# 商用密码应用与维护

# 职业技能等级标准

（2021年1.0版）

**中盈创信（北京）科技有限公司 制定**

2021 年 4 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：中国电子商会、中盈创信（北京）科技有限公司、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。

本标准主要起草人：周明、孙昕炜、武春岭、陈振宇、潘成、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。

## 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

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、网站建设与管理、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、移动商务、跨境电子商务、网络营销、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、虚拟现实技术应用、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、移动商务、商务数据分析与应用、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。

应用型本科学校：计算机应用工程、网络工程技术、软件工程技术、大数据技术与应用、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。

**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，面向安全管理员、安全保密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，防止黑客攻击和用户越权访问引起的信息泄露和损失。

【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，面向安全管理工程师等岗位（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密码安全产品，能够对重要数据进行备份和恢复，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安全管理高级工程师等岗位（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。

## 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，为企业挑选和购买合适的密码产品，并进行基本的软硬件使用和维护，掌握本单位涉密终端和密码设备的配用情况，建立管理台账，包括数量、密级、责任人、责任处室、安放地点等。

【商用密码应用与维护】（中级）：根据密码技术国家标准，指导密码管理员选择合适的密码技术和安全体系架构，灵活部署到企业生产环境中，负责安全设备的日常管理和维护，每月对重要安全产品的日志进行分析整理，向上级主管部门提出升级改造的具体需求和愿望。

【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，能够主持测评不同规模和类型的企业网络商用密码系统的安全性并给出针对性的整改意见。

### 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 能够拆装常见密码设备主板。<br>1.1.2 能够更换常见密码设备的存储模块。<br>1.1.3 能够合理选用芯片维修工具。<br>1.1.4 能够分析存储介质的控制电路和工作原理。 |
| | 1.2 密码系统数据软恢复 | 1.2.1 能够使用 WinHex、Diskgenius 等磁盘编辑器修复磁盘和数据。 |
| | 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施设备。 |
| 2. 加密产品应用 | 2.1 应用层加密技术使用 | 2.1.1 能够选择使用 DES、3DES、AES、SM4 对称加密算法。<br>2.1.2 能够选择使用 SSL、SSH、SOCKS、HTTPS、S-MIME 等安全协议。<br>2.1.3 能够配置实现邮件客户端加密。<br>2.1.4 能够配置实现 SSL VPN 客户端。 |
| | 2.2 主机层加密技术使用 | 2.2.1 能够选择操作系统文件加密方法并实施。<br>2.2.2 能够选择操作系统磁盘加密方法并实施。<br>2.2.3 能够选择加密文件数据恢复的方法并实施。<br>2.2.4 能够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。 |
| | 2.3 网络层加密技术使用 | 2.3.1 能够选择 PPP、PPTP、L2TP、IPSec 相关隧道协议并实施。<br>2.3.2 能够配置实现不同隧道协议的 VPN 客户端。<br>2.3.3 能够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。 |

| | | |
|---|---|---|
| | 2.4 物理层加密产品使用 | 2.4.1 能够合理选择和使用加密狗、U 盾等加密产品。<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。 |
| 3.认证产品应用 | 3.1 信息系统中认证“人”的身份 | 3.1.1 能够部署和使用口令认证技术。<br>3.1.2 能够部署和使用 USB Key 认证技术。<br>3.1.3 能够部署和使用基于生物特征认证技术。 |
| | 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。<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。<br>3.3.2 能够实现 PKI 技术架构。<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。<br>3.3.4 能够实现电子签名。<br>3.3.5 能够实现电子签名的合法性验证。 |

**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 能够配置实现 DV SSL。<br>1.1.2 能够配置实现 OV SSL。<br>1.1.3 能够配置实现 EV SSL。<br>1.1.4 能够配置实现 PGP 个人邮件加密。<br>1.1.5 能够配置实现 PGP 企业级邮件加密。<br>1.1.6 能够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，能够进行“合规性”工作审查。 |
| | 1.2 主机层加密技术配置 | 1.2.1 能够配置实现操作系统文件加密。<br>1.2.2 能够配置实现操作系统磁盘加密。<br>1.2.3 能够配置实现加密文件数据恢复。<br>1.2.4 能够实现操作系统密码破解。 |
| | 1.3 网络层加密技术配置 | 1.3.1 能够配置实现各种隧道协议的 VPN 安全访问。<br>1.3.2 能够配置实现多点 IPSec VPN 的实现与 NAT 地址转换。<br>1.3.3 能够在交换机、路由器、防火墙等设备上配置实现身份认证。 |
| | 1.4 物理层加密产品配置 | 1.4.1 能够配置和使用银行服务业身份认证产品。<br>1.4.2 能够配置和使用网上证券服务身份认证产品。<br>1.4.3 能够配置和使用电子政务服务身份认证产品。<br>1.4.4 能够配置和使用移动数据业务身份认证产品。 |
| 2.认证系统配置 | 2.1 微软 Windows 数字身份认证 | 2.1.1 能够配置实现 Windows 证书服务器。<br>2.1.2 能够使用 Web 方式申请和安装证书。<br>2.1.3 能够查看和吊销证书。<br>2.1.4 能够服务器端审核、发放、管理证书。<br>2.1.5 能够使用微软代码签名工具。 |
| | 2.2 Kerberos 数字身份认证 | 2.2.1 能够安装并配置 Kerberos。<br>2.2.2 能够配置 Kerberos 时间戳 TS。<br>2.2.3 能够配置 Kerberos 票据。<br>2.2.4 能够配置基于 Kerberos 的 AS 认证服务。 |

| | | |
|---|---|---|
| | | 2.2.5 能够配置基于Kerberos 的TGS 票据许可服务器。 |
| | 2.3 PKI 数字身份认证 | 2.3.1 能够配置实现公钥密码的创建与分发。<br>2.3.2 能够配置实现基于公钥密码体制的保密通信与数字签名。<br>2.3.3 能够配置实现安全数字签名——嵌套型加密。<br>2.3.4 能够配置 PKI 实现基于非对称型加密系统密钥交换。<br>2.3.5 能够配置 PKI 实现基于公钥体制的双向身份验证。<br>2.3.6 能够完成常用浏览器(Chrome、火狐、IE等)中的证书安装、更新和删除。 |
| 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》进行设备选型。<br>3.1.2 能够根据《商用密码产品目录》进行设备选型。 |
| | 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。<br>3.3.2 能够指导监理各类商用密码产品的部署和调试。 |
| | 3.3 区块链技术密码解决方案的设计与实施 | 3.1.1 能够选择和设计合适的密码算法用于建立区块链共识机制。<br>3.1.2 能够选择和设计合适的密码算法用于构建区块。<br>3.1.3 能够选择和设计去中心化服务器之间进行加密传输的方案。 |
| 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 能够测评数据传输密码技术应用安全性。<br>4.1.2 能够测评数据存储密码技术应用安全性。 |
| | 4.2 应用层测评 | 4.2.1 能够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。 |

| | | |
|---|---|---|
| | | 4.2.2 能够测评应用层的访问控制完整性密码保护技术安全性。<br>4.2.3 能够测评应用层的审计记录完整性密码保护技术安全性。 |
| | 4.3 主机层测评 | 4.3.1 能够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。<br>4.3.2 能够测评主机层的访问控制完整性密码保护技术安全性。<br>4.3.3 能够测评主机层的审计记录完整性密码保护技术安全性。 |

**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。<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。<br>1.1.3 能够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。<br>1.2.2 能够根据《商用密码产品目录》进行设备选型。<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。 |
| | 1.3 商用密码系统 | 1.3.1 能够根据《信息安全技术网络安全等级 |

| | | |
|---|---|---|
| | 建设方案的实施 | 保护基本要求》实施密码系统集成施工。<br>1.3.2 能够指导监理各类商用密码产品的部署和调试。 |
| | 1.4 区块链技术密码解决方案的设计与实施 | 1.4.1 能够选择和设计合适的密码算法用于建立区块链共识机制。<br>1.4.2 能够选择和设计合适的密码算法用于构建区块。<br>1.4.3 能够选择和设计去中心化服务器之间进行加密传输的方案。<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。 |
| 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 能够测评数据传输密码技术应用安全性。<br>2.1.2 能够测评数据存储密码技术应用安全性。 |
| | 2.2 应用层测评 | 2.2.1 能够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。<br>2.2.2 能够测评应用层的访问控制完整性密码保护技术安全性。<br>2.2.3 能够测评应用层的审计记录完整性密码保护技术安全性。<br>2.2.4 能够测评应用层的通信安全密码技术应用安全性。 |
| | 2.3 主机层测评 | 2.3.1 能够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。<br>2.3.2 能够测评主机层的访问控制完整性密码保护技术安全性。<br>2.3.3 能够测评主机层的审计记录完整性密码保护技术安全性。<br>2.3.4 能够测评主机层的程序完整性密码保护技术安全性。 |
| | 2.4 网络层测评 | 2.4.1 能够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。 |

| | | |
|---|---|---|
| | | 2.4.2 能够测评网络层的访问控制完整性密码保护技术安全性。<br>2.4.3 能够测评网络层的审计记录完整性密码保护技术安全性。<br>2.4.4 能够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。 |
| | 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 能够规划制定适合的密码设备使用策略。<br>3.3.3 能够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] 《中等职业学校专业目录》

[22] 《普通高等学校高等职业教育（专科）专业目录》

[23] 《普通高等学校本科专业目录》

[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）