据网络通信结构体系要求，在交换机、路由器、防火墙等设备上配置实现身份认证，完成各类网络设备的设备加密访问配置。 |
| | 1.4 物理层加密产品配置 | 1.4.1 能够根据使用说明书，配置和使用银行服务业身份认证产品，正常访问银行类应用服务。<br>1.4.2 能够根据使用说明书，配置和使用网上证券服务身份认证产品，正常访问证券类应用服务。<br>1.4.3 能够根据使用说明书，配置和使用电子 |

| | | |
|---|---|---|
| | | 政务服务身份认证产品，正常访问电子政务类应用服务。<br>1.4.4 能够根据使用说明书，配置和使用移动数据业务身份认证产品，正常访问移动数据业务应用服务。 |
| 2.认证系统配置 | 2.1 微软 Windows 数字身份认证 | 2.1.1 能够按照网络认证系统设计要求，配置实现 Windows 证书服务器，为其他应用提供数字身份认证服务。<br>2.1.2 能够按照网络数字身份认证操作规范要求，使用 Web 方式申请和安装证书，为其他应用提供数字身份认证服务。<br>2.1.3 能够在 Windows 证书服务器上按操作说明要求，进行查看和吊销证书，完成证书日常管理任务。<br>2.1.4 能够在 Windows 证书服务器上按操作说明要求，进行服务器端审核、发放、管理证书，完成证书日常管理任务。<br>2.1.5 能够按照网络数字身份认证操作规范要求，使用微软代码签名工具，完成在微软系统上开发出来的各类应用的数字签名工作。 |
| | 2.2 Kerberos 数字身份认证 | 2.2.1 能够按照网络认证系统设计要求，安装并配置 Kerberos，为其他应用提供数字身份认证服务。<br>2.2.2 能够按照配置说明要求，正确配置 Kerberos 时间戳 TS，为其他应用提供数字身份认证服务。<br>2.2.3 能够按照配置说明要求，配置 Kerberos 票据，为其他应用提供数字身份认证服务。<br>2.2.4 能够按照配置说明要求，配置基于 Kerberos 的 AS 认证服务，为其他应用提供数字身份认证服务。<br>2.2.5 能够按照配置说明要求，配置基于 Kerberos 的 TGS 票据许可服务器，为其他应用提供数字身份认证服务。 |
| | 2.3 PKI 数字身份认证 | 2.3.1 能够按照网络认证系统设计要求，配置实现公钥密码的创建与分发，完成商用密码体系功能搭建。<br>2.3.2 能够按照网络认证系统设计要求，配置实现基于公钥密码体制的保密通信与数字签名，实现商用密码体系认证功能。<br>2.3.3 能够按照网络认证系统设计要求，配置实现安全数字签名——嵌套型加密，实现商用密码体系认证功能。<br>2.3.4 能够按照网络认证系统设计要求，配置 |

| | | |
|---|---|---|
| | | PKI 实现基于非对称型加密系统密钥交换，实现商用密码体系认证功能。<br>2.3.5 能够按照网络认证体系设计要求，配置 PKI 实现基于公钥体制的双向身份验证，实现商用密码体系认证功能。<br>2.3.6 能够根据用户提出对不同商用密码体系的应用要求，完成常用浏览器(Chrome、火狐、IE 等)中的证书安装、更新和删除，实现相应应用的正常使用。 |
| 3.密码应用方案设计与系统集成 | 3.1 商用密码系统产品选用 | 3.1.1 能够根据《信息安全等级保护商用密码管理办法》进行商用密码设备选型，完成相应方案设计。<br>3.1.2 能够根据《商用密码产品目录》进行商用设备选型，完成密码体系方案中的设备清单明细内容。 |
| | 3.2 商用密码系统建设方案的实施 | 3.3.1 能够根据《信息安全技术网络安全等级保护基本要求》实施密码系统集成施工，并验证其功能正常。<br>3.3.2 能够指导监理各类商用密码产品的部署和调试，保证系统正常工作。 |
| | 3.3 区块链技术密码解决方案的设计与实施 | 3.3.1 能够根据区块链应用加密体系要求，选择和设计合适的密码算法用于建立区块链共识机制，完成区块链应用的搭建。<br>3.3.2 能够根据区块链应用系统的具体要求，选择和设计合适的密码算法用于构建区块，完成区块链应用内容的搭建。<br>3.3.3 能够根据区块链应用系统的具体要求，选择和设计去中心化服务器之间进行加密传输的方案，实现服务器之间的加密通信。 |
| 4.密码应用系统安全性测评 | 4.1 数据安全及备份恢复 | 4.1.1 能够根据密码应用体系的整体设计要求，测评数据传输密码技术应用安全性，并提供评估报告。<br>4.1.2 能够根据数据存储加密体系的整体设计要求，测评数据存储密码技术应用安全性，并提供评估报告。 |
| | 4.2 应用层测评 | 4.2.1 能够根据应用系统设计的加密要求，测评应用层的身份标识与鉴别抗抵赖密码保护技术安全性，并提供评估报告。<br>4.2.2 能够根据应用系统设计的加密要求，测评应用层的访问控制完整性密码保护技术安全性，并提供评估报告。<br>4.2.3 能够根据应用系统设计的加密要求，测评应用层的审计记录完整性密码保护技术安全性，并提供评估报告。 |

| | | |
|---|---|---|
| | 4.3 主机层测评 | 4.3.1 能够根据主机系统设计的加密要求，测评主机层的身份标识与鉴别抗抵赖密码保护技术安全性，并提供评估报告。<br>4.3.2 能够根据主机系统设计的加密要求，测评主机层的访问控制完整性密码保护技术安全性，并提供评估报告。<br>4.3.3 能够根据主机系统设计的加密要求，测评主机层的审计记录完整性密码保护技术安全性，并提供评估报告。 |

表 3 商用密码应用与维护职业技能等级要求（高级）

| 工作领域 | 工作任务 | 职业技能标准 |
|---|---|---|
| 1.密码应用方案设计与系统集成 | 1.1 商用密码系统建设方案设计 | 1.1.1 能够理解《信息安全等级保护商用密码技术实施要求》、《信息安全等级保护商用密码技术要求》使用指南、《信息系统密码应用基本要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准的要求，并在商业密码方案设计过程中合理应用，满足各项国家标准要求。<br>1.1.2 能够根据不同场景分析并选用合适的密码体系架构，为用户提供满足应用要求的合理设计方案。<br>1.1.3 能够按照标准要求，撰写规范的信息系统安全需求分析报告。<br>1.1.4 能够根据不同应用场景设计完成满足国家标准的商用密码系统建设方案。<br>1.1.5 能够根据应用场景要求，设计制定完善、可行的商用密码管理制度。 |
| | 1.2 商用密码系统产品选用 | 1.2.1 能够根据《信息安全等级保护商用密码管理办法》进行设备选型，完成系统方案设计。<br>1.2.2 能够根据《商用密码产品目录》进行设备选型，完成系统设备清单。<br>1.2.3 能够分析总结各类商用密码产品特性及其适用范围，并在系统设计过程中合理应用，正确选型。 |
| | 1.3 商用密码系统建设方案的实施 | 1.3.1 能够根据《信息安全技术网络安全等级保护基本要求》实施密码系统集成施工，实现系统和应用的加密功能。<br>1.3.2 能够指导监理各类商用密码产品的部署和调试，解决系统部署配置过程中遇到的不同问题，保证系统正常工作。。 |
| | 1.4 区块链技术密码解决方案的设计与 | 1.4.1 能够根据区块链应用加密体系要求，选择和设计合适的密码算法用于建立区块链共识机制，完成区块链应用的搭建。 |

| | | |
|---|---|---|
| | 实施 | 1.4.2 能够根据区块链应用系统的具体要求，选择和设计合适的密码算法用于构建区块，完成区块链应用内容的搭建。<br>1.4.3 能够根据区块链应用系统的具体要求，选择和设计去中心化服务器之间进行加密传输的方案，实现服务器之间的加密通信。<br>1.4.4 能够根据不同应用场景设计合适的区块链解决方案，满足不同交易频次，交易类型的区块链应用业务功能的实现。 |
| 2.密码应用系统安全性测评 | 2.1 数据安全及备份恢复 | 2.1.1 能够根据密码应用体系的整体设计要求，测评数据传输密码技术应用安全性，进行等级评定，并提供评估报告。。<br>2.1.2 能够根据数据存储加密体系的整体设计要求，测评数据存储密码技术应用安全性，进行等级评定，并提供评估报告。 |
| | 2.2 应用层测评 | 2.2.1 能够根据应用系统设计的加密要求，测评应用层的身份标识与鉴别抗抵赖密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.2.2 能够根据应用系统设计的加密要求，测评应用层的访问控制完整性密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.2.3 能够根据应用系统设计的加密要求，测评应用层的审计记录完整性密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.2.4 能够根据应用系统设计的加密要求，测评应用层的通信安全密码技术应用安全性，进行等级评定，并提供评估报告。 |
| | 2.3 主机层测评 | 2.3.1 能够根据主机系统设计的加密要求，测评主机层的身份标识与鉴别抗抵赖密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.3.2 能够根据主机系统设计的加密要求，测评主机层的访问控制完整性密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.3.3 能够根据主机系统设计的加密要求，测评主机层的审计记录完整性密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.3.4 能够根据主机系统设计的加密要求，测评主机层的程序完整性密码保护技术安全性，进行等级评定，并提供评估报告。 |
| | 2.4 网络层测评 | 2.4.1 能够根据网络系统设计的加密要求，测评网络层的安全访问路径可靠性、真实性、完整性密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.4.2 能够根据网络系统设计的加密要求，测 |

| | | |
|---|---|---|
| | | 评网络层的访问控制完整性密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.4.3 能够根据网络系统设计的加密要求，测评网络层的审计记录完整性密码保护技术安全性，进行等级评定，并提供评估报告。<br>2.4.4 能够根据网络系统设计的加密要求，测评网络层的身份标识与鉴别抗抵赖密码保护技术安全性，进行等级评定，并提供评估报告。 |
| | 2.5 密码风险评估 | 2.5.1 能够运用工具对密码产品漏洞进行扫描，发现并记录密码产品脆弱性或安全隐患。<br>2.5.2 根据密码等级和要求，能够对密码强度及安全性进行全面测试，并完成密码产品的风险评估报告。<br>2.5.3 能够发现影响核心密码、普通密码安全的“风险隐患”，并能够立即采取应对措施。 |
| 3.密码应用系统维护与管理 | 3.1 密码应用系统秘钥管理 | 3.1.1 能够按照商用密码应用系统管理制度要求，实施密钥的生成、存储、分发、导入、导出、备份、恢复、归档和销毁。 |
| | 3.2 密码应用日常管理 | 3.2.1 能够按照商用密码应用系统管理制度要求，监控并分析商用密码系统的运行状况。<br>3.2.2 能够根据信息系统规模、业务范围以及用户等要素的变化，调整商用密码系统功能和策略。<br>3.2.3 能够根据运维实际情况，向上级主管部门提出系统改造升级的具体需求。 |
| | 3.3 密码应用策略管理 | 3.3.1 能够根据系统应用情况的不同规模和发展阶段，规划制定适合的密码算法和密码协议配用策略。<br>3.3.2 能够根据系统应用的具体要求，规划制定适合的密码设备使用策略。<br>3.3.3 能够根据企业系统应用规模和加密等级保护的不同要求，设计制定适合的密码安全防护要求。 |

# 参考文献


[1] GM/Z 4001-2013 密码术语

[2] GM/Z 0054-2018 信息系统密码应用基本要求

[3] GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》

[4] GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》

[5] GM/T 0050 密码设备管理 设备管理技术规范

[6] GB/T 38625-2020《信息安全技术 密码模块安全检测要求》

[7] GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》

[8] GB/T 38635.1-2020《信息安全技术 SM9标识密码算法 第1部分：总则》

[9] GB/T 38635.2-2020《信息安全技术 SM9标识密码算法 第2部分：算法》

[10] GB/T 38636-2020《信息安全技术 传输层密码协议（TLCP）》

[11] GB/T 38647.1-2020《信息技术 安全技术 匿名数字签名 第1部分：总则》

[12] GB/T 38647.2-2020《信息技术 安全技术 匿名数字签名 第2部分：采用群组公钥的机制》

[13] GM/T 0051 密码设备管理 对称密钥管理规范

[14] GM/T 0052 密码设备管理 VPN设备监察管理规范

[15] GM/T 0053 密码设备管理 远程监控与合规性检验接口数据规范

[16] 霍炜，郭启全，马原 《商用密码应用与安全性评估》[J].电子工业出版社,2020(04).

[17] 中华人民共和国密码法

[18] 中华人民共和国职业教育法

[19] 中华人民共和国高等教育法

[20] 中华人民共和国标准化法

[21] 教育部关于印发《职业教育专业目录（2021年）》的通知（教职成〔2021〕2号）

[22] 教育部关于公布2019年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2020〕2号）

[23] 《教育部关于公布2020年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2021〕1号）

[24] 中华人民共和国职业分类大典

[25] 《关于开展职业教育校企深度合作项目建设工作的通知》（教职成厅函〔2018〕55号）

[26] 《国家职业教育改革实施方案》（国发〔2019〕4号）