# 4 安全目标及设计原则

## 4.1安全目标

围绕GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中关于信息系统在系统规划阶段的密码应用要求，综合考虑物理和环境、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GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标要求，确保信息系统可顺利通过密码应用安全性评估，提升XXX系统在密码应用安全性，确保密码应用的正确性、合规性。

## 4.2设计原则与依据

**1.整体性原则。**按照GB/T 39786对信息系统密码应用的基本要求,以及信息系统的安全需求、责任单位的密码应用规划和密码管理需求,进行顶层设计。

**2.科学性原则。**参考信息系统的密码需求、管理需求和整体规划,合理整合和部署密码资源,切实解决应用中的安全问题。

**3.完备性原则。**依据法律、法规、标准等关于密码使用的要求,设计满足信息系统安全需求的密码应用方案。

**4.可行性原则。**密码应用方案切合实际,便于实现,能作为信息系统密码应用建设、验收和密码应用安全性评估的依据。

**5.合规性原则。**密码应用方案中使用的密码算法遵循国家有关法律法规的要求;使用的密码技术遵循国家及行业相关标准:涉及国家安全、国计民生、社会公共利益的信息系统,其使用的密码产品和服务经商用密码认证机构认证合格。

**主要依据**

* + - 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》
    - GB/T 37092-2018《信息安全技术密码模块安全要求》
    - GB/T 38541-2020《信息安全技术 电子文件密码应用指南》
    - GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》
    - GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》
    - GB/T 33482-2016《党政机关电子公文系统建设规范》
    - GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
    - GB/T 36968-2018《信息安全技术 IPSec VPN技术规范》
    - GM/T 0024-2014《SSL VPN 技术规范》
    - GM/T 0025-2014《SSL VPN 网关产品规范》
    - GM/T 0026-2014《安全认证网关产品规范》
    - 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《证书认证系统密码协议规范》
    - GM/T 0033-2014《时间戳接口规范》