{{sysname}}

密码应用方案

{{sysunit}}

{{sysdate}}

# 目 录

目 录 I

1 项目背景 5

1.1 国家政策法规要求 6

1.2 密码应用现状 6

1.3 项目实施的必要性 7

2 系统概述 9

2.1 系统基本情况 9

2.1.1 基本情况 9

2.1.2 用户情况 10

2.1.3 系统架构 10

2.1.4 机房情况 11

2.2 系统网络拓扑 12

2.2.1 网络拓扑 12

2.2.2 网络通信信道 13

2.3 承载的业务情况 13

2.3.1 业务应用 13

2.6.2 重要数据 14

2.4 系统软硬件构成 14

2.5 管理制度 15

3 密码应用需求分析 16

3.1 风险控制需求 16

3.1.1 物理和环境安全 16

3.1.2 网络和通信安全 18

3.1.3 设备和计算安全 22

3.1.4 应用和数据安全 26

3.1.5 密码安全管理 30

3.2 需求分析 31

4 密码应用设计目标及原则 33

4.1 设计目标 33

4.2 设计原则与依据 33

5 密码应用技术方案 36

5.1 密码应用技术框架 36

5.2 物理和环境安全 41

5.3 网络和通信安全 43

5.4 设备和计算安全 46

5.5 应用和数据安全 54

5.6 密钥管理 56

5.7 密码应用部署 58

5.8 密码软硬件产品 59

5.9 安全与合规性分析 60

5.9.1 物理和环境安全 60

5.9.2 网络和通信安全 61

5.9.3 设备和计算安全 63

5.9.4 应用和数据安全 66

6 密码安全管理方案 68

6.1 管理制度 68

6.2 管理机构 69

6.3 建设运行 70

6.4 密钥管理 71

6.5 密码软硬件管理 72

6.6 人员管理 72

6.7 应急方案 73

6.7.1 潜在的安全事件分析 73

6.7.2 应急处置组织机构与职责 75

6.7.3 应急处置预案设计 77

7 实施保障方案 82

7.1 实施内容 82

7.1.1 软硬件开发及改造 82

7.1.2 系统集成 82

7.1.3 综合调试 82

7.1.4 试运行 83

7.1.5 最终验收 83

7.1.6 风险点及应对措施 83

7.2 实施计划 85

7.2.1 实施路线图 86

7.2.2 进度计划 86

7.3 保障措施 87

7.3.1 组织保障 87

7.3.2 人员保障 91

7.3.3 经费保障 91

7.3.4 质量保障 91

7.3.5 监督检查 93

7.4 经费概算 94

# 1 项目背景

{{s1}}

## 1.1 国家政策法规要求

1. 《中华人民共和国网络安全法》；
2. 《中华人民共和国密码法》；
3. GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》；
4. GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》；
5. 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》；
6. GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》；
7. GB/T 25058-2019《信息安全技术 信息系统安全等级保护实施指南》；
8. GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》；
9. 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》；
10. GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》；
11. GB/T 38541-2020《信息安全技术 电子文件密码应用指南》；
12. GB/T 38556-2020《信息安全技术 动态口令密码应用技术规范》；
13. GB/T 33560-2017《信息安全技术 密码应用标识规范》；
14. GB/T 37092-2018《信息安全技术 密码模块安全要求》；
15. GM/T 0115-2021《信息系统密码应用测评要求》；
16. GM/T 0116-2021《信息系统密码应用测评过程指南》；
17. GM/T 0054-2018《信息系统密码应用基本要求》；
18. 《信息系统密码应用高风险判定指引》
19. 《商用密码安全性评估FAQ（第二版）》
20. 《商用密码应用安全性评估量化评估规则（2021）》
21. 《政务信息系统密码应用与安全性评估工作指南》
22. 《中华人民共和国电子签名法》；
23. 《关键信息基础设施安全保护条例》；
24. 《网络安全等级保护条例（征求意见稿）》；
25. 《关于贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》；
26. 《商用密码应用安全性评估管理办法（试行）》；
27. 《国家政务信息化项目建设管理办法》国办发【2019】57号；
28. 《国家密码管理局关于请进一步加强国家政务信息系统密码应用与安全性评估工作的函》国密局函【2020】119号；

## 1.2 密码应用现状

如何合规、正确、有效使用商用密码，充分发挥商用密码在保障网络安全的核心技术和基础支撑作用，关乎国家大局、关乎网络空间安全、关乎用户隐私，然而当前密码安全形势严峻，商用密码应用现状不容乐观，主要存在密码应用不广泛、密码应用不规范和密码应用不安全等问题。

{{sysname}}密码应用建设充分考虑建立健全网络和信息系统密码保障体系的必要性，完善密码基础设施，提升密码适用管理水平，推进密码在重要领域系统身份认证、安全隔离、信息加密、信息数据保护等方面的应用，实现密码应用安全工作全面展开迫在眉睫。

然而当前{{sysname}}平台中存在广泛的安全隐患。如，系统设计初期在网络通信方面采用HTTP协议或不合规的HTTPS协议访问，未对通信实体进行身份鉴别，未采取措施提供数据传输的机密性和完整性保护；设备计算安全方面通过账号口令登录系统进行运维管理；在应用数据方面使用账号口令或动态验证密码实现应用登录验证；应用数据未使用加密技术加密存储。{{sysname}}平台整体现状未涉及商用密码安全应用。

## 1.3 项目实施的必要性

为贯彻落实《密码法》关于信息系统密码应用的要求，结合《国家电子政务建设指导意见》，决定对{{sysname}}进行密码应用方案设计，进一步加强重要基础设施的安全防范能力，提高运行保障水平，确保重要信息系统安全稳定运行，防止敏感信息泄露。

通过对{{sysname}}的现状和密码应用需求进行分析，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》设计密码应用方案。

在网络安全上升到国家安全层面之后，{{sysname}}安全性要求，就成为了重中之重。{{sysname}}安全隐患主要分为两个层面：一是系统的安全，包括设备主机安全、中间件安全、操作系统安全、网络安全、应用安全等；二是数据的安全，在数据聚集化的趋势下，集中后的数据如何安全的存储、传输和使用也是个挑战。商用密码对于网络空间技术领域具有重要的基础性、引领性、关键性地位，特别是在数据加密、身份鉴别、访问控制、取证溯源等方面依然发挥着难以替代的重要作用。

到目前为止，密码技术仍是保障网络与信息安全最有效、最可靠、最经济的关键核心技术。通过基于密码技术的身份鉴别、信任管理、访问控制、数据加密、可信计算、密文计算、数据脱敏等措施，可以有效解决数据产生、传输、存储、处理、分析、使用等全生命周期安全问题，解决基础网络资源、信息设施、计算分析、应用服务、网络接入等全体系安全问题。

目前国际上通用的密码算法存在安全隐患，如RSA会被植入后门等，且使用的芯片大部分都是国外产品和技术，在我国尚未完成对这些核心技术控制的现状下，采用国产自主密码技术保障系统安全也成为必然的选择。

《中华人民共和国网络安全法》、《中华人民共和国密码法》（2020年1月1日正式施行）、《网络安全等级保护条例》的陆续颁布，及中央、地方的政策加强，进一步奠定了密码技术作为网络安全保护重要手段的地位。

因此，本项目的建设将切合国家网络安全政策要求，同时将有力地消除密码安全隐患，提升业务系统综合防护能力，保护国家和公共利益。