**4 密码应用设计目标及原则**

密码应用方案设计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。密码应用方案设计还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，是开展密评工作不可或缺的重要参考文件。

密码应用方案的设计需依照《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，综合考虑北京市医疗系统物理和环境、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**

结合设计目标及相关法规的要求，北京市医疗系统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

北京市医疗系统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，为北京市医疗系统改进和完善创造条件。

1. 经济性和适度性并重原则

北京市医疗系统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。

**4.3 设计依据**

国家标准：

* GB/T 20984-2022《信息安全技术 信息安全风险评估方法》
* GB/T 39786-2021《信息安全技术 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 25070-2019《信息安全技术 网络安全等级保护设计技术要求》
* GB/T 31722-2015《信息技术 安全技术 信息安全风险管理》
* GB/Z 24364-2009《信息安全技术 信息安全风险管理指南》
* GB/T 38626-2020《信息安全技术 智能联网设备口令保护指南》
* GB/T 38628-2020《信息安全技术 汽车电子系统网络安全指南》

行业规范：

* GM/T 0054-2018 《信息系统密码应用基本要求》
* GM/T 0052-2016 《密码设备管理 VPN设备监察管理规范》
* 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 0048-2016 《智能密码钥匙密码检测规范》
* GM/T 0047-2016 《安全电子签章密码检测规范》
* GM/T 0046-2016 《金融数据密码机检测规范》
* GM/T 0045-2016 《金融数据密码机技术规范》
* GM/T 0041-2015 《智能IC卡密码检测规范》
* GM/T 0039-2015《密码模块安全检测要求》
* GM/T 0038-2014《证书认证密钥管理系统检测规范》
* GM/T 0037-2014《证书认证系统检测规范》
* GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》
* GM/T 0031-2014《安全电子签章密码应用技术规范》
* GM/T 0030-2014《服务器密码机技术规范》
* GM/T 0029-2014《签名验签服务器技术规范》
* GM/T 0028-2014《密码模块安全技术要求》
* GM/T 0027-2014《智能密码钥匙技术规范》
* GM/T 0026-2014《安全认证网关产品规范》
* GM/T 0025-2014《SSL VPN网关产品规范》
* GM/T 0024-2014《SSL VPN技术规范》
* GM/T 0023-2014《IPSec VPN网关产品规范》