{{sysname}}系统

密码应用方案

项目建设单位：

编制日期：

编制说明

1. 本应用方案由项目建设单位组织编写并提交。
2. 编写要求：
   1. 语言规范、文字简练、重点突出、描述清晰、内容全面、附件齐全；
   2. 采用A4幅面，上、下、左、右边距均为2.5厘米；正文内容仿宋四号字，1.5倍行距；一级标题黑体三号字，二级标题楷体小三号字，三级标题仿宋四号字，各级标题均加黑；
   3. 涉及到的外文缩写要注明全称；
   4. 材料内容不得涉及国家秘密。

本页留白，便于双面打印。

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 Xxx系统密码应用现状 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

2.1.1 系统名称 5

2.1.2 网络安全保护等级 5

2.1.3 系统用户情况 5

2.2 系统网络拓扑 5

2.2.1 体系架构 6

2.2.2 网络所在机房情况 7

2.2.3 网络边界划分 7

2.3 承载的业务情况 7

2.3.1 业务应用 7

2.3.2 信息种类 8

2.3.3 关键数据类型 8

2.4 系统软硬件构成 8

2.5 管理制度 9

3 密码应用需求分析 10

3.1 风险控制需求 10

3.1.1 物理和环境安全 10

3.1.2 网络和通信安全 11

3.1.3 设备和计算安全 13

3.1.4 应用和数据安全 15

3.1.5 密码安全管理 17

3.2 密码应用需求分析清单 18

4 密码应用设计目标及原则 20

4.1 设计目标 20

4.2 设计原则 20

4.3 设计依据 21

5 密码应用技术方案 23

5.1 密码应用技术框架 23

5.2 方案整体设计 24

5.2.1 密码基础服务层 25

5.2.2 密码协议 28

5.2.3 密钥管理 29

5.3 方案详细设计 31

5.3.1 物理和环境安全 31

5.3.2 网络和通信安全 32

5.3.3 设备和计算安全 35

5.3.4 应用和数据安全 37

5.4 密码应用部署 39

5.5 密码软硬件产品清单 40

5.6 安全与合规性分析 45

6 密码安全管理方案 48

6.1 管理制度 48

6.2 管理机构 49

6.3 建设运行 50

6.4 密钥管理 51

6.5 密码软硬件管理 52

6.6 人员管理 52

6.7 应急方案 53

6.7.1 潜在的安全事件分析 53

6.7.2 应急处置组织机构与职责 55

6.7.3 应急处置预案设计 57

7 实施保障方案 61

7.1 实施内容 61

7.1.1 软硬件开发及改造 61

7.1.2 系统集成 61

7.1.3 综合调试 61

7.1.4 试运行 62

7.1.5 最终验收 62

7.1.6 风险点及应对措施 62

7.2 实施计划 64

7.2.1 实施路线图 64

7.2.2 进度计划 65

7.3 保障措施 66

7.3.1 组织保障 66

7.3.2 人员保障 70

7.3.3 经费保障 70

7.3.4 质量保障 70

8 经费概算 73

# 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。**

## 国家政策法规要求

法律：

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. 《中华人民共和国电子签名法》；
4. 《中华人民共和国数据安全法》；
5. 《中华人民共和国电子商务法》；
6. 《中华人民共和国个人信息保护法》；
7. 《关键信息基础设施安全保护条例》；
8. 《商用密码管理条例（中华人民共和国国务院 第 273 号令）》

其他：

1. 《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》
2. 《政务信息系统密码应用与安全性评估工作指南》
3. 《金融和重要领域密码应用与创新发展工作规划（2018-2022年）》
4. 《关于促进网络安全产业发展的指导意见（征求意见稿）》
5. 《十部门关于印发加强工业互联网安全工作的指导意见的通知》
6. 《关于加强电力行业网络安全工作的指导意见》
7. 《工业互联网发展行动计划（2018-2020年）》
8. 《关于推动资本市场服务网络强国建设的指导意见》
9. 《公共互联网网络安全威胁监测与处置办法》
10. 《国家网络安全事件应急预案》【2020】119号；

## 系统密码应用现状

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}}系统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}}系统中存在广泛的安全隐患。如，系统设计初期使用账号口令实现在网络通信方面的通信实体的身份认证；且传输通道未采取数据保密性措施;设备计算安全方面仅通过账号口令登录操作系统系统进行运维管理；在应用数据方面仅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等。以上都意味着{{sysname}}系统未涉及商用密码安全应用。

## 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}}系统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}}系统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}}系统安全性要求，就成为了重中之重。{{sysname}}系统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。

1 国家网络安全战略所需

中共中央办公厅 国务院办公厅下发《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 明确指出：

【密码】是保障网络安全的核心技术和基础支撑，在维护国家安全、促进经济社会发展、保护人民群众利益中发挥着不可替代的重要作用。并部署在金融和重要领域推进密码全面应用，着力在构建自主可控信息技术体系中推进密码优先发展，构建以密码技术为核心、多种技术相互融合的新网络安全体系，建设以密码基础设施为支撑的新网络安全环境。

全面提升密码基础支撑能力，进一步完善法规制度，促进密码产业发展，规范密码应用，加强事中事后监管，完善密码应用安全性评估审查机制，建立商用密码测评认证和分类检测体系。

密码应用和密码测评成为落实国家网络安全战略的重要手段

2 技术所需

关键技术受制于人：中兴事件、华为事件，充分暴露出我国的网络技术及其他信息安全领域的技术受制于人。

密码技术不可控：密码技术作为网络安全的基础性核心技术，是信息保护和网络信任体系建设的基础，是保障网络空间安全的关键技术。但前期通用的国际密码算法频繁被爆出漏洞。

建设自主可控、安全领先、整体合规的密码体系迫在眉睫。

3 法治所需

我国社会全面进入法治社会，各行各业都需在法治框架下进行工作开展，信息化行业也不例外，《中华人民共和国网络安全法》就是现行信息化建设特别是网络安全工作的法律基础。在此基础上诸如《电子商务法》、《数据安全法》、《个人信息保护法》、《电子签名法》、《密码法》、《网络安全等级保护条例》等相关法律都在颁布、修订或制订中。

其中所有的法律或条例都明确要求要采用密码对系统、环境、数据等进行安全保护。

《密码法》明确指出：

【国家推进密码检测认证体系建设，制定密码检测、认证规则。密码检测、认证机构应当依法取得相关资质，并依照法律、法规的规定和密码检测、认证规则开展密码检测、认证。

国家对关键信息基础设施的密码应用安全性进行分类分级评估，按照国家安全审查的要求对影响或者可能影响国家安全的密码产品、密码相关服务和密码保障系统进行安全审查。】

《网络安全等级保护条例》对于密码更是做了详实的要求说明，密码要求涉及【物理环境、通信网络、区域边界、计算环境、管理中心、管理制度、管理机构、管理人员、建设管理、运维管理】十个方面，达到全覆盖。同时对【云计算、移动互联网、物联网、工业控制系统】这样新型的应用形式给出了密码应用要求。同时特别强调【在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖】。

密码应用和密码测评是落实《网络安全法》，践行依法治网重要保障

4 业务所需

业务在安全技术层面重点涉及保密、完整、可靠，在体系层面涉及认证、授权、责任认定，在结果层面涉及真实、关联、合法，而这三个层面的实现保障手段非密码技术莫属，而密码评测又是确实保障密码技术在落实“三三原则”时是否达到合规、正确、有效的直接可行方法（有明确的标准和规范）。

政务：

《密码法》的颁布实施，从法律层面为开展商用密码应用提供了根本遵循，《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。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》，决定对已经建成的政务系统进行密码应用改造。

密码保障业务安全、密码评测保障密码体系完善，二者有机协同，才能建立完善的网络安全环境

5 信创所需（可选）

我国“新基建”进程不断提速，因其深度依赖网络空间，促使网络安全成为“新基建”有序开展的关键环节。密码作为网络安全的核心技术和基础支撑，随之成为“新基建”底层信息安全的重要发展方向。

2019年以来，为摆脱对国外密码技术和产品的过度依赖，实现金融领域信息安全核心产品及系统的自主可控，我国已在金融行业逐步推进国密算法升级改造工作。2020年1月，《中华人民共和国密码法》正式施行，要求银行、证券、基金、银联、第三方支付等金融机构使用商用密码对关键信息基础设施进行保护。在金融行业“新基建”如火如荼开展的同时，如何为信息基础设施筑起一道数据安全的铜墙铁壁，成为银行关注重点。

总之：密码体系是网络安全环境的基础，密码评测是密码体系建设优良重要的考量，密码应用与密码评测工作同为网络安全环境建设的重要部分，意义重大。