{{sysname}}密码应用方案

项目名称： {{sysname}}

项目建设单位： {{sysunit}}

编制日期：{{sysdate}}

**目录**

[1背景 1](#_Toc167377439)

[1.1系统的建设规划 1](#_Toc167377440)

[1.2国家有关法律法规要求 1](#_Toc167377441)

[1.3与规划有关的前期情况描述 4](#_Toc167377442)

[1.4项目实施的必要性 5](#_Toc167377443)

[1.5信息系统相关的其他情况说明（如有） 7](#_Toc167377444)

[2系统概述 7](#_Toc167377445)

[2.1基本情况 7](#_Toc167377446)

[2.2计算平台现状 9](#_Toc167377447)

[2.3业务应用现状 13](#_Toc167377448)

[2.4密码应用现状 16](#_Toc167377449)

[2.5密码应用管理现状 18](#_Toc167377450)

[3. 密码应用需求分析 18](#_Toc167377451)

[3.1计算平台 19](#_Toc167377452)

[3.2业务应用 30](#_Toc167377453)

[3.3安全管理 34](#_Toc167377454)

[4. 安全目标及设计原则 35](#_Toc167377455)

[4.1安全目标 35](#_Toc167377456)

[4.2设计原则与依据 35](#_Toc167377457)

[5. 密码应用设计 37](#_Toc167377458)

[5.1密码应用技术框架 37](#_Toc167377459)

[5.2计算平台密码应用方案 44](#_Toc167377460)

[5.3密码支撑平台方案 53](#_Toc167377461)

[5.4业务应用密码应用方案 60](#_Toc167377462)

[5.5密码应用部署 71](#_Toc167377463)

[6. 安全管理方案 74](#_Toc167377464)

[6.1管理制度 74](#_Toc167377465)

[6.1 密码安全管理制度 75](#_Toc167377466)

[6.2 人员管理 78](#_Toc167377467)

[6.3 密钥管理 81](#_Toc167377468)

[6.4 建设运行 83](#_Toc167377469)

[6.5 密码软硬件及介质管理 84](#_Toc167377470)

[6.6 应急方案 86](#_Toc167377471)

[7. 安全与合规性分析 94](#_Toc167377472)

[8. 实施保障方案 99](#_Toc167377473)

[8.1 实施内容 99](#_Toc167377474)

[8.2实施计划 104](#_Toc167377475)

[8.3保障措施 106](#_Toc167377476)

[8.4经费概算 112](#_Toc167377477)

# 1 背景

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：明确系统的建设规划、国家有关法律法规要求、与规划有关的前期情况概述和项目实施的必要性,以及信息系统相关的其他情况说明。根据系统实际情况，示例写法如下：**

## 1.1系统的建设规划

## 1.2国家有关法律法规要求

### 1.2.1《中华人民共和国密码法》

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》，习近平主席签署第35号主席令予以公布，于2020年1月1日起正式施行。

根据密码法第二条的规定，本法中的密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。密码是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段，在我国革命、建设、改革各个历史时期，都发挥了不可替代的重要作用。密码就像网络空间的DNA，是构筑网络信息系统免疫体系和网络信任体系的基石，直接关系国家政治安全、经济安全、国防安全和信息安全，是保护党和国家根本利益的战略性资源，是国之重器。

在商用密码使用方面，一方面，为了保障关键信息基础设施安全稳定运行，维护国家安全和社会公共利益，密码法第二十七条要求关键信息基础设施必须依法使用商用密码进行保护并开展商用密码应用安全性评估，要求关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当依法通过国家网信办会同国家密码管理局等有关部门组织的国家安全审查。另一方面，密码法第八条规定公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

### 1.2.2《广东省省级政务信息化项目管理办法》（广东省特有）

为进一步落实“数字政府”改革建设工作任务，理顺政务信息化管理体制，推进“数字政府”管运分离建设模式，实现政务信息化项目由条块化管理向整体化管理转变、由政府投资建设向购买服务转变，根据广东省“数字政府”改革建设要求，2020年4月，《广东省省级政务信息化项目管理办法》正式印发。相关章节说明如下：

第九条省政务服务数据管理局依托管理平台牵头建立政务信息系统目录动态管理机制。具有以下情形之一的，相关运行维护、运营以及升级项目原则上不予立项。

（一）未纳入政务信息系统目录的系统；

（二）未按要求共享数据资源或者重复采集数据的政务信息系统；

（三）不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统；

（四）不符合国家安全可靠应用政策的政务信息系统。

### 1.2.3《网络安全等级保护条例（征求意见稿）》

第二十条“网络运营者应当落实数据分类、重要数据备份和加密等措施”；第四十七条“【非涉密网络密码保护】非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务”。

第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地区市的密码管理部门备案。

### 1.2.4《商用密码应用安全性评估管理办法》

第六条 法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统（以下简称重要网络与信息系统），其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

第八条 重要网络与信息系统建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。重要网络与信息系统运行前，其运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。网络与信息系统未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。

### 1.2.5《商用密码管理条例》

第四十一条 网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级，确定商用密码的使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。

第四十二条 商用密码应用安全性评估、关键信息基础设施安全检测评估、网络安全等级测评应当加强衔接，避免重复评估、测评。

## 1.3与规划有关的前期情况描述

{{xtsfxj}}

## 1.4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。

通过对某信息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}}安全性要求，就成为了重中之重。某信息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。

## 1.5信息系统相关的其他情况说明（如有）