# 4 密码应用设计目标及原则

根据《政务信息系统密码应用与安全性评估工作指南（2020版）》、《国家政务信息化项目建设管理办法》、《商用密码应用安全性评估管理办法（试行）》、《政务信息系统政府采购管理暂行办法》（财库〔2017〕210 号），信息系统无论在规划、建设、运行哪个阶段，项目建设单位和使用单位都应当开展商用密码应用与安全性评估工作。首要就是要撰写《密码应用方案》，密码应用方案是信息系统密码应用的起点，它直接决定着信息系统的密码应用能否合规、正确、有效地部署实施，密码应用方案也是开展信息系统密码应用情况分析和评估工作的基础条件，其设计需依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，结合信息系统的实际情况进行设计，并遵循以下设计目标及原则。

## 4.1 设计目标

围绕《信息系统密码应用基本要求》标准要求，综合考虑{{sysname}}物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的密码应用方案，满足《基本要求》中三级指标要求，并为通过密码应用安全性评估奠定基础。

## 4.2 设计原则与依据

结合设计目标及相关法规的要求，{{sysname}}密码应用设计应遵循以下原则：

1. 全面考虑、重点部署、分步实施原则

{{sysname}}中重要的基础设施和关键信息系统，是融合设备、技术、管理于一体的系统工程，需要全面考虑。同时，要考虑到涉及信息系统安全的重点因素，充分考虑可扩展性和可持续性，从解决眼前问题、夯实基础、建设整个体系方面做好边密码应用工作。

1. 规范性、先进性、可扩展性、完整性并重原则

为保证系统管理工作的有效性和规范性，相关工作应按照国家有关标准实施。系统应采用成熟先进的技术，密码应用总体框架和密码产品必须有较强的可扩展性，为{{sysname}}改进和完善创造条件。

1. 经济性和适度性并重原则

{{sysname}}的建设需要综合考虑资产价值、风险等级，实现总体安全保障。坚持运用风险评估的方法，提出相应的改进措施，对重要基础设施和关键信息系统进行适度的安全建设。

1. 技术和管理并重原则

先进成熟的安全技术防护体系是信息系统稳定运行的必备前提，遵循电子政务信息化发展思路，依据相关国家及行业标准，实现技术体系建设和管理体系建设的有效融合，技术与管理双管齐下，协同发展，有效保障电子政务密码应用的可持续发展。

**主要依据**

{{sysname}}的设计主要依据的国家法律法规具体如下所示：

* GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》
* GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》
* GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
* GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》
* GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》
* GB/T 25058-2019《信息安全技术 信息系统安全等级保护实施指南》
* GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》
* GB/T 36627-2018《信息安全技术 网络安全等级保护测试评估技术指南》
* GB/T 37092-2018《信息安全技术 密码模块安全要求》
* GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》
* GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》
* GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》
* GB/T 33560-2017《信息安全技术 密码应用标识规范》
* GB/T 17901.1-2020《信息技术 安全技术 密钥管理 第1部分：框架》
* GB/T 17901.3-2021《信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制》
* GB/T 15843.3-2016《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》
* GM/T 0054-2018《信息系统密码应用基本要求》
* GM/T 0115-2021《信息系统密码应用测评要求》
* GM/T 0116-2021《信息系统密码应用测评过程指南》
* GM/T 0003-2012《SM2椭圆曲线公钥密码算法》
* GM/T 0009-2012《SM2密码算法使用规范》
* GM/T 0010-2012《SM2密码算法加密签名消息语法规范》
* GM/T 0004-2012《SM3密码杂凑算法》
* GM/T 0002-2012《SM4分组密码算法》
* GM/T 0005-2012《随机性检测规范》
* GM/T 0006-2012《密码应用标识规范》
* GM/T 0018-2012《密码设备应用接口规范》
* GM/T 0016-2012《智能密码钥匙密码应用接口规范》
* GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》
* GM/T 0051-2016《密码设备管理 对称密钥管理技术规范》
* GM/T 0050-2016《密码设备管理 设备管理技术规范》
* GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
* GM/T 0022-2014《IPSec VPN 技术规范》
* GM/T 0023-2014《IPSec VPN 网关产品规范》
* GM/T 0024-2014《SSL VPN 技术规范》
* GM/T 0025-2014《SSL VPN 网关产品规范》
* GM/T 0104-2021《云服务器密码机技术规范》
* GM/T 0088-2020《云服务器密码机管理接口规范》
* GM/T 0030-2014《服务器密码机技术规范》
* GM/T 0027-2014《智能密码钥匙技术规范》
* GM/T 0014-2012《数字证书认证系统密码协议规范》
* GM/T 0033-2014《时间戳接口规范》
* GM/T 0029-2014《签名验签服务器技术规范》
* GM/T 0031-2014《安全电子签章密码应用技术规范》
* GM/T 0087-2020《浏览器密码应用接口规范》
* GW0013-2017《政务云安全要求》
* 《信息系统密码应用高风险判定指引》
* 《商用密码安全性评估FAQ（第二版）》
* 《商用密码应用安全性评估量化评估规则（2021）》
* 《政务信息系统密码应用与安全性评估工作指南》