{{sysname}}

密码应用方案

{{sysunit}}

{{sysdate}}

# 目 录

编制说明 I

目 录 I

1 项目背景 1

1.1 国家政策法规要求 2

1.2 密码应用现状 3

1.3 项目实施的必要性 3

2 系统概述 5

2.1 系统基本情况 5

2.2 物理和环境 6

2.3 网络和通信 6

2.3.1 网络拓扑 6

2.3.2 网络通信信道 7

2.4 设备和计算 7

2.5 应用和数据 9

2.5.1 业务应用 9

2.5.2 重要数据 10

2.6 管理制度 10

3 密码应用需求分析 11

3.1 通用需求分析 11

3.1.1 风险分析 11

3.1.2 密码应用需求 11

3.2 物理和环境 11

3.2.1 风险分析 11

3.2.2 密码应用需求 12

3.2.3 本系统需求分析清单-物理和环境 12

3.3 网络和通信 13

3.3.1 风险分析 13

3.3.2 密码应用需求 13

3.3.3 本系统需求分析清单-网络和通信 14

3.4 设备和计算 14

3.4.1 风险分析 14

3.4.2 密码应用需求 15

3.4.3 本系统需求分析清单-设备和计算 16

3.5 应用和数据 16

3.5.1 风险分析 16

3.5.2 密码应用需求 17

3.5.3 本系统需求分析清单-应用和数据 18

3.6 密钥安全管理 19

3.6.1 风险分析 19

3.6.2 密码应用需求 19

4 密码应用设计目标及原则 21

4.1 设计目标 21

4.2 设计原则 21

4.3 设计依据 22

5 密码应用技术方案 24

5.1 密码应用技术框架 24

5.2 物理和环境 27

5.2.1 密码应用技术方案 27

5.2.2 本系统密码应用技术方案-物理和环境 28

5.3 网络和通信 29

5.3.1 密码应用技术方案 29

5.3.2 本系统密码应用技术方案-网络和通信 30

5.4.1 密码应用技术方案 30

5.4 设备和计算 32

5.4.2 本系统密码应用技术方案-设备和计算 32

5.5 应用和数据 34

5.5.1 密码应用技术方案 34

5.5.2 本系统密码应用技术方案-应用和数据 35

5.6 密钥管理 37

5.6.1 密码应用技术方案 37

5.6.2 本系统密码应用技术方案-密钥管理 37

5.7 密码应用部署 39

5.8 密码软硬件产品 40

5.8.1 密码软硬件产品清单 40

5.8.2 密码软硬件产品介绍 42

5.9 安全与合规性分析 45

5.9.1 物理和环境 45

5.9.2 网络和通信 46

5.9.3 设备和计算 47

5.9.4 应用和数据 48

6 密码安全管理方案 50

6.1 管理制度 50

6.2 管理机构 51

6.3 建设运行 52

6.4 密钥管理 53

6.5 密码软硬件管理 54

6.6 人员管理 54

6.7 应急方案 55

6.7.1 潜在的安全事件分析 55

6.7.2 应急处置组织机构与职责 57

6.7.3 应急处置预案设计 59

7 实施保障方案 64

7.1 实施内容 64

7.1.1 软硬件开发及改造 64

7.1.2 系统集成 67

7.1.3 综合调试 68

7.1.4 试运行 68

7.1.5 最终验收 68

7.1.6 风险点及应对措施 68

7.2 实施计划 70

7.2.1 实施路线图 71

7.2.2 进度计划 71

7.3 保障措施 72

7.3.1 组织保障 73

7.3.2 人员保障 76

7.3.3 经费保障 76

7.3.4 质量保障 76

# 1 项目背景

密码技术作为网络与信息安全保障的核心技术和基础支撑，在身份认证、信息加密、安全隔离、完整性保护和操作抗抵赖等方面发挥着不可替代的作用。《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）提出“加强以密码技术为基础的信息保护和网络信任体系建设，要建立协调管理机制，规范和加强以身份认证、授权管理、责任认定等为主要内容的网络信任体系建设”。《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）也提出“加强网络信任体系建设和密码保障，强化密码在保障电子政务、电子商务安全和保护公民个人信息等方面的支撑作用”。

2019年10月26日，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，习近平主席签署主席令予以公布，于2020年1月1日起正式实施。密码法的出台，为密码科技实现跨越式发展、密码科技创新再上新台阶提供了宝贵的战略机遇和发展契机。当今以数字化、网络化、智能化为特征的信息技术日新月异，围绕5G、大数据、区块链等技术应用带来了大量的新的安全问题。密码技术是解决当前安全问题，保障信息安全最有效的关键核心技术。

2019年年底，国务院办公厅印发《国家政务信息化项目建设管理办法》，明确提出不符合密码应用和网络安全要求等情况的政务信息系统，不安排运行维护经费。项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

2020年4月，国家发改委明确了“新基建”建设范畴。信息基础设施、融合基础设施、创新基础设施3个方面被纳入新型基础设施范畴。新型基础设施是以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系。

2021年3月9日，《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）正式发布，并于2021年10月1日起实施。“基本要求”从行业标准上升为国家标准，是**商用密码应用与安全性评估工作的重要里程碑。**

## 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. 2018年7月中央办公厅印发的《金融和重要领域密码应用与创新发展工作规划（2018-2022)》；
4. 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）；
5. 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）；
6. 《信息安全技术网络安全等级保护设计技术要求》（GB/T 25070-2019）；
7. 《中华人民共和国电子签名法》；
8. 《关键信息基础设施安全保护条例》；
9. 《网络安全等级保护条例（征求意见稿）》；
10. 《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》；
11. 《商用密码应用安全性评估管理办法（试行）》；
12. 《金融和重要领域密码应用与创新发展工作规划（2018-2022年）》 厅字【2018】36号；
13. 《国家政务信息化项目建设管理办法》国办发【2019】57号；
14. 《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。