上海市重要网络和信息系统

密码应用与安全性评估工作指南

（2024 版）

上海市密码管理局

2024 年 5 月

目 录

为规范和加强我市重要网络和信息系统的密码应用与安全性评估工作，特制定本工作指南。本指南发布之日起，《上海市重要网络和信息系统密码应用与安全性评估工作指南（2023 版）》同时废止。

一、法律法规和政策文件

（一）《中华人民共和国密码法》（2020 年 1 月实施）；

（二）《中华人民共和国网络安全法》（2017 年 6 月实施）；

（三）《中华人民共和国数据安全法》（2021 年 9 月实施）；

（四）《中华人民共和国个人信息保护法》（2021 年 11 月实施）；

（五）《关键信息基础设施安全保护条例》（2021 年 9 月实施）；

（六）《商用密码管理条例》（2023 年 7 月实施）；

（七）《政务信息系统政府采购管理暂行办法》（财库〔2017〕210 号，2018 年 1 月实施）；

（八）《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号，2020 年 2 月实施）；

（九）《商用密码应用安全性评估管理办法》（2023 年 11 月实施）；

（十）《关于进一步加强和规范关键信息基础设施密码应用工作的通知》（中共上海市委网络安全和信息化委员会办公室，上海市密码管理局，2020 年 3 月印发）；

（十一）《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》（公网安〔2020〕1960 号，2020 年 11 月实施）；

（十二）《关于规范和加强我市重要网络和信息系统密码应用与安全性评估工作的通知》（沪密局〔2021〕5 号，2021 年 5 月印发）；

（十三）中共上海市委办公厅 上海市人民政府办公厅印发《推进治理数字化转型实现高效能治理行动方案》的通知（沪委办发〔2021〕31 号，2021 年 10 月发布）；

（十四）《关于规范商用密码应用安全性评估结果备案工作的通知》（国密局字〔2021〕392号，2021年11月印发）；

（十五）国家发展改革委关于印发《“十四五”推进国家政务信息化规划》的通知（发改高技〔2021〕1898号，2021年12月发布）；

（十六）《上海市密码管理局关于印发<上海市电子政务云政务移动办公信息系统密码应用建设指南（暂行）>》的通知（沪密局〔2022〕1号，2022年1月印发）；

（十七）《关于进一步加强我市电子政务云及上云信息系统密码应用工作的通知》（沪密局〔2022〕5号，2022年2月印发）；

（十八）上海市人民政府办公厅关于印发《上海市政务云管理暂行办法》的通知（沪府办规〔2022〕6号，2022年4月印发）；

（十九）《关于印发医疗卫生机构网络安全管理办法的通知》（国卫规划发〔2022〕29号，2022年8月印发）；

（二十）《上海市市级数字化项目支出预算管理暂行办法》（沪经信推〔2022〕535号，2022年8月印发）；

（二十一）国家能源局关于印发《电力行业网络安全管理办法》的通知（国能发安全规〔2022〕100号，2022年11月发布）；

（二十二）《关于进一步规范商用密码应用安全性评估试点工作的通知》(国密局字〔2022〕454号，2022年12月印发）；

（二十三）《工业和信息化领域数据安全管理办法（试行）》（工信部网安〔2022〕166号，2022年12月发布）；

（二十四）《证券期货业网络和信息安全管理办法》（2023年5月实施）；

（二十五）《关于进一步加强我市重要网络和信息系统密码应用情况监督管理工作的通知》（沪密局〔2023〕7号，2023年5月印发）；

（二十六）《政务服务电子文件归档和电子档案管理办法》（国办发

〔2023〕26 号，2023 年 7 月印发）；

（二十七）《关于印发工业控制系统网络安全防护指南的通知》（工信部网安〔2024〕14 号，2024 年 1 月印发）；

（二十八）上海市人民政府关于印发《上海市落实〈全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案〉的实施方案》的通知（沪府发〔2024〕1 号，2024 年 2 月印发）；

（二十九）GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》（国家市场监督管理总局、国家标准化管理委员会,2019 年 12 月实施）；

（三十）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》（国家市场监督管理总局、国家标准化管理委员会,2019 年 12 月实施）；

（三十一）GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（国家市场监督管理总局、国家标准化管理委员会,2021 年 10 月实施）；

（三十二）GM/T 0116-2021《信息系统密码应用测评过程指南》（国家密码管理局,2022 年 5 月实施）；

（三十三）GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》（国家市场监督管理总局、国家标准化管理委员会，2024 年 4 月实施）；

（三十四）GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》（国家市场监督管理总局、国家标准化管理委员会，2024 年 4 月实施）；

（三十五）《政务信息系统密码应用与安全性评估工作指南（2020 版）》（中国密码学会密评联委会，2020 年 9 月发布）；

（三十六）《信息系统密码应用高风险判定指引》（中国密码学会密

评联委会,2021 年 12 月发布）；

（三十七）《政务领域政务云密码应用与安全性评估实施指南》（中国密码学会密评联委会,2024 年 4 月发布）；

（三十八）《政务领域政务服务平台密码应用与安全性评估实施指南》（中国密码学会密评联委会,2024 年 4 月发布）；

（三十九）国家其他相关政策文件。

二、密码应用与安全性评估范围

党政机关及事业单位、教育、卫生健康、国资、公安、电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、社会保障、国防科技工业等重要行业领域的非涉密网络和信息系统，以及法律法规和政策文件要求使用商用密码进行保护的其他网络和信息系统（包括但不限于关键信息基础设施、网络安全等级保护第三级及以上网络和信息系统、政务信息系统，以下简称重要网络和信息系统），应当落实密码应用工作有关要求，同步规划、同步建设、同步运行密码保障系统并定期进行密码应用安全性评估（以下简称密评）。

三、密码应用与安全性评估实施过程指南

本章节依据上述密码有关法律法规、管理办法和标准规范，给出重要网络和信息系统建设、使用、管理单位（以下简称责任单位）在信息系统规划、建设和运行阶段的密码应用与安全性评估实施过程指南。

（一）规划阶段

1、方案编制。责任单位在编制项目建议书、可行性研究报告与初步设计方案时，应当按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《密码应用基本要求》）、GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》（以下简称《密码应用设计指南》）和密码应用方案模板（见附录 1）同步编制密码应用方案。方案编制可参考

密码应用方案示例（见附录2、3）[1]。

2、方案评估。责任单位应当委托商用密码检测机构（以下简称检测机构）（见附录6）或组织专家评审会对密码应用方案进行评估。对于重大项目（包括投资金额3000万元（含）以上的；数字化转型年度重点工作所涉及的；“一网通办”、“一网统管”、相关重点领域的跨部门、跨层级、跨区域的；市委、市政府明确要求建设的数字化项目），责任单位应会同市密码管理局组织开展密码应用方案的评估工作，具体来说，责任单位若委托检测机构进行方案评估，需将评估结果报送市密码管理局复核；若组织专家评审会进行方案评估，市密码管理局相关工作人员列席专家评审会。评估结果作为项目立项的重要依据。

（二）建设阶段

1、建设实施。责任单位应当按照通过评估的密码应用方案建设密码保障系统，建设过程中涉及密码应用方案结构性调整的，应当委托检测机构或组织专家评审会对调整后的密码应用方案进行复评。

2、验收测评。项目建设完成后，责任单位应当根据项目验收要求，在验收前委托检测机构对项目进行密评[2]或密码应用测评。项目通过密评或密码应用测评是项目验收的必要条件。

（三）运行阶段

1、定期评估。在运行阶段，责任单位应当定期（每年至少一次）自行或委托检测机构对系统开展密评，并自密评报告形成后30日内将密评结果报市密码管理局备案（备案流程详见附录5）。对于未通过密评的系统，责任单位应当针对评估中发现的安全问题及时整改，整改完成后进行复评与备案。通过密评是项目运维经费审批的重要条件。

---

[1] 信息系统的密码应用等级一般按已定级或拟定级备案的网络安全等级保护的级别确定，未明确网络安全等级保护级别的信息系统，其密码应用等级默认为第三级。

[2] 对项目进行密评是指对项目中涉及的信息系统进行密码应用安全性评估。

2、应急评估。信息系统出现密码应用重大安全事件、重大调整或特殊紧急情况时，责任单位应当立即组织检测机构进行密评。

四、密码应用措施规划部署指南

本章节依据《密码应用基本要求》，结合当前密码技术、产品和服务的实际情况，给出了针对信息系统密码应用的措施建议。责任单位也可结合实际，自主选取适合的密码技术、产品和服务，以满足相关密码应用要求。

（一）通用要求

责任单位需从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个层面采用密码技术措施，建立安全的密钥管理方案，并采取有效的安全管理措施，对信息系统进行保护。

信息系统使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应遵循密码相关国家标准和行业标准，没有标准可遵循时可提请国家密码管理部门组织对相关算法、技术进行安全性审查。信息系统采用电子认证服务的，责任单位需选择具有电子认证服务资质的机构（若为政务信息系统，需选择具有电子政务电子认证服务资质的机构，详见附录7）。

（二）物理和环境安全

实现对信息系统所在机房等重要区域的物理防护，应具备的密码功能包括：

1、确认进入各重要区域人员的身份，防止无关和假冒人员进入；

2、保护电子门禁系统进出记录和视频监控音像记录的存储完整性，防止被非授权篡改。

实现上述功能，可结合信息系统的网络安全保护等级选用以下密码应用措施：

1、部署基于密码技术的安全门禁系统，对重要物理区域（如计算机集中办公区、设备机房等）出入人员的身份进行鉴别，并对安全门禁系统进出记录等数据进行完整性保护；

2、部署基于密码技术的视频监控系统，对视频监控音像记录等数据进行完整性保护。

（三）网络和通信安全

实现对信息系统与外部实体之间网络通信的安全防护，应具备的密码功能包括：

1、确认通信实体的身份，防止与假冒实体进行通信；

2、保护通信过程中的数据，防止数据被非授权篡改，防止重要数据泄露。

实现上述功能，可结合信息系统的网络安全保护等级选用以下密码应用措施：

1、部署 IPSec VPN 类产品，实现通信双方的身份鉴别，通信过程中重要数据的机密性、完整性保护；

2、在客户端部署智能密码钥匙和安全浏览器（含密码模块），在服务端部署 SSL VPN 类产品或服务，实现通信主体的身份鉴别，通信过程中重要数据的机密性、完整性保护。

（四）设备和计算安全

实现对信息系统中各类设备和计算环境的安全防护，应具备的密码功能包括：

1、对设备的特权用户（含系统管理员、安全管理员、审计管理员等）和普通用户的身份进行鉴别，防止假冒人员登录；

2、在远程管理时，对远程管理通道进行保护，防止与假冒实体进行通信，防止数据被非授权篡改，防止重要数据泄露；

3、保护计算机、服务器等设备中的系统资源访问控制信息（如设备配置信息、安全策略、资源访问控制列表等）、重要信息资源安全标记（如数据标签等）、日志记录（如系统日志、数据库日志等）和重要可执行程序（如重要应用程序等），防止被非授权篡改；保护重要可执行程序的来源真实性，防止假冒程序文件的加载。

实现上述密码功能，可结合信息系统的网络安全保护等级选用以下密码应用措施：

1、部署智能密码钥匙、智能 IC 卡或其它具备身份鉴别功能的密码产品，对登录的用户进行身份鉴别；

2、为远程管理搭建安全通信链路（如 SSL VPN 或 IPSec VPN 安全隧道）；

3、部署或使用签名验签服务器、服务器密码机等密码产品或服务，实现重要信息的完整性保护，以及重要可执行程序的完整性和来源真实性保护。

（五）应用和数据安全

实现对信息系统中应用及其数据的安全防护，应具备的密码功能包括：

1、鉴别应用系统的特权用户和普通用户的身份，防止假冒人员登录；

2、对应用系统的访问控制策略（如安全策略、资源访问控制列表等）、数据库表访问控制信息（如用户身份信息、数据库安全策略、用户权限列表等）、重要信息资源安全标记（如数据标签）等进行保护，防止被非授权篡改；

3、保护客户端与服务端之间、应用系统之间在非安全网络信道中传输的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息等），防止数据被非授权篡改，防止重要数据泄露；

4、保护存储的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息、业务审计日志等），防止数据被非授权篡改，防止重要数据

泄露；

5、保护应用系统中可能涉及法律责任认定的数据发送和接收操作，确保发送方和接收方无法否认已经发生的操作行为。

实现上述功能，可结合信息系统的网络安全保护等级选用以下密码应用措施：

1、部署证书认证系统或采用具有电子认证服务资质的机构提供的电子认证服务，为用户签发数字证书并配置智能密码钥匙、智能 IC 卡、移动智能终端密码模块等密码产品，基于数字签名机制，确保系统登录用户身份的真实性；

2、部署安全认证网关产品或服务，对访问应用系统的登录用户进行身份鉴别和权限控制，对客户端与服务端之间传输的数据进行机密性和完整性保护；

3、部署签名验签服务器、服务器密码机等产品或服务，对存储的重要数据进行机密性和完整性保护；

4、根据应用系统需要，部署签名验签、电子印章、时间戳等密码产品或服务，对收发的数据及相关操作记录进行签名，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

（六）密钥管理

在信息系统密码应用方案中，应包含完整的密钥管理方案，明确采用的密钥种类及管理环节，并设计安全的技术实现方式，确保密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等生存周期的安全。

密钥管理方案的技术实现应由经检测认证合格的密码产品提供，未采用该方式的密钥管理方案技术实现可提请国家密码管理部门组织开展安全性审查。

（七）安全管理

依据《密码应用基本要求》，信息系统的安全管理措施包括管理制度、人员管理、建设运行和应急处置4个方面。

管理制度方面，责任单位需建立相应的密码应用安全管理制度和操作规范，覆盖密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等相关内容。相关制度可针对密码保障系统单独制定，也可在已有的信息系统安全管理相关制度规范中体现。

人员管理方面，责任单位需根据信息系统密码管理工作需要设立密码管理及操作相关岗位，制订人员岗位责任、人员考核、人员培训、人员保密和调离等相关规定，并按照规定进行人员的配备与管理。

建设运行方面，责任单位需参照本指南要求制定信息系统密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，重点做好密码应用方案设计与评估、密码保障系统建设与密码应用测评、密评、以及相关闭环管理工作。

应急处置方面，责任单位应制定密码应用应急处置方案，需在项目建设阶段和系统运行阶段，分别明确典型紧急事件及应急处理处置方案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置。

附录 1

重要网络和信息系统密码应用方案模板

（方案编写示例参见附录 2、3）

××系统密码应用方案

系统名称：

系统建设单位：

编制日期：

编 制 说 明

1、本应用方案由系统建设单位组织编写。

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，各级标题均加粗；

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。

基本信息表

<table>
<tr><td colspan="6">责任单位</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td>所属省部密码管理部门</td><td colspan="5"></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td colspan="6">信息系统</td></tr>
<tr><td>系统名称</td><td colspan="5"></td></tr>
<tr><td>是否为关键信息基础设施</td><td colspan="5">☐已认定，所属安全保护工作部门：_____
☐未认定</td></tr>
<tr><td rowspan="2">网络安全等级保护定级和备案情况</td><td colspan="5">☐已定级备案，第__级（一至四），S__A__G__ 备案证明编号：
系统密码应用安全要求等级与等级保护定级是否一致：
☐是 ☐否，变化情况说明：</td></tr>
<tr><td colspan="5">☐未定级，系统密码应用按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》第三级信息系统要求</td></tr>
<tr><td>网络安全等级测评情况</td><td colspan="5">☐已测评
测评机构名称：_____ 测评时间：_____ 测评结论：
☐正在测评 测评机构名称：_____
☐未测评</td></tr>
<tr><td>商用密码应用安全性评估情况</td><td colspan="5">☐已评估
检测机构名称：_____ 评估时间：_____评估结论：
☐正在评估 检测机构名称：_____
☐未评估</td></tr>
<tr><td rowspan="2">系统是否依赖不在本系统范围内的云平台运行</td><td colspan="2">☐是
云平台名称：</td><td colspan="3">☐云平台已评估 ☐云平台未评估
检测机构名称：☐
评估时间： 评估结论：</td></tr>
<tr><td colspan="5">☐否</td></tr>
</table>

目　录

一级目录为黑体三号字体，二级目录为楷体小三号字体，三级目录为仿宋四号字体。每级目录缩进两个字符。

1 背景

包含系统的建设规划、国家有关法律法规要求、与规划有关的前期情况概述，以及该项目实施的必要性。

2 系统概述

2.1 基本情况

包含系统名称、系统责任主体单位情况（名称、地址、所属密码管理部门、单位类型等）、系统上线运行时间、系统用户情况（使用单位、使用人员、使用场景等）、是否为关键信息基础设施、等级保护定级和备案情况、网络安全等级测评情况、密码应用安全性评估情况等。

2.2 计算平台[3]现状

根据信息系统的部署方式（本地或上云）进行描述。

对于本地部署的情形，需包括以下内容：

1、物理和环境：包括机房或重要场所地点、系统部署情况、内外部环境和管理责任主体。

2、网络和通信：包括网络框架、网络边界划分、内外部数据交互情况、设备组成及实现功能、所采取的安全防护措施，并给出系统网络拓扑图。

3、设备和计算：包括系统软硬件构成（如服务器、用户终端、网络设备、存储设备、安全防护设备、密码设备等硬件资源和操作系统、数据库系统、应用中间件等软件资源）。

对于上云的情形，需包括以下内容：

[3] 计算平台是指承载业务应用的物理环境、网络环境和计算环境。物理环境提供机房、供电、通风、空调、门禁和监控等保障条件；网络环境为业务应用提供数据传输通道和通信设备；计算环境提供承载业务应用运行和数据存储的设备或服务。

1、物理和环境：云计算平台的场所地点，包括物理环境的部署位置、内外部环境以及运维主体等。

2、网络和通信：网络框架、网络边界划分、内外部数据交互情况、设备组成及实现功能、所采取的安全防护措施，并给出系统网络拓扑图。

3、设备和计算：包括但不限于云平台提供的服务器虚拟机、数据库管理系统、应用中间件、网络安全防护服务、密码服务等。

2.3 业务应用现状

需从以下两个方面进行描述：

1、业务应用的基本情况，包括承载的业务情况（系统承载的业务应用、业务功能和关键数据类型）和责任主体等。

2、描述信息系统包含的子应用，包含系统承载的业务应用、业务功能、信息种类、关键数据类型等。

2.4 密码应用现状

需从计算平台、密码支撑平台和业务应用三个方面描述密码应用现状。

2.4.1 计算平台

描述计算平台的密码应用现状，包括部署密码设施设备的基本情况（包括数量）、责任主体，以及密码支撑保障计算平台运行安全和管理安全的情况。

2.4.2 密码支撑平台[4]

根据部署方式（本地或上云）、是否已建设密码支撑平台进行描述，详见表1。

[4] 密码支撑平台：为计算平台上运行的各类业务应用提供密码支撑服务，该服务以接口的形式提供密码功能，供各业务应用调用，以解决各业务应用的安全问题。

表 1　密码支撑平台密码应用现状

部署方式	是否已建设密码支撑平台	现状描述
本地	在系统部署的机房中未建密码支撑平台	无
	在系统部署的机房中已建密码支撑平台	描述该密码支撑平台建设和使用情况，包括部署密码设施设备的基本情况（包括数量）、责任主体，以及该平台支撑的信息系统密码应用情况。
上云	在系统部署的云平台上未建云密码服务支撑平台	无
	在系统部署的云平台上已建云密码服务支撑平台	描述该密码支撑平台的基本情况及其支撑系统建设单位的情况，包括平台所提供的密码服务基本情况、责任主体，以及系统建设单位对应的 VPC[5] 内信息系统的密码服务使用情况。

2.4.3 业务应用

根据部署方式（本地或上云）、项目类型（新建或改造）进行描述，详见表 2。

表 2　业务应用密码应用现状

部署方式	项目类型	现状描述
本地	新建	无
	改造	描述本系统业务应用的密码应用现状，包括部署密码设施设备的基本情况和密码支撑保障应用和数据安全的情况。

[5] VPC（Virtual Private Cloud）：虚拟私有云，是一套为云服务器、云容器、云数据库等云上资源构建的逻辑隔离的、由用户自主配置和管理的虚拟网络环境。

上云	新建	无
	改造	描述本系统业务应用的密码应用现状，包括密码服务/产品使用情况和密码支撑保障应用和数据安全的情况。

2.5 密码应用管理现状

描述管理要求，包括信息系统管理制度、人员管理、建设运行和应急处置等内容。

3 密码应用需求分析

3.1 安全风险分析

结合信息系统现状和《密码应用基本要求》中对不同等级的信息系统提出的密码应用基本要求，从计算平台、业务应用两方面，梳理信息系统的重点保护对象；对密码应用方案涉及的计算平台、业务应用、安全管理进行安全风险分析。

3.2 密码应用需求

根据系统安全风险，结合《密码应用基本要求》中与该系统密码应用安全等级相对应的指标要求，确定风险控制措施、分析密码应用基本需求和密码应用特殊需求。对需求中不适用指标要求的部分，及使用非密码技术的风险控制措施以缓解信息系统存在的高风险，应作出相关说明。

4 安全目标及设计原则

4.1 安全目标

提出本方案所涉及对象的密码应用安全目标。

4.2 设计原则与依据

提出本方案的设计原则、遵循的法律法规、政策文件和标准规范等。

5 密码应用设计

5.1 密码应用技术框架

根据密码应用需求进行设计，包括密码应用技术框架图及框架说明，密码应用技术框架包括计算平台、密码支撑平台和业务应用密码应用架构等，综合描述各平台、系统之间的关系，能清晰展示密码应用整体技术框架。

5.2 计算平台密码应用方案

5.2.1 物理和环境安全

应包括密码功能设计和资源配置估算。

需描述本层密码保护的对象、采用的密码措施，包括选择的密码技术和标准、采用的密码设备、密码设备的部署位置和方式等，以及需使用的密码设备或密码资源估算情况。

5.2.2 网络和通信安全

说明同 5.2.1。

5.2.3 设备和计算安全

说明同 5.2.1。

5.3 密码支撑平台方案

对于新建密码支撑平台的情形，需按照以下要求给出相应的设计方案。

密码支撑平台为承载在计算平台上的各类业务应用提供密码服务，可选择采用经认证合格的密码支撑服务产品（如密码服务平台等），也可根据各类应用的密码需求、性能需求和责任主体的规划要求等，基于经认证合格的密码产品进行设计，设计的内容为：

1、密码服务机构的确定、接入方式和服务策略；

2、支持的密码体制和密码算法；

3、接口和功能遵循的标准；

4、提供的密码支撑方式（如租密码机方式、租密码服务器方式和租密码服务方式）；

5、提供的密码功能及接口（如实体鉴别、签名验签和加密解密），也可提供密码应用服务（如时间戳、电子印章和安全认证网关）；

6、部署的位置和方式（如部署的位置、部署的方式、使用和管理等内容），部署的方式包括全网统一部署和分租户分散部署；

7、接入计算平台的方式（如独立的形态，不占用计算平台的任何资源；非独立的形态，借用或租用计算平台的计算资源和网络资源）；

8、密钥管理方式，按责任主体的规划要求确定（如租户自行管理，支撑平台提供管理界面；租户委托管理，支撑平台代管密钥）；

9、支撑平台的自身安全性，包括密钥安全、访问安全、管理安全和租户间的隔离安全等。

对于已建密码支撑平台，若仅涉及已有密码设备/密码资源扩容，可不作描述，只需说明“不涉及密码支撑平台的建设或结构性调整，方案略”。否则，需根据新部署的密码设备/密码资源或其他结构性调整进行设计并给出相应的方案。

5.4 业务应用的密码应用方案

业务应用保护的对象是信息系统中的所有应用及其重要数据，按照《密码应用基本要求》中应用和数据安全对应等级的密码应用要求和各业务系统实际需求，对需要保护的对象进行密码应用方案设计，需从以下几个方面进行考虑：

1、按照系统规划，责任主体需求，现有或规划的密码功能提供模式，

确定密码体制；

2、梳理业务流程，根据流程安全需求，为关键环节设计密码保护机制；

3、梳理业务数据，根据数据安全需求，为重要数据设计密码保护机制；

4、梳理业务对象（如文件、证照、票据、病历、采集的数据和控制指令等），根据安全需求，为其设计密码保护机制；

5、根据角色和访问控制，为其权限和访问策略等设计密码保护机制；

6、根据审计策略，为日志记录设计密码保护机制；

7、使用加密功能的，需指明密码算法、加密模式、数据填充方式和密钥属性等；

8、使用签名功能的，需指明签名算法和签名机制（如签名内容、签名主体和签名位置等）；

9、使用完整性保护功能，需指明使用的算法和校验机制；

10、根据保护机制，修改被保护对象的数据结构，将上述内容添加到原数据结构中，使其成为带安全机制的数据结构；

11、实现保护机制用到的密码功能和用户登录用到的身份鉴别功能，由密码支撑平台提供，数据传输和数据存储安全，由计算平台负责，有单独需求（如互通且长期保存）或计算平台没有提供的，可设计信源加密机制。

根据确定的密码体制和密码应用方案，设计密钥管理策略，内容包括密钥的种类和用途，密钥的载体和保管方式，密钥的使用和更新，密钥的备份和恢复等，分别针对上述内容所涉及的人员、责任、介质、材料和流程等设计管理机制。密钥管理策略详见附录 4。

5.5 密码应用部署

应包含软硬件设备清单（软硬件设备均需包括已有的密码产品/密码服务清单）、部署示意图及说明等，新增加的密码设备/密码服务需要明确标

识。

5.6 密码应用功能模块

根据实际情况，如需开发密码应用功能模块，应进行说明及工作量估算。

6 安全管理方案

根据信息系统网络安全等级保护定级备案情况，按照部署的密码产品管理机制，设计安全管理方案，包括管理制度、人员管理、建设运行、应急处置方面的制度。

7 安全与合规性分析

对方案的适用情况、采取的密码保障措施、采取的缓解及替代性措施及自评结果进行说明（详见表 3）：

1、若指标为适用，说明采取的密码保障措施或未采取的密码保障措施的情况（如采取的缓解及替代性措施）；

2、针对适用的指标，存在部分保护对象不适用的情况，论证其不适用性；

3、若指标为不适用，说明其不适用的理由。

表 3　安全与合规性分析对照表

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
物理和环境安全	身份鉴别	宜				
	电子门禁记录数据存储完整性	宜				

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	视频监控记录数据存储完整性	宜				
网络和通信安全	身份鉴别	应				
	通信数据完整性	宜				
	通信过程中重要数据的机密性	应				
	网络边界访问控制信息的完整性	宜				
	安全接入认证	可				
设备和计算安全	身份鉴别	应				
	远程管理通道安全	应				
	系统资源访问控制信息完整性	宜				
	重要信息资源安全标记完整性	宜				
	日志记录完整性	宜				
	重要可执行程序完整性、重要可执行程序来源真实性	宜				
应用和	身份鉴别	应				

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
数据安全	访问控制信息完整性	宜				
	重要信息资源安全标记完整性	宜				
	重要数据传输机密性	应				
	重要数据存储机密性	应				
	重要数据传输完整性	宜				
	重要数据存储完整性	宜				
	不可否认性	宜				
管理制度	具备密码应用安全管理制度	应				
	密钥管理规则	应				
	建立操作规程	应				
	定期修订安全管理制度	应				
	明确管理制度发布流程	应				
	制度执行过程记录留存	应				

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
人员管理	了解并遵守密码相关法律法规和密码管理制度	应				
	建立密码应用岗位责任制度	应				
	建立上岗人员培训制度	应				
	定期进行安全岗位人员考核	应				
	建立关键岗位人员保密制度和调离制度	应				
建设运行	制定密码应用方案	应				
	制定密钥安全管理策略	应				
	依据密码应用方案实施建设	应				
	投入运行前进行密码应用安全性评估	应				
	定期开展密码应用安全性评估及攻防对抗演习	应				
应急处置	应急策略	应				
	事件处置	应				
	向有关主	应				

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	管部门上报处置情况					

8 实施保障方案

8.1 实施内容

应描述项目实施对象的边界及密码应用的范围、任务要求等。

实施内容包括但不限于采购、软硬件开发或改造、系统集成、综合调试、试运行等。

分析项目实施的重难点问题，提出实施过程中可能存在的风险点及应对措施。

8.2 实施计划

应包含实施路线图、进度计划、重要节点等。

按照施工进度计划确定实施步骤，并分阶段描述任务分工、实施主体、项目建设单位、阶段交付物等。

8.3 保障措施

应包含项目实施过程中的组织保障、人员保障、经费保障、质量保障和监督检查等措施。

8.4 经费概算

按照经费使用要求，对密码应用项目建设和产生的相关费用进行概算。采购的密码产品、密码服务应描述产品名称、服务类型和数量等，以及密码应用功能模块的开发适配工作量与费用等。

附录 2

重要网络和信息系统密码应用方案示例（本地部署）

电子公文处理系统密码应用方案

系统名称：电子公文处理系统

系统建设单位：

编制日期：

编 制 说 明

1、本应用方案由系统建设单位组织编写。

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，各级标题均加粗；

（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。

基本信息表

<table>
<tr><td colspan="6">责任单位</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td>所属省部密码管理部门</td><td colspan="5"></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td colspan="6">信息系统</td></tr>
<tr><td>系统名称</td><td colspan="5"></td></tr>
<tr><td>是否为关键信息基础设施</td><td colspan="5">☐已认定，所属安全保护工作部门：_____
☐未认定</td></tr>
<tr><td rowspan="2">网络安全等级保护定级和备案情况</td><td colspan="5">☐已定级备案，第__级（一至四），S__A__G__ 备案证明编号：
系统密码应用安全要求等级与等级保护定级是否一致：
☐是 ☐否，变化情况说明：</td></tr>
<tr><td colspan="5">☐未定级，本次密评按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》第三级信息系统要求</td></tr>
<tr><td>网络安全等级测评情况</td><td colspan="5">☐已测评
测评机构名称：_____
测评时间：_____
测评结论：_____
☐正在测评 测评机构名称：_____
☐未测评</td></tr>
<tr><td>商用密码应用安全性评估情况</td><td colspan="5">☐已评估
检测机构名称：_____ 评估时间：_____评估结论：
☐正在评估 检测机构名称：_____
☐未评估</td></tr>
<tr><td>系统是否依赖不在</td><td colspan="2">☐是
云平台名称：</td><td colspan="3">☐云平台已评估 ☐云平台未评估
检测机构名称：☐</td></tr>
</table>

本系统范围内的云平台运行		评估时间：　　评估结论：
	□否	

目　录

一级目录为黑体三号字，二级目录为楷体小三号字，三级目录为仿宋四号字。每级目录缩进两个字符。

（本方案主要以已建电子公文处理系统的密码应用改造为示例；对于新建信息系统的密码应用建设，将另行描述说明。）

1 背景

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。《密码法》《网络安全法》《商用密码管理条例》《关键信息基础设施安全保护条例》等多部法律法规的颁布实施，从法律层面为信息系统开展商用密码应用提供了根本遵循。

为落实相关法律法规对于信息系统密码应用的要求，结合《国家政务信息化项目建设管理办法》《政务信息系统政府采购管理暂行办法》等规范性依据，我单位决定对已运行的电子公文处理系统进行密码应用改造。

该系统部署于我单位自有机房，为我单位日常办公的重要信息系统，为单位各级领导及办公人员提供业务审批、公文签批、公文办理、公文管理等业务过程的信息化管理，实现各部门之间横向与纵向业务流转和内部信息资源共享。

通过对该系统的现状和密码应用需求分析，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《密码应用基本要求》）、GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》（以下简称《密码应用设计指南》），从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理等层面，设计了该系统密码应用的技术方案、安全管理方案和实施保障方案。

2 系统概述

2.1 基本情况

本系统于 XX 年 XX 月 XX 日上线运行，投资规模约 XX 万，责任单位为

XX 单位，使用人员为本单位各级领导及办公人员，系统部署模式为本地部署，用户可通过互联网、政务外网的 PC 终端访问。

2.2 计算平台现状

2.2.1 物理和环境

我单位电子公文处理系统部署于 XX 路 XX 号 XX 层 XX 室 XX 机房，机房由 XX 负责运维。机房入口处部署有安全门禁系统和视频监控系统，可实现对进入机房人员的身份鉴别，且机房有专人值守，外部人员进入机房需进行登记，并由工作人员全程陪同。

2.2.2 网络和通信

本系统网络拓扑如图1所示。

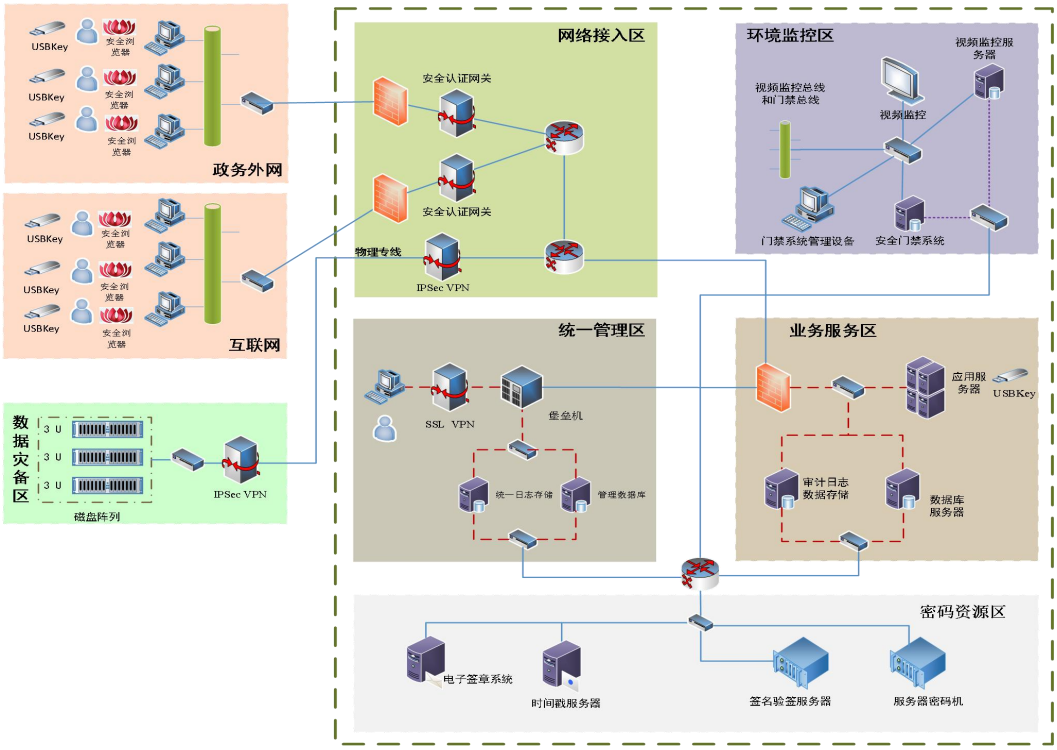


图 1 系统网络拓扑图

系统部署在我单位XX大楼XX层机房中，系统网络划分为网络接入区、业务服务区、统一管理区、环境监控区、密码资源区、数据灾备区等六个区。

网络接入区位于系统的网络边界，提供互联网和政务外网用户的访问接入，部署了防火墙、交换机、IPSec VPN、安全认证网关等设备。

业务服务区是系统的核心服务区域，主要部署系统应用服务器、数据存储服务器等设备，实现业务审批、公文签批、公文办理、公文管理等业务过程的信息化管理。

统一管理区主要部署远程运维管理终端、堡垒机、SSL VPN等设备，实现对系统中各设备的集中管理。

环境监控区主要部署安全门禁系统和视频监控系统，实现系统所在机房的物理安防管理。

数据灾备区主要部署磁盘阵列等设备，实现重要业务数据的备份。

2.2.3 设备和计算

本系统部署了服务器、磁盘阵列、堡垒机、防火墙、SSL VPN、安全认证网关、IPSec VPN 等硬件设备以及操作系统、数据库系统、应用中间件等软件产品，运维人员在单位内部通过堡垒机对服务器操作系统、数据库等设备进行远程运维管理。

2.3 业务应用现状

电子公文处理系统是我单位日常办公的重要信息系统，为单位各级领导及办公人员提供业务审批、公文签批、公文办理、公文管理等业务过程的信息化管理，实现各部门之间横向与纵向业务流转，以及内部信息资源共享，关键数据类型为电子公文数据。PC 终端通过浏览器登录访问系统。

2.4 密码应用现状

2.4.1 计算平台

在物理和环境安全方面，机房已部署基于 SM4 密码算法的安全门禁系统，实现对进出机房人员的身份鉴别；使用服务器密码机，通过 HMAC-S

M3 密码算法对机房进出记录和视频监控影像记录等数据进行完整性保护。（对于新建信息系统，需描述该系统拟部署机房提供的门禁系统和视频监控系统的密码应用情况。）

在网络和通信安全方面，在统一管理区已部署 SSL VPN，通过基于 SM2 密码算法的数字证书对通信服务端进行身份鉴别，并基于 TLCP 通信协议建立安全的远程运维通信通道；在网络接入区和数据灾备区分别部署 IPSec VPN，通过基于 SM2 密码算法的数字证书对跨区域通信双方进行身份鉴别，并基于 SM3、SM4 等密码算法建立安全的数据备份传输通道；在网络接入区边界部署安全认证网关，在互联网用户、政务外网用户与服务端通信前，通过基于 SM2 密码算法的数字证书对服务端进行身份鉴别，并基于 TLCP 通信协议建立安全的数据传输通道。（对于新建信息系统，需描述该系统拟部署机房提供的远程运维通信信道、数据灾备通信信道的密码应用情况。）

在设备和计算安全方面，系统管理员通过用户名+口令方式远程访问堡垒机，并基于 HTTPS 协议与堡垒机之间建立安全连接。应用服务器中重要可执行程序和文件均明文存储。服务器、数据库等设备日志和访问控制信息均明文存储。（对于新建信息系统，需描述该系统拟部署机房提供的设备远程运维管理通信信道的密码应用情况。）

计算平台密码应用现状如表 1 所示。

表 1 计算平台密码应用现状

序号	名称	数量	责任主体	密码应用情况
1	安全门禁系统	1	本单位基础设施部	实现运维人员进出物理机房的身份鉴别。
2	服务器密码机	1	本单位业务部	本设备由密码支撑平台提供,实现机房进出记录和视频监控影像记录等数据进行完整性保护。
3	SSL VPN	1	本单位基础设施部	实现远程运维管理通信数据的安全传输。
4	IPSec VPN	2	本单位基础设施部	实现灾备数据的安全传输。

5	安全认证网关	2	本单位业务部	本设备由密码支撑平台提供,实现业务应用访问的网络安全通信。

2.4.2 密码支撑平台

本单位已建设密码支撑平台，实现对人事管理系统、档案管理系统等信息系统的密码支撑。本系统将与已建信息系统共享使用密码资源，现状如表 2 所示。

表 2 密码支撑平台密码应用现状

序号	名称	数量	责任主体	密码支撑情况
1	安全认证网关	2	本单位业务部	提供业务应用访问的身份鉴别服务;同时支持业务应用访问的网络和通信安全。 支撑的系统包括：人事管理系统、档案管理系统和本系统。
2	服务器密码机	1	本单位业务部	提供数据加解密服务和完整性保护服务,实现业务应用的数据存储机密性和完整性;计算平台的完整性也可复用该设备密码功能。 支撑的系统包括：人事管理系统、档案管理系统和本系统。
3	签名验签服务器	1	本单位业务部	提供签名验签服务,实现业务应用用户访问权限控制列表、用户身份鉴别数据和业务日志数据的完整性保护。 支撑的系统包括：人事管理系统、档案管理系统和本系统。
4	安全电子签章系统	1	本单位业务部	提供安全电子签章服务,实现档案管理存档操作行为的不可否认性。 支撑的系统包括：档案管理系统、本系统。
5	时间戳服务器	1	本单位业务部	提供时间戳服务，配合安全电子签章系统，实现档案管理存档操作行为的不可否认性。 支撑的系统包括：人事管理系统、档案管理系统和本系统。

2.4.3 业务应用

系统互联网、政务外网用户均通过用户名+口令方式登录；系统用户身份鉴别数据、系统内流转的电子公文数据等重要数据均明文传输、存储；系统应用访问控制信息、业务日志数据等重要数据均明文存储；电子公文数据未使用密码技术实现不可否认性保护。

2.5 密码应用管理现状

我单位根据等保 2.0 管理制度要求，制定了通用的《单位信息安全管理制度汇编》，该制度汇编内容涉及安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等 5 个方面的安全管理要求。

3 密码应用需求分析

3.1 安全风险分析

根据《密码应用基本要求》《密码应用设计指南》，结合密码应用现状，从计算平台、业务应用、安全管理等层面，围绕重要数据、系统角色、关键软硬件设备、关键业务环节、关键操作行为等重点对象,对本系统进行风险分析。（对于新建信息系统，需分析描述系统的潜在安全风险。）

以下仅为示例，针对具体系统应给出更为详尽的风险分析。

3.1.1 重点保护对象分析

本系统计算平台、业务应用等层面重点保护对象如表 3 所示。

表3 系统各层面重点保护对象

序号	安全层面		保护对象	说明
1	计算平台	物理和环境安全	机房电子门禁系统及其数据	无
			机房视频监控数据	
2		网络和通信安全	互联网访问应用通信信道	从互联网访问应用的通信信道
3			政务外网访问应用通信信道	从政务外网访问应用的通信信道
4			远程运维通信信道	通过远程管理终端对系统内设备进行运维的通信信道
5			数据灾备通信信道	进行数据备份的通信信道
6		设备和计算安全	服务器	应用服务器和数据库服务器
7			重要可执行程序和文件	关键业务应用软件安装包、升级包等
8				系统关键组件

序号	安全层面		保护对象	说明
9			数据库	无
10			堡垒机	用于集中运维管理
11			密码产品	无
12	业务应用	应用和数据安全	应用用户	政务外网用户
13				互联网用户
14			重要数据	用户登录口令（用户身份鉴别数据）
15				系统中通知、报告、批复等电子公文数据
16				系统业务日志数据
17				系统访问控制信息
18			操作行为	系统重要电子公文数据的签发行为

3.1.2 计算平台安全分析

3.1.2.1 物理和环境安全分析

系统所在机房已符合密码应用要求，本节略。

（对于新建机房，以下描述仅供参考：机房存在非授权人员进入物理环境，对软硬件设备和数据进行直接破坏的风险。）

3.1.2.2 网络和通信安全分析

系统互联网访问应用通信信道、政务外网访问应用通信信道、远程运维通信信道、数据灾备通信信道等已符合密码应用要求，本节略。

（对于新建信息系统，以下描述仅供参考：

1、业务服务区和数据灾备区之间的通信数据存在被非授权截取、非授权篡改风险；

2、政务外网和互联网用户访问应用时存在通信主体身份被假冒，通信数据在信息系统外部被非授权截取、非授权篡改风险。）

3.1.2.3 设备和计算安全分析

1、系统管理员通过远程运维管理终端访问堡垒机时，未使用密码技术对管理员登录进行身份鉴别，未使用合规的密码技术保护远程管理通道安

全，存在设备被非授权人员登录、身份鉴别数据被非授权获取或非授权使用等风险；

2、目前系统应用服务器中重要可执行程序和文件未使用密码技术进行完整性和来源真实性保护，存在重要可执行程序或文件被非授权篡改、来源不可信风险；

3、目前系统中服务器、数据库等设备日志和访问控制信息未使用密码技术进行完整性保护，存在设备日志记录和访问控制信息被非授权篡改的风险。

（对于新建信息系统，以下描述仅供参考：

1、对设备进行远程运维管理时，存在设备被非授权人员登录、身份鉴别数据被非授权获取或非授权使用等风险；

2、系统应用服务器存在重要可执行程序或文件被非授权篡改、来源不可信等风险；

3、系统中服务器、数据库等设备存在日志记录和访问控制信息被非授权篡改的风险。）

3.1.3 业务应用安全分析

1、系统互联网、政务外网用户未使用密码技术进行身份鉴别，存在应用系统被非授权人员登录风险；

2、系统用户身份鉴别数据、系统内流转的电子公文数据等重要数据未使用密码技术实现数据传输和存储的机密性、完整性保护，存在身份鉴别数据、电子公文数据被窃取和非授权篡改风险；

3、系统应用访问控制信息、业务日志数据等重要数据未使用密码技术进行完整性保护，存在应用访问控制信息、业务日志数据被非授权篡改风险；

4、未使用密码技术对系统内流转的电子公文数据的签发进行不可否认性保护，存在数据发送者否认其操作行为的风险。

（对于新建信息系统，以下描述仅供参考：

1、系统应用存在被非授权人员登录风险；

2、用户身份鉴别数据、系统内流转的电子公文数据等重要数据在数据传输和存储过程中存在被窃取和非授权篡改风险；

3、应用访问控制信息、业务日志数据等重要数据存在被非授权篡改风险；

4、在系统内进行电子公文数据流转时，存在数据发送者否认其操作行为的风险。）

3.1.4 安全管理分析

本系统未按照《密码应用基本要求》安全管理要求，从密钥管理、人员管理、建设运行、应急处置等方面制定相应的密码应用安全管理制度，存在由于管理制度和密钥管理策略不完善、管理流程不健全、职责不明确等导致的密钥泄露、数据泄露等风险。

（对于新建信息系统，以下描述仅供参考：存在密码应用安全管理制度缺失或不合规导致的密钥泄露、数据泄露等风险。）

3.2 密码应用需求

根据安全风险分析，并对照《密码应用基本要求》中三级指标要求和《密码应用设计指南》，梳理出本系统密码应用需求清单，如表 4 所示。

表 4 系统密码应用需求清单

安全层面		指标要求	系统密码应用需求	不适用说明/缓解风险的措施说明
计算平台安全	物理和环境安	身份鉴别	已符合密码应用要求。	无
		电子门禁记录数据完整性	已符合密码应用要求。	无

安全层面		指标要求	系统密码应用需求	不适用说明/缓解风险的措施说明
	全	视频监控记录数据完整性		
		密码服务	不适用。	无密码服务需求
		密码产品	采用的密码产品应达到 GB/T 37092-2018 二级及以上安全要求。	无
	网络和通信安全	身份鉴别	已符合密码应用要求。	无
		通信数据完整性	已符合密码应用要求。	无
		通信过程中重要数据的机密性		无
		网络边界访问控制信息的完整性	已符合密码应用要求。	无
		安全接入认证	不适用。	无外部设备接入本系统的需求
		密码服务	采用的数字证书由具有电子认证服务资质的机构签发。	无
		密码产品	采用的密码产品应达到 GB/T 37092-2018 二级及以上安全要求。	无
	设备和计算安全	身份鉴别	管理员通过远程运维管理终端访问堡垒机、服务器、数据库、密码产品等设备时，对其身份真实性进行识别和确认，防止假冒人员登录。	无
		远程管理通道安全	在设备实施远程运维管理时，对设备的运维管理通道进行保护，防止运维管理数据泄漏。	无
		系统资源访问控制信息完整性	保护系统中服务器、数据库、密码产品等设备访问控制信息的完整性，防止被非授权篡改。	无

安全层面		指标要求	系统密码应用需求	不适用说明/缓解风险的措施说明
		重要信息资源安全标记完整性	不适用。	设备没有安全标记
		日志记录完整性	保护系统中服务器、数据库、密码产品等设备日志记录的完整性，防止被非授权篡改。	无
		重要可执行程序完整性、来源真实性	保护应用服务器等设备中重要可执行程序的完整性和来源真实性，防止被非授权篡改。	无
		密码服务	不适用。	无密码服务需求
		密码产品	采用的密码产品应达到 GB/T 37092-2018 二级及以上安全要求。	无
业务应用安全	应用和数据安全	身份鉴别	确认应用系统用户身份的真实性，防止假冒人员登录。	无
		访问控制信息完整性	对应用系统的访问权限控制列表进行完整性保护，防止被非授权篡改。	无
		重要信息资源安全标记完整性	不适用。	应用没有安全标记。
		数据传输机密性	保护政务外网、互联网客户端与服务端之间传输和存储的用户登录身份鉴别信息、电子公文数据等重要数据的机密性和完整性，防止数据泄露给非授权的个人、进程等。保护系统业务日志数据的完整性，防止该数据被非授权篡改。	无
		数据存储机密性		
		数据传输完整性		
		数据存储完整性		
		不可否认性	保护系统中流转的电子公文数据的不可否认性，确保发送方对已经发生的操作行为无法否认。	无
		密码服务	采用的数字证书由具有电子认证服务资质的机构签发。	无
		密码产品	采用的密码产品，应达到 GB/T 37092-2018 二级及以上安全要求。	无

4 安全目标及设计原则

4.1 安全目标

综合考虑本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用需求，充分利用已有密码资源，设计合规、正确、有效的密码应用技术方案，以达到《密码应用基本要求》中三级指标要求，并为后续密码保障体系建设、密码应用测评和密码应用安全性评估奠定坚实基础。

4.2 设计原则和依据

本系统密码应用技术方案设计应遵循以下原则：

1、总体性原则。根据本系统密码应用安全要求等级，结合密码应用需求和预期目标，对本系统密码应用开展顶层设计，形成涵盖技术、管理和实施保障的整体方案，为在系统中落实密码应用相关要求奠定基础。

2、完备性原则。围绕本系统实际业务应用与安全要求等级，通过自上而下的体系化设计，综合考虑物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等多个层面密码应用需求，设计本系统密码应用技术方案。

3、经济性原则。结合本系统规模，在合理、够用的前提下，考虑本系统规模、并发数、冗余、部署方式、管理模式等情况，充分利用已有密码资源，设计符合《密码应用基本要求》的密码应用技术方案，确保系统密码应用改造投资合理，规模适度，避免资金浪费和过度保护。

主要设计依据：

●GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》

●GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

●GB/T 32922-2023《信息安全技术 IPSec VPN 安全接入基本要求与实

施指南》

- ●GB/T 38636-2020《信息安全技术 传输层密码协议（TLCP）》
- ●GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》
- ●GB/T 38541-2020《信息安全技术 电子文件密码应用指南》
- ●GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》
- ●GB/T 37092-2018《信息安全技术 密码模块安全要求》
- ●GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》
- ●GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》
- ●GB/T 33482-2016《党政机关电子公文系统建设规范》
- ●GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
- ●GM/T 0033-2023《时间戳接口规范》
- ●GM/T 0030-2014《服务器密码机技术规范》
- ●GM/T 0026-2023《安全认证网关产品规范》
- ●GM/T 0025-2023《SSL VPN 网关产品规范》
- ●GM/T 0023-2023《IPSec VPN 网关产品规范》

5 密码应用设计

5.1 密码应用技术框架

本系统密码应用技术框架如图2所示。

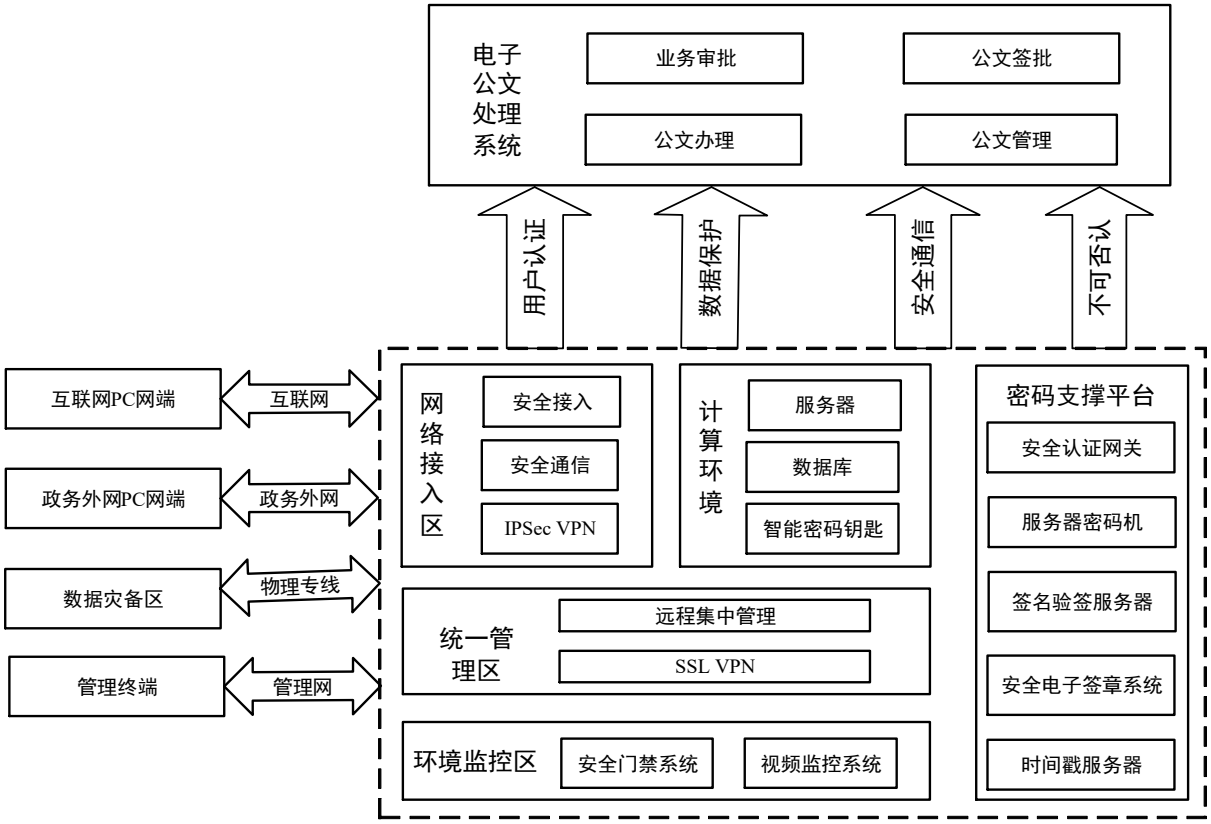


图 2 系统密码应用技术框架

本系统密码应用技术框架涉及计算平台、密码支撑平台、业务应用系统：

1、计算平台：是承载业务应用的物理环境、网络环境和计算环境。物理环境提供机房、供电、通风、空调、门禁和监控等保障条件；网络环境为业务应用提供数据传输通道和通信设备；计算环境提供承载业务应用运行和数据存储的设备或服务。计算平台中部署的密码设备,为计算平台的运行安全和管理安全提供密码保障。

2、密码支撑平台：基于部署的密码产品，为计算平台上运行的各类业务应用提供密码支撑服务，该服务以接口的形式提供密码功能，供各业务应用调用，以解决各业务应用的安全问题。

3、电子公文处理系统：是运行在计算平台上，实现电子公文处理业务的应用系统，其密码应用安全按照《密码应用基本要求》中的应用和数据

安全要求设计。本系统需要使用的密码功能，由密码支撑平台提供。

5.2 计算平台密码应用方案

5.2.1 物理和环境安全

（一）密码功能设计

本单位已建设安全门禁系统和视频监控系统，方案略。

（二）资源配置估算

本系统复用部署机房已有安全门禁系统、视频监控系统和服务器密码机。

5.2.2 网络和通信安全

（一）密码功能设计

本单位已部署安全认证网关、SSL VPN和IPSec VPN，仅涉及已有密码设备/密码资源扩容，方案略。

（二）资源配置估算

本系统面向互联网和政务外网提供服务，系统性能测算如下：

系统最大并发连接数：1900 个；

系统最大流量：500Mbps；

系统最大每秒事务数（TPS）：3400 次；

系统每秒最大备份数据量：300Mbps。

1、安全认证网关估算

根据密码资源使用现状，结合本系统性能测算数据，对安全认证网关的总体需求进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2,C1/C2)/(1-D)，说明如下：

X：安全认证网关估算数量。

A1：系统最大并发连接数。

A2：安全认证网关支持最大并发连接数。

B1：系统最大流量（Mbps）。

B2：安全认证网关支持最大流量（Mbps）。

C1：最大每秒事务数（TPS）。

C2：安全认证网关支持最大每秒事务数（TPS）。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

安全认证网关一般按最大并发连接数、最大流量、最大每秒事务数这三项指标来计算性能负载，三项中资源使用占比最大的主要性能指标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 5、6 所示：

表 5 互联网安全认证网关数量估算表

应用系统	系统最大并发连接数（个）A1	安全认证网关支持最大并发连接数（个）A2	系统最大流量(Mbps) B1	安全认证网关支持最大流量(Mbps) B2	最大每秒事务数（TPS）C1	安全认证网关支持最大每秒事务数（TPS）C2	密码设备计算负荷的冗余边界 D	安全认证网关估算数量 X
人事管理系统	1500	5500	400	2000	3000	25000	0.2	0.34
档案管理系统	2340	5500	300	2000	6000	25000	0.2	0.53
电子公文处理系统	1900	5500	500	2000	3400	25000	0.2	0.43
总计								1.3
安全认证网关基本需求（向上取整）								2
高可用需求数量								1
总计（安全认证网关需求总数）								3

表 6 政务外网安全认证网关数量估算表

应用系统	系统最大并发连接数（个）A1	安全认证网关支持最大并发连接数（个）A2	系统最大流量(Mbps) B1	安全认证网关支持最大流量(Mbps) B2	最大每秒事务数（TPS）C1	安全认证网关支持最大每秒事务数（TPS）C2	密码设备计算负荷的冗余边界 D	安全认证网关估算数量 X
人事管理系统	1500	5500	400	2000	3000	25000	0.2	0.34
档案管理系统	2340	5500	300	2000	6000	25000	0.2	0.53
电子公文处理系统	1900	5500	500	2000	3400	25000	0.2	0.43
总计								1.3
安全认证网关基本需求（向上取整）								2
高可用需求数量								1
总计（安全认证网关需求总数）								3

根据上述估算表中安全认证网关需求总量（互联网 3 台、政务外网 3 台）与实际数量（互联网 1 台、政务外网 1 台）比较可知，本系统需新增 4 台安全认证网关（互联网 2 台、政务外网 2 台）。

2、SSL VPN 估算

SSL VPN 用于系统运维，考虑本系统未增加运维规模，故复用原有 SSL VPN。

3、IPSec VPN 估算

根据密码资源使用现状，结合本系统性能测算数据，对 IPSec VPN 的使用进行综合估算。估算公式为 X=(A1/A2)/(1-D)，说明如下：

X：IPSec VPN 估算数量。

A1：系统最大备份流量(Mbps)。

A2：IPSec VPN 每秒最大加密流量(Mbps)。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 7 所示：

表 7 IPSec VPN 数量估算表

应用系统	系统最大备份流量(Mbps)A1	IPSec VPN 每秒最大加密流量(Mbps)A2	密码设备计算负荷的冗余边界 D	IPSec VPN 估算数量 X
人事管理系统	200	800	0.2	0.31
档案管理系统	400	800	0.2	0.63
电子公文处理系统	300	800	0.2	0.47
			总计	1.41
			IPSec VPN 基本需求（向上取整）	2
			高可用需求数量	1
			总计（IPSec VPN 需求总数）	3

根据上述估算表中单侧 IPSec VPN 需求总量为 3 台，双侧部署 IPSec VPN 需求总量为 6 台，与实际数量 2 台比较可知，本系统需新增 4 台 IPSec VPN。

4、电子认证服务

本系统采用独立域名发布，原有域名证书无法复用，需申请 1 张域名证书。新增 4 台安全认证网关，需申请 4 张设备证书。

5.2.3 设备和计算安全

（一）密码功能设计

1、向系统远程运维管理员配发智能密码钥匙（载有 SM2 密码算法数字证书），通过使用 SSL VPN（已部署于统一管理区）和智能密码钥匙，对堡垒机的管理员用户进行身份鉴别，并对远程运维管理通道进行保护，防止非授权人员登录、远程运维管理信息被非授权窃取或篡改。

2、通过使用智能密码钥匙（载有SM2密码算法数字证书）对应用服务器中重要可执行程序和文件进行数字签名，使用或读取这些程序和文件时，通过智能密码钥匙进行验签以确认其完整性和来源真实性；公钥存放在智能密码钥匙中。

3、通过调用服务器密码机，使用HMAC-SM3密码算法对服务器、数据库等设备日志和访问控制信息进行完整性保护。

密码产品的设备和计算安全相关指标要求由该产品自身实现。

（二）资源配置估算

本层面需配置服务器密码机 1 台（与物理和环境层面共用），SSL VPN 1 台（与网络和通信层面共用），智能密码钥匙若干，安全浏览器（含密码模块）若干。

以上资源复用现有密码资源，无需新增。

5.3 密码支撑平台方案

本单位已建设密码支撑平台，仅涉及已有密码设备/密码资源扩容，不涉及密码支撑平台的建设或结构性调整，密码支撑平台方案略。

（对于新建密码支撑平台的情形，需根据新部署的密码设备/密码资源或其他结构性调整进行设计并给出相应的方案。）

5.4 业务应用的密码应用方案

（一）密码功能设计

1、在互联网和政务外网PC端部署安全浏览器（含密码模块）并向相关用户配发智能密码钥匙，签发基于SM2密码算法的数字证书，通过调用密码支撑平台的身份鉴别服务，基于SM2密码算法的签名验签机制，对互联网和政务外网PC端用户进行身份鉴别，防止非授权人员访问应用；通信数据的安全防护由网络和通信层面的安全认证网关及其承载的加密通信信道实

现。

2、通过调用密码支撑平台的服务器密码机，分别使用SM4-CBC算法和基于SM2密码算法的数字信封对互联网和政务外网PC端用户身份鉴别数据、电子公文数据进行存储机密性保护，实现身份鉴别数据、电子公文数据等重要数据的防泄露。

3、通过调用密码支撑平台的签名验签服务器，使用SM2密码算法对应用用户访问权限控制列表、用户身份鉴别数据和业务日志数据的进行完整性保护，防止被非授权用户篡改。

4、通过调用密码支撑平台提供的电子签章系统、时间戳服务器，基于SM2密码算法对电子公文数据进行数字签名，并加盖时间戳，实现电子公文数据的完整性保护以及文件签发人操作行为的不可否认性。

（二）资源配置估算

本系统面向互联网和政务外网提供服务，系统性能测算如下：

系统每秒最大加解密数据量：272Mbps;

系统签名验签每秒最大签名次数：800次，每秒最大验签次数：700次;

系统时间戳每秒最大签名次数：800次，每秒最大验签次数：700次;

系统电子签章每秒最大盖章次数：300次，每秒最大验章次数：200次。

1、服务器密码机估算

根据密码资源使用现状，结合本系统性能测算数据，对服务器密码机的使用进行综合估算。估算公式为 X=(A1/A2)/(1-D)，说明如下：

X：服务器密码机估算数量。

A1：系统每秒最大加解密数据量(Mbps)。

A2：服务器密码机每秒最大加解密数据量(Mbps)。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如

表 8 所示：

表 8 服务器密码机数量估算表

应用系统	系统每秒最大加解密数据量(Mbps)A1	服务器密码机每秒最大加解密数据量(Mbps)A2	密码设备计算负荷的冗余边界 D	服务器密码机估算数量 X
人事管理系统	180	875	0.2	0.26
档案管理系统	240	875	0.2	0.34
电子公文处理系统	272	875	0.2	0.39
总计				0.99
服务器密码机基本需求（向上取整）				1
高可用需求数量				1
总计（服务器密码机需求总数）				2

根据上述估算表中服务器密码机需求总量 2 台与实际数量 1 台比较可知，本系统需新增 1 台服务器密码机。

2、签名验签服务器估算

根据密码资源使用现状，结合本系统性能测算数据，对签名验签服务器的使用进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2)/(1-D)，说明如下：

X：签名验签服务器估算数量。

A1：系统每秒最大签名次数。

A2：签名验签服务器支持每秒最大签名次数。

B1：系统每秒最大验签次数。

B2：签名验签服务器支持每秒最大验签次数。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

签名验签服务器一般按签名验签服务器支持每秒最大签名次数和验签次数这两项指标来计算性能负载，两项中资源使用占比较大的主要性能指

标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 9 所示：

表 9 签名验签服务器数量估算表

应用系统	系统每秒最大签名次数 A1	签名验签服务器支持每秒最大签名次数 A2	系统每秒最大验签次数 B1	签名验签服务器支持每秒最大验签次数 B2	密码设备计算负荷的冗余边界 D	签名验签服务器估算数量 X
人事管理系统	500	9000	1000	6000	0.2	0.21
档案管理系统	1000	9000	3000	6000	0.2	0.63
电子公文处理系统	800	9000	700	6000	0.2	0.15
总计						0.99
签名验签服务器基本需求（向上取整）						1
高可用需求数量						1
总计（签名验签服务器需求总数）						2

根据上述估算表中签名验签服务器需求总量 2 台与实际数量 1 台比较可知，本系统需新增 1 台签名验签服务器。

3、时间戳服务器估算

根据密码资源使用现状，结合本系统性能测算数据，对时间戳服务器估算的使用进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2)/(1-D)，说明如下：

X：时间戳服务器估算数量。

A1：系统每秒最大签名时间戳次数。

A2：时间戳服务器支持每秒最大签名时间戳次数。

B1：系统每秒最大验证时间戳次数。

B2：时间戳服务器支持每秒最大验证时间戳次数。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码

设备计算负荷的水位线）。

时间戳服务器一般按时间戳服务器支持每秒最大签名和验证时间戳次数这两项指标来计算性能负载，两项中资源使用占比较大的主要性能指标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 10 所示：

表 10 时间戳服务器数量估算表

应用系统	系统每秒最大签名次数 A1	时间戳服务器支持每秒最大签名时间戳次数 A2	系统每秒最大验签次数 B1	时间戳服务器支持每秒最大验签时间戳次数 B2	密码设备计算负荷的冗余边界 D	时间戳服务器估算数量 X
人事管理系统	500	9000	1000	6000	0.2	0.21
档案管理系统	1000	9000	3000	6000	0.2	0.63
电子公文处理系统	800	9000	700	6000	0.2	0.15
总计						0.99
时间戳服务器基本需求（向上取整）						1
高可用需求数量						0
总计（时间戳服务器需求总数）						1

根据上述估算表中时间戳服务器需求总量 1 台与实际数量 1 台比较可知，原有设备可覆盖本系统需求，无需新增设备。

4、电子签章系统估算

根据密码资源使用现状，结合本系统性能测算数据，对电子签章服务器的使用进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2)/(1-D)，说明如下：

X：电子签章系统设备估算数量。

A1：系统每秒最大盖章次数。

A2：电子签章服务器支持每秒最大盖章次数。

B1：系统每秒最大验章次数。

B2：电子签章服务器支持每秒最大验章次数。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

电子签章系统一般按电子签章系统支持每秒最大盖章和验章次数这两项指标来计算性能负载，两项中资源使用占比较大的主要性能指标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 11 所示：

表 11 电子签章系统数量估算表

应用系统	系统每秒最大盖章次数 A1	电子签章系统支持每秒最大盖章次数 A2	系统每秒最大验章次数 B1	电子签章系统支持每秒最大验章次数 B2	密码设备计算负荷的冗余边界 D	电子签章系统估算数量 X
档案管理系统	300	800	100	1200	0.2	0.47
电子公文处理系统	300	800	200	1200	0.2	0.47
总计						0.94
电子签章服务器基本需求（向上取整）						1
高可用需求数量						0
总计（电子签章服务器需求总数）						1

根据上述估算表电子签章系统需求总量 1 台与实际数量 1 台比较可知，原有设备可覆盖本系统需求，无需新增设备。

5、电子认证服务

新增 1 台签名验签服务器，需申请 1 张设备证书。

（三）密钥管理安全

本系统使用的域名证书和设备证书均由具有电子认证服务资质的机构签发。

本系统选用经检测认证合格的安全浏览器（含密码模块）、智能密码

钥匙等商用密码产品，并根据这些产品提供的安全策略,制定密钥管理方案，严格遵照该方案进行使用和实施。

5.5 密码应用部署

本系统密码应用部署如图 3 所示。

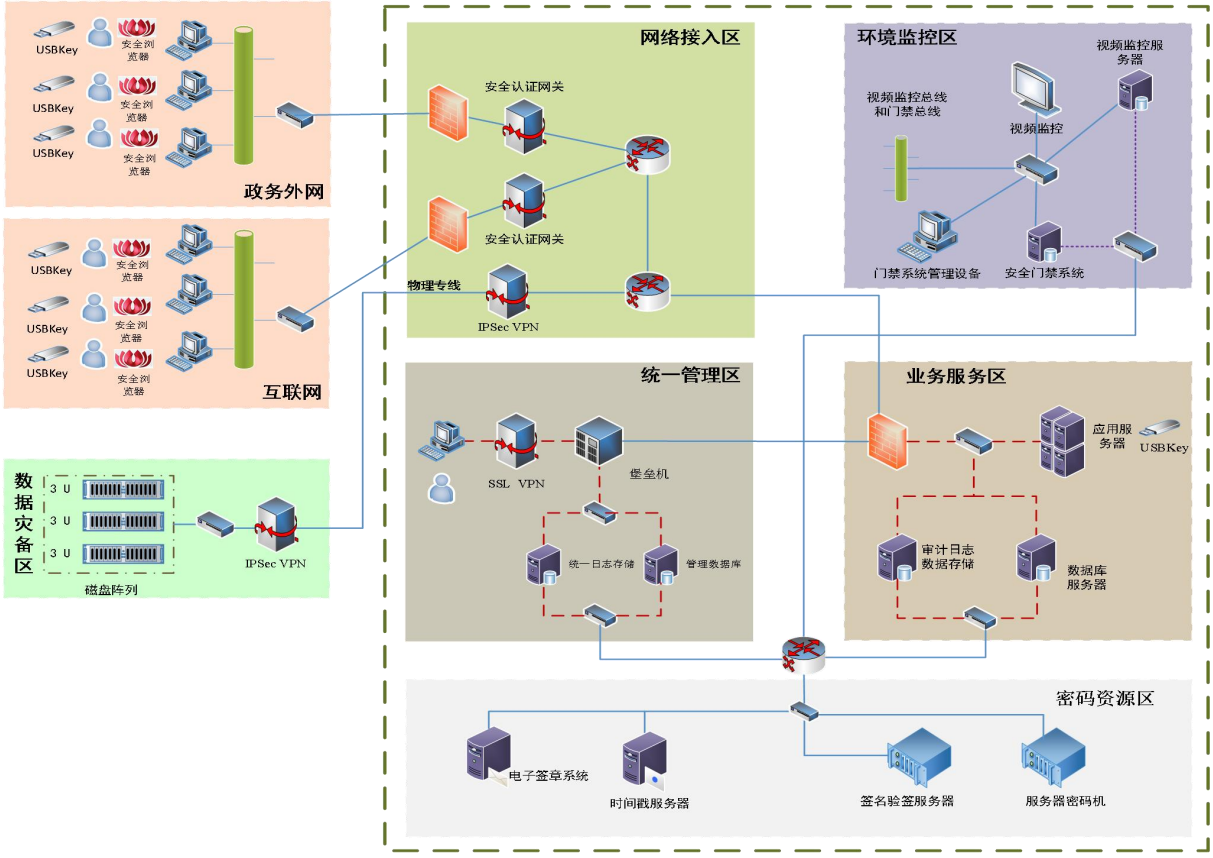


图3 系统密码应用部署图

所需密码产品、密码服务等配置如表 12 所示。

表12 密码产品/服务配置列表

序号	密码产品/服务类型	数量	备注说明
1	安全门禁系统	1	复用已有密码产品。
2	安全认证网关	6	其中 2 台复用已有密码产品，4 台新增。

3	SSL VPN	1	复用已有密码产品。
4	IPSec VPN	6	其中 2 台复用已有密码产品，4 台新增。
5	服务器密码机	2	其中 1 台复用已有密码产品，1 台新增。
6	签名验签服务器	2	其中 1 台复用已有密码产品，1 台新增。
7	时间戳服务器	1	复用已有密码产品。
8	安全电子签章系统	1	复用已有密码产品。
9	电子认证服务(设备证书)	5	新增 4 台安全认证网关、1 台签名验签服务器，需申请 5 张设备证书。
10	电子认证服务(域名证书)	1	新增 1 个域名，需申请 1 张域名证书。
11	安全浏览器(含密码模块)	xx	远程运维管理终端 xx 台、政务外网和互联网 PC 终端 xx 台，各需配置 xx 套产品。
12	智能密码钥匙	xx	远程运维管理终端 xx 台、政务外网和互联网 PC 终端 xx 台，各需配置 xx 套产品。

5.6 密码应用功能模块组成

为实现本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用功能，需开发适配若干密码应用功能模块。

以下仅为示例,针对具体系统应给出更为详尽的密码应用功能模块建设内容描述,包括模块实现的功能等。

1、门禁进出记录完整性模块

开发门禁进出记录完整性模块，调用服务器密码机提供的HMAC-SM3功能接口，实现电子门禁系统进出记录数据的存储完整性保护。

2、视频监控记录完整性模块

开发视频监控记录完整性模块，调用服务器密码机提供的HMAC-SM3功能接口，实现视频监控音像记录数据的存储完整性保护。

3、用户身份认证模块

开发用户身份认证模块，对接安全认证网关身份鉴别接口，绑定应用系统的用户数字证书和用户ID，实现应用系统对用户的安全身份鉴别。

4、业务重要数据安全传输模块

开发业务重要数据安全传输模块，对接安全认证网关SSL安全通信接口，实现应用系统通信数据的机密性和完整性保护。

5、服务器设备日志/访问控制信息完整性模块

开发服务器设备日志/访问控制信息完整性模块，调用服务器密码机提供的HMAC-SM3功能接口，实现应用服务器、数据库服务器等设备日志/访问控制信息的完整性保护。

6、重要可执行程序签名验签模块

开发重要可执行程序签名验签模块，调用智能密码钥匙提供的SM2密码算法数字签名功能接口，实现重要可执行程序的完整性、来源真实性保护。

7、用户访问控制信息签名验签模块

开发用户访问控制信息签名验签模块，调用签名验签服务器提供的SM2密码算法数字签名功能接口，实现应用系统用户的访问控制列表完整性保护。

8、应用系统重要数据加解密模块

开发应用系统重要数据加解密模块，调用服务器密码机提供的SM4密码算法加解密功能接口和SM2密码算法数字信封接口，实现用户身份鉴别数据、电子公文数据的存储机密性保护。

9、应用系统重要数据签名验签模块

开发应用系统重要数据签名验签模块，调用服务器密码机提供的SM2密码算法数字签名验签功能接口，实现用户身份鉴别数据、业务日志信息的存储完整性保护。

10、电子公文电子印章模块

开发电子公文电子印章模块，调用安全电子签章系统、时间戳服务器提供的数字签名和时间戳服务功能接口，实现系统内电子公文签批的不可否认性。

系统密码应用功能模块的开发适配总体工作量预估为2.5人•月。（注：对于建设投资规模为500万元以下的系统，其密码应用功能模块的开发适配工作量可大致估计为2.5人•月；若系统功能及业务复杂度较高，则密码应用功能模块的开发适配工作量可相应调增，此时需列明相应的工作量估算明细）。

6 安全管理方案

6.1 管理制度

根据《密码应用基本要求》中安全管理制度方面的要求，制定与系统相适应的密码安全管理制度和操作规范，内容至少包含密码设计、建设、运维、人员、设备、密钥等六个方面，并同步在单位现有的制度发布流程中补充密码相关管理制度发布流程，待新制定的密码安全管理制度和操作规范内部评审通过后，按照密码相关管理制度发布流程予以发布并遵照执行。

密码安全管理制度和操作规范发布后，每年年底，在本单位内部组织专家和密码相关人员对密码安全管理制度和操作规范在使用过程中的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

6.2 人员管理

根据《密码应用基本要求》中人员管理的要求，完善系统现有人员管理制度。

1、设置密码专题培训机制，每六个月组织一次，由内部专业人员或聘请外部专家担任培训讲师，内容涉及密码相关法律法规、标准规范、密码应用、密码应用安全性评估等多个方面，使相关人员了解密码相关法律法规，掌握密码应用基本原理，并遵照执行。

2、系统完成密码应用改造后，安排项目建设单位、相关密码产品厂商对本系统部署使用的密码产品开展操作培训，确保相关人员能够正确配置使用。

3、结合系统情况，分别设立密钥管理员、密码安全审计员、密码操作员等岗位，明确各岗位职责，每个岗位均由 2 人担任。

4、在现有的安全管理制度中，补充密码相关人员考核、奖惩、保密、调离制度，每年对密钥管理员、密码安全审计员、密码操作员组织一次考核，对考核成绩优异的予以表扬和奖励，考核成绩不合格者，进行批评教育；密钥管理员、安全审计员、密码操作员与单位签订保密协议，承担保密义务，相关人员若要调离岗位时，按照制定的人员调离制度承担相应的保密义务。

6.3 建设运行

完成本方案编制后，我单位将委托检测机构或组织专家评审会对本方案进行评估，并基于通过评估后的方案，合规、正确、有效地建设密码保障系统。

依据评估通过的密码应用方案完成建设后，我单位将委托检测机构对本系统进行密码应用安全性评估或密码应用测评，通过后才能上线运行。

系统上线运行后，我单位会定期（每年至少一次）自行或委托检测机构对系统开展密码应用安全性评估，并根据评估意见进行整改。当系统在运行过程中发现重大密码应用安全隐患时，须停止运行，制定整改方案，按照整改方案对系统进行整改，整改完成后自行或委托检测机构对系统开展密码应用安全性评估，评估通过后重新上线运行。

6.4 应急处置

根据《密码应用基本要求》关于应急处置的要求，完善系统现有应急管理制度，补充制定密码应用应急处置预案，做好应急资源准备，明确密码安全事件处理流程及其它管理措施。

7 安全与合规性分析

对方案的适用情况、采取的密码保障措施、采取的缓解及替代性措施及自评结果进行说明（详见表 13）：

1、若指标为适用，说明采取的密码保障措施或未采取的密码保障措施的情况（如采取的缓解及替代性措施）；

2、针对适用的指标，存在部分保护对象不适用的情况，论证其不适用性；

3、若指标为不适用，说明其不适用的理由。

表 13 密码应用合规性对照表

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
物理和环境安全	身份鉴别	宜	适用	在系统所在机房部署安全门禁系统,使用SM4密码算法实现人员的身份鉴别。	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	电子门禁记录数据存储完整性	宜	适用	在密码资源区部署服务器密码机，使用HMAC-SM3密码算法对安全门禁系统进出记录、视频监控音像记录等数据进行存储完整性保护。	/	通过
	视频监控记录数据存储完整性	宜	适用		/	通过
网络和通信安全	身份鉴别	应	适用	在网络接入区和数据灾备区分别部署IPSec VPN，对通信双方进行身份鉴别； 在网络接入区部署安全认证网关，对业务通信链路的服务端进行身份鉴别； 在统一管理区部署SSL VPN，对运维管理链路的服务端进行身份鉴别。	/	通过
	通信数据完整性	宜	适用	在业务服务区和数据灾备区分别部署IPSec VPN，基于SM4、SM3密码算法建立安全数据传输通道； 在网络接入区部署安全认证网关，通过TLCP通信协议实现用户与系统通信数据的机密性和完整性保护；在统一管理区部署SSL VPN，通过TLCP通信协议对运维管理数据进行传输机密性和完整性保护。	/	通过
	通信过程中重要数据的机密性	应	适用		/	通过
	网络边界访问控制信息的完	宜	适用	由安全认证网关、IPSec VPN、SSL VPN等密码产品提供网	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	整性			络边界访问控制信息完整性保护。		
	安全接入认证	可	不适用	/	无外部设备接入本系统的需求。	通过
设备和计算安全	身份鉴别	应	适用	在远程运维管理终端部署安全浏览器（含密码模块），并向管理员配发智能密码钥匙,对访问堡垒机的用户进行身份鉴别并通过SSL VPN建立安全的远程管理信息传输通道。	管理员身份鉴别未使用密码技术，通过SSL VPN双向鉴别降低风险。	通过
	远程管理通道安全	应	适用			通过
	系统资源访问控制信息完整性	宜	适用	调用部署在密码资源区中的服务器密码机，使用HMAC-SM3密码算法对服务器、数据库等设备的系统资源访问控制信息进行完整性保护。密码设备访问控制信息的完整性保护由该设备自身实现。	/	通过
	重要信息资源安全标记完整性	宜	不适用	/	本系统不涉及重要信息资源的安全标记。	通过
	日志记录完整性	宜	适用	调用部署在密码资源区中的服务器密码机，使用HMAC-SM3密码算法对服务器、数据库等设备日志进行完整性保护。密码设备日志记录的完整性保护由该设备自身实现。	/	通过
	重要可执	宜	适用	在应用服务器部署	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	行程序完整性、重要可执行程序来源真实性			智能密码钥匙，对应用服务器中重要可执行程序和文件进行完整性保护，使用或读取这些程序和文件时，通过智能密码钥匙以及SM2密码算法签名验签机制以确认其完整性和来源真实性。		
应用和数据安全	身份鉴别	应	适用	在系统互联网和政务外网PC端部署安全浏览器（含密码模块），并向相关用户配发智能密码钥匙，通过调用密码支撑平台的身份鉴别服务，对相关用户进行身份鉴别。	/	通过
	访问控制信息完整性	宜	适用	通过调用密码支撑平台的签名验签服务，使用基于SM2密码算法的数字签名验签技术对系统应用用户访问权限控制列表进行完整性保护。	/	通过
	重要信息资源安全标记完整性	宜	不适用	/	本系统不涉及重要信息资源的安全标记。	通过
	重要数据传输机密性	应	适用	通过调用密码支撑平台的数据加解密服务、签名验签服务，对访问用户身份鉴别数据、电子公文数据、业务日志数据等重要数据进行存	通过网络和通信层面的密码技术进行弥补和降低风险。	通过
	重要数据存储机密性	应	适用			通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	重要数据传输完整性	宜	适用	储机密性、完整性保护，实现身份鉴别数据、电子公文数据、业务日志数据等重要数据的防窃取和防篡改保护； 通过网络和通信层面的安全认证网关实现身份鉴别数据、电子公文数据、业务日志数据等重要数据的安全传输防护。		通过
	重要数据存储完整性	宜	适用			通过
	不可否认性	宜	适用	通过调用密码支撑平台提供的安全电子签单服务、时间戳服务，使用密码技术对系统内流转的电子公文数据进行数字签名，并加盖时间戳，实现操作行为的不可否认性。	/	通过
管理制度	具备密码应用安全管理制度	应	适用	制定密码应用安全管理制度	/	通过
	密钥管理规则	应	适用	制定密钥管理规则	/	通过
	建立操作规程	应	适用	建立操作规程	/	通过
	定期修订安全管理制度	应	适用	定期修订安全管理制度	/	通过
	明确管理制度发布流程	应	适用	明确管理制度发布流程	/	通过
	制度执行过程记录留存	应	适用	留存制度执行过程记录	/	通过
人员管理	了解并遵守密码相	应	适用	对密码相关法律法规和密码管理制度	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	关法律法规和密码管理制度			进行定期培训		
	建立密码应用岗位责任制度	应	适用	建立密码应用岗位责任制度	/	通过
	建立上岗人员培训制度	应	适用	建立上岗人员培训制度	/	通过
	定期进行安全岗位人员考核	应	适用	定期对安全岗位人员进行考核	/	通过
	建立关键岗位人员保密制度和调离制度	应	适用	建立关键岗位人员保密制度和调离制度	/	通过
建设运行	制定密码应用方案	应	适用	制定密码应用方案	/	通过
	制定密钥安全管理策略	应	适用	制定密钥安全管理策略	/	通过
	依据密码应用方案实施建设	应	适用	依据密码应用方案实施建设	/	通过
	投入运行前进行密码应用安全性评估	应	适用	系统投入运行前进行密码应用安全性评估	/	通过
	定期开展密码应用安全性评估及攻防对抗演习	应	适用	定期开展密码应用安全性评估及攻防对抗演习	/	通过
应急处置	应急策略	应	适用	制定密码应用应急策略	/	通过
	事件处置	应	适用	制定密码应用事件处置规范	/	通过
	向有关主	应	适用	向有关主管部门上	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	管部门上报处置情况			报处置情况		

8 实施保障方案

8.1 实施内容

1、项目实施内容

本项目主要对我单位电子公文处理系统进行密码应用改造，以达到《密码应用基本要求》对信息系统密码应用安全第三级的要求，合规、正确、有效地使用商用密码对系统进行保护，并通过密码应用安全性评估。

本项目将依据方案中确定的密码应用需求、密码应用设计方案，使用经检测认证合格的商用密码产品、服务，对现有的应用进行开发改造、系统集成、联调测试等方式建设密码技术体系；依据安全管理方案，制定密码安全相关人员、制度、业务、运维、应急等方面的管理措施，同步建立密码安全管理体系。

2、可能存在的风险点及应对措施

密码应用改造可能会给系统带来一定风险，主要风险及其规避方法如下：

1）影响系统正常运行的风险：应用系统密码模块开发改造、联调测试、试运行等环节。

规避方法：在测试系统中进行充分测试，选择夜间或休息日进行线上联调测试，确保系统运行的稳定性和可用性。

2）项目延期：方案编制、招标、改造、验收测试等环节。

规避方案：制定细致的实施计划，并严格遵照执行，设立周报制度，每周汇报进度，进度不达标的地方及时进行督促，确保项目进度。

8.2 实施计划

本项目实施周期为XX个月，自20XX年XX月开始，至20XX年XX月。

1、项目总体进度及阶段性节点如下：

1）20XX年XX月，完成密码应用方案设计，并通过评估；

2）20XX年XX月，完成密码应用改造；

3）20XX年XX月，完成系统改造后的密码应用安全评估或密码应用测评，并上线试运行；

4）20XX年XX月，完成系统运行效率、使用效果的后评价工作，并通过项目验收。

2、项目详细进度计划如表 14 所示。

表 14 项目详细进度计划

阶段	时间节点	工作内容	实施主体	阶段性节点
密码应用改造方案设计	20XX 年 XX 月	密码应用方案沟通研讨，确定改造内容和范围。	系统建设单位	
		开展密码应用方案设计，确定项目总体整体架构，明确项目实施周期和关键时间节点。		
		开展详细的密码应用方案编制，完成系统现状分析、密码应用需求分析、技术方案、安全管理方案和实施保障方案等内容的编制。		

		根据密码应用的场景及方案设计内容。		
		对方案进行评估。	检测机构	密码应用方案通过评估
选择集成商	20XX 年 XX 月	选择集成商，负责系统的密码应用改造。	系统建设单位	选择密码应用改造集成商
密码应用改造	20XX 年 XX 月-20XX 年 XX 月	根据密码应用技术方案中的软硬件密码产品清单，采购密码产品。	系统建设单位、系统集成商	完成本系统密码保障体系中的技术体系建设
		根据密码应用技术方案，复用系统所在机房电子门禁系统、视频监控系统。		
		根据密码应用技术方案，对系统网络和通信层面的身份鉴别、网络传输通道、集中管理通道等方面的安全需求进行密码应用改造。		
		根据密码应用技术方案，对系统设备和计算层面的管理员登录身份鉴别、远程管理身份鉴别信息传输、访问控制信息、重要应用程序、日志记录等方面的安全需求进行密码应用改造。		

		根据密码应用技术方案，对系统应用和数据层面的访问用户身份鉴别数据、电子公文数据、业务日志数据等方面的安全需求进行密码应用。		
		根据安全管理方案，设计密码安全管理制度、人员管理、设备管理、应急处置等方面的管理体系。		完成本系统密码保障体系中的管理体系设计
测评	20XX 年 XX 月	选择检测机构。	系统建设单位	选择检测机构
		检测机构依据评估通过的密码应用方案对改造后的系统进行密码应用安全性评估或密码应用测评。	检测机构	完成系统密码应用改造后的密码应用安全性评估或密码应用测评
试运行	20XX 年 XX 月	开展系统试运行、收集试运行期间的性能，效率、安全状态等数据，根据试运行情况做进一步评估和优化。	系统建设单位	开始试运行
项目验收	20XX 年 XX 月	完成系统运行效率、使用效果的后评价工作，根据评价结果进行项目验收。	系统建设单位	通过项目验收

8.3 保障措施

8.3.1 组织和人员保障

我单位将该项目作为重点任务，在项目组织上本着“统一领导、健全组织、合理分工、密切协作”的原则，明确项目组织形式，设置项目组织

架构，按照职责分工开展工作，为顺利实施密码应用改造项目，高质量、高效率完成密码应用改造提供组织保障。

项目组织形式见图4，各组工作实行组长负责制。

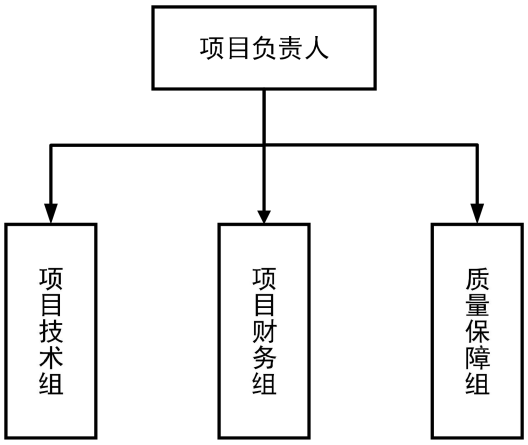


图 4 组织结构图

各组人员组成及工作职责如表15所示。

表 15 组织人员构成表

序号	名 称	人员组成	工作职责
1	项目负责人	张三	总体负责项目的技术、组织和财务等方面工作，宏观把握项目改造内容和建设目标。
2	项目技术组	组长：李四 组员：	由项目负责人及项目骨干组成，负责项目总体管理、各部分工作协调、项目进展情况和项目完成情况的监督检查、项目改造后的质量把关。
3	项目财务组	组长：李四 组员：	由本单位财务部门负责人和骨干组成，负责项目执行过程中的经费管理。
4	质量保障组	组长：李四 组员：	负责按照本项目制定的质量保障措施，落实质量监督和管理。

8.3.2 经费保障

本项目执行过程中，将严格按照单位资金使用管理办法，进行经费使用，确保经费使用合规。

8.3.3 质量保障

在项目建设实施过程中，通过组织项目定期会议，保障实施工作按计划进行；同时对于项目实施过程中出现的偏差或问题，及时沟通协调，必要时通过项目技术组向项目负责人进行汇报，并形成相应的决策意见和修订方案。

1、项目例会制度

项目通过定期例会和不定期会议来跟踪项目进度，反馈和讨论项目实施过程中的问题，对项目技术方案进行评审，对计划完成情况进行总结和说明，同时对后续计划进行确认。在遇到技术障碍或方案涉及重大变更时，通过不定期会议，由项目技术组或质量保障组讨论决策，针对出现的变更或重大问题进行及时修正，并制定相应的措施和方案。

2、项目周报机制

由项目技术组制定项目进展周报机制，每周五提交本周的项目进展、阶段成果、遗留问题和下周计划，质量保障组对项目进度进行统筹跟踪，协调相关人员和资源，保障项目如期完成。

3、风险管理机制

项目在实施过程中，建立完善的风险管理机制，包括项目风险的识别、评估和管理，从资金、成本控制、采购合规、技术、人才、管理等多个方面进行风险管控，包括确定风险发生时的备选方案、资金、设备和人员等；定期检查和评估风险消减措施是否有效；定期进行风险排查；制定风险应对的启动机制等措施。

8.3.4 监督检查

监督检查是保证项目实施各阶段的活动顺利开展的重要措施，拟通过如下几类活动开展监督检查工作：

阶段评审：在系统实施过程中，定期地或阶段性地对系统和文档进行评审。在本项目中拟进行以下三次评审：第一次评审方案合理性、确认验

收方法；第二次评审方案的实施计划，实施步骤、测试方法，试运行方案等，并对第一次评审结果复核；第三次评审功能和综合检查。阶段评审要组织专门的评审小组，评审小组原则上由实施小组成员、用户项目管理小组成员、我公司代表等构成。

日常检查：在本项目实施过程中，督促各子系统填写项目进展报告，即各个设备调试进展报告、软件安装部署阶段进度表、项目完成情况表等三张表格。项目管理人员可以通过项目进展报告发现有关项目实施过程中的问题。

8.4 经费概算

8.4.1 密码产品/服务费用列表

密码产品/服务费用详见表 16。

表 16 密码产品/服务费用列表（仅为示例）

序号	类别	在示例中提供的密码功能	单价（万元）	数量	总价（万元）
1	安全认证网关	为互联网和政务外网用户提供安全接入通道；配合 PC 端部署的安全浏览器（含密码模块），实现 PC 端到服务端之间数据传输机密性和完整性保护。	20	6（其中，复用 2 台，新增 4 台。）	80
2	IPSec VPN	为进行数据灾备的通信双方进行双向身份鉴别，对数据备份传输通道进行传输机密性、完整性保护。	20	6（其中，复用 2 台，新增 4 台）	80
3	签名验签服务器	供系统调用，通过数字签名技术对系统重要数据进行完整性保护。	20	2（其中，复用 1 台，新增 1 台）	20

序号	类别	在示例中提供的密码功能	单价（万元）	数量	总价（万元）
4	服务器密码机	为多个应用实体提供密码运算、密钥管理。	12	2（其中，复用 1 台，新增 1 台）	12
5	电子认证服务（域名证书）	为域名申请数字证书，用于保证信息传输的机密性，确认网站的真实性。	1	1（新增）	1
6	电子认证服务（设备证书）	为安全认证网关、签名验签服务器等设备申请数字证书，用来证明设备的身份信息。	0.6	5（新增）	3
7	安全浏览器（含密码模块）	确保设备管理员安全登录堡垒机，互联网和政务外网用户安全访问系统。	/	XX	/
8	智能密码钥匙	为设备管理员登录堡垒机、系统用户/管理员登录系统进行身份鉴别。	/	XX	/

8.4.2 密码应用功能模块开发费列表

密码应用功能模块开发费用详见表 17。

表 17 密码应用功能模块开发费列表（仅为示例）

序号	类别	人·月	单价（万元）	总价（万元）
1	密码应用功能模块	2.5	2	5

附录 3

重要网络和信息系统密码应用方案示例（上云系统）

电子公文处理系统密码应用方案

系统名称：电子公文处理系统

系统建设单位：

编制日期：

编 制 说 明

1、本应用方案由系统建设单位组织编写。

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，各级标题均加粗；

（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。

基本信息表

<table>
<tr><th colspan="6">责任单位</th></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td>所属省部密码管理部门</td><td colspan="5"></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><th colspan="6">信息系统</th></tr>
<tr><td>系统名称</td><td colspan="5"></td></tr>
<tr><td>是否为关键信息基础设施</td><td colspan="5">☐已认定，所属安全保护工作部门：_____
☐未认定</td></tr>
<tr><td rowspan="2">网络安全等级保护定级和备案情况</td><td colspan="5">☐已定级备案，第__级（一至四），S__A__G__ 备案证明编号：
系统密码应用安全要求等级与等级保护定级是否一致：
☐是 ☐否，变化情况说明：</td></tr>
<tr><td colspan="5">☐未定级，系统密码应用按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》第三级信息系统要求</td></tr>
<tr><td>网络安全等级测评情况</td><td colspan="5">☐已测评
测评机构名称：_____ 测评时间：_____ 测评结论：
☐正在测评 测评机构名称：_____
☐未测评</td></tr>
<tr><td>商用密码应用安全性评估情况</td><td colspan="5">☐已评估
检测机构名称：_____ 评估时间：_____评估结论：
☐正在评估 检测机构名称：_____
☐未评估</td></tr>
<tr><td>系统是否依赖不在</td><td colspan="2">☐是
云平台名称：</td><td colspan="3">☐云平台已评估 ☐云平台未评估
检测机构名称：☐
评估时间： 评估结论：</td></tr>
</table>

本系统范围内的云平台运行	□否

目　录

一级目录为黑体三号字体，二级目录为楷体小三号字体，三级目录为仿宋四号字体。每级目录缩进两个字符。

（本方案主要以新建电子公文处理系统（部署于电子政务云）为例；对于存量系统迁移上云或云上已建系统的密码应用改造等情形，将另行描述说明。）

1 背景

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。《密码法》《网络安全法》《商用密码管理条例》《关键信息基础设施安全保护条例》等多部法律法规的颁布实施，从法律层面为信息系统开展商用密码应用提供了根本遵循。

为落实相关法律法规对于信息系统密码应用的要求，结合《国家政务信息化项目建设管理办法》《政务信息系统政府采购管理暂行办法》等规范性依据，我单位决定对已运行的电子公文处理系统进行密码应用改造。

该系统部署于电子政务云，为我单位日常办公的重要信息系统，为单位各级领导及办公人员提供业务审批、公文签批、公文办理、公文管理等业务过程的信息化管理，实现各部门之间横向与纵向业务流转和内部信息资源共享。

通过对该系统的现状和密码应用需求分析，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《密码应用基本要求》）、GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》（以下简称《密码应用设计指南》），从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理等层面，设计了该系统密码应用的技术方案、安全管理方案和实施保障方案。

2 系统概述

2.1 基本情况

本系统为新建信息系统,系统投资规模约为 XX 万,责任单位为 XX 单位,使用人员为本单位各级领导及办公人员,系统拟部署于电子政务云平台(以下简称云平台)互联网区,用户可通过互联网的 PC 终端访问。

(对于存量系统迁移上云或云上已建系统的密码应用改造等情形,还需明确系统验收时间、上线运行时间、部署模式、网络安全等级保护定级及备案情况等。)

2.2 计算平台现状

2.2.1 物理和环境

本系统部署于云平台,物理和环境安全由云平台提供保障,云平台部署于 XX 路 XX 号 XX 层 XX 室,由 XX 负责运维。

2.2.2 网络和通信

本系统网络拓扑如图 1 所示。

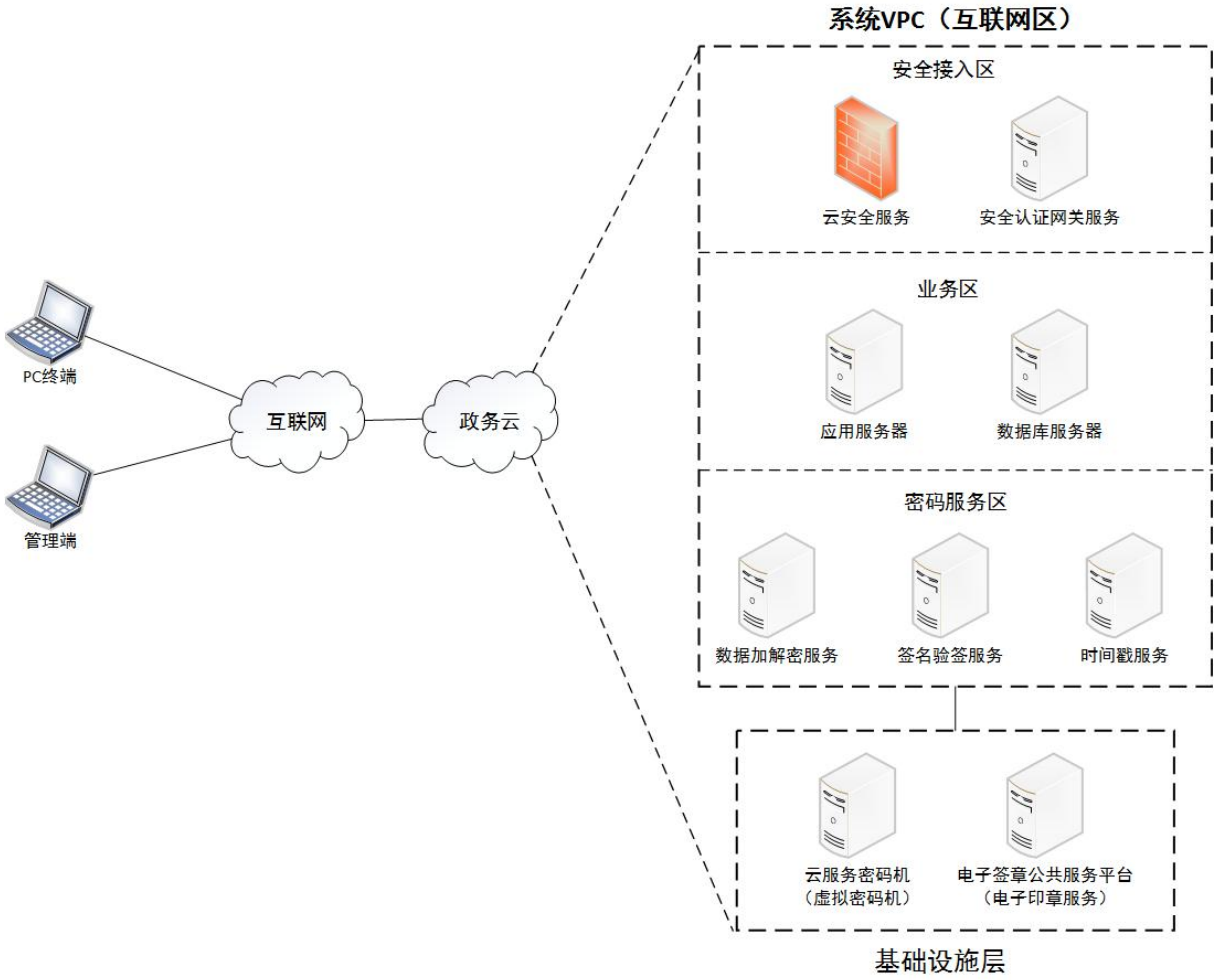


图 1 系统网络拓扑图

电子政务云网络划分为互联网区和政务外网区，本系统部署于电子政务云的互联网区域。系统网络划分为安全接入区、业务区、密码服务区等。

安全接入区位于系统的网络边界，提供互联网用户的访问接入，基于云平台已有的安全资源和密码资源，部署了防火墙、安全认证网关等服务。

业务区是电子公文处理系统拟部署的核心区域，基于云平台的计算资源，拟部署应用服务器、数据库服务器等设备，实现业务审批、公文签批、公文办理、公文管理等业务过程的信息化管理。

依托于云平台提供的密码服务，在密码服务区引入了电子签章、时间戳、签名验签、数据加解密等密码服务，为系统提供各类密码功能应用支

撑。

本单位通过云平台提供的SSL VPN接入云平台，对服务器、数据库、防火墙、密码服务等进行统一运维。该SSL VPN以及运维审计平台由云平台负责管理。

2.2.3 设备和计算

本系统所有计算、存储、网络、密码和安全资源均由云平台提供，包括服务器虚拟机、堡垒机、防火墙、安全认证网关服务、电子签章服务、时间戳服务、签名验签服务、数据加解密服务等；本系统拟部署操作系统、数据库系统、应用中间件等软件产品；运维人员通过互联网接入SSL VPN登录堡垒机对服务器操作系统、数据库、密码服务等进行远程运维管理。

2.3 业务应用现状

电子公文处理系统是我单位拟建设的日常办公信息系统，为单位各级领导及办公人员提供业务审批、公文签批、公文办理、公文管理等业务过程的信息化管理，实现各部门之间横向与纵向业务流转，以及内部信息资源共享，关键数据类型为电子公文数据。PC终端通过浏览器登录访问系统。

2.4 密码应用现状

2.4.1 计算平台

1、物理和环境

本系统部署于XX电子政务云平台，由云平台提供物理机房的安全保障。该云平台已通过密码应用安全性评估（第三级）。

2、网络和通信

云平台部署 SSL VPN 供系统运维管理人员访问堡垒机，该 SSL VPN 通过 SM2 密码算法数字证书对通信服务端进行身份鉴别，并基于 TLCP 通信协议建立安全的远程运维通信通道。

（对于已建系统，还需描述本系统网络和通信安全的密码应用情况，以下描述仅供参考：目前 PC 端用户通过互联网链路访问 XX 系统，通过应用系统中间件配置了 HTTPS 通信链路（TLSv1.2），建立了数据传输通道，基于 RSA2048、AES128、SHA256 等密码算法实现通信实体的身份鉴别和数据的安全传输保护。）

3、设备和计算

云平台为系统运维管理人员配发智能密码钥匙（载有 SM2 密码算法数字证书），并与 SSL VPN 实现双向鉴别，以缓解远程运维管理设备身份鉴别和设备远程运维管理通道的安全风险。

（对于已建系统，还需描述本系统设备和计算安全的密码应用情况，以下描述仅供参考：系统运维管理人员通过用户名+口令方式登录堡垒机对设备进行远程运维,并基于 HTTPS 协议建立设备与堡垒机之间的安全连接。）计算平台密码应用现状如表 1 所示。

表 1 计算平台密码应用现状

序号	名称	数量	管理责任主体	密码应用情况
1	安全门禁系统	/	云平台营运商	本系统部署于 XX 电子政务云平台，由云平台提供物理机房的安全保障。该云平台已通过密码应用安全性评估（第三级）。

2	视频监控系统	/	云平台营运商	本系统部署于 XX 电子政务云平台，由云平台提供物理机房的安全保障。该云平台已通过密码应用安全性评估（第三级）。
3	SSL VPN	1	云平台营运商	实现远程运维管理通信数据的安全传输。

2.4.2 密码支撑平台

本系统部署在云平台互联网区 VPC x 中，与已部署于该 VPC x 中的人事管理系统和档案管理系统共用密码资源，责任主体为 XX 单位，目前，本单位部署的密码支撑平台现状如表 2 所示。

表 2 密码支撑平台现状

序号	名称	数量	责任主体	密码支撑情况
1	安全认证网关服务	2	本单位	实现业务应用访问的身份鉴别；同时支持业务应用访问的网络和通信安全。 支撑的系统包括：人事管理系统、档案管理系统。
2	数据加解密服务	1	本单位	实现业务应用的存储机密性和完整性。 支撑的系统包括：人事管理系统、档案管理系统。
3	签名验签服务	1	本单位	实现应用用户访问权限控制列表、用户身份鉴别数据和业务审计日志数据的完整性保护。 支撑的系统包括：人事管理系统、档案管理系统。
4	电子签章服务	1	本单位	实现档案管理存档操作行为的不可否认性。 支撑的系统包括：人事管理系统。
5	时间戳服务	1	本单位	配合电子签章服务，实现档案管理存档操作行为的不可否认性。 支撑的系统包括：人事管理系统。

2.4.3 业务应用

无。

2.5 密码应用管理现状

依据《密码应用基本要求》，本系统的安全管理措施包括管理制度、人员管理、建设运行和应急处置等 4 个方面。其中，云平台密码支撑服务相关管理制度，包括密码人员管理、密钥管理、应急处置等，由云平台提供。

3 密码应用需求分析

3.1 安全风险分析

根据《密码应用基本要求》《密码应用设计指南》，结合系统密码应用现状，从计算平台、业务应用、安全管理等层面，围绕重要数据、系统角色、关键软硬件设备、关键业务环节、关键操作行为等重点对象,对本系统进行风险分析。

以下仅为示例，针对具体系统应给出更为详尽的风险分析。

3.1.1 重点保护对象分析

本系统计算平台、业务应用等层面重点保护对象如表 3 所示。

表 3 系统各层面重点保护对象

序号	安全层面		保护对象	说明
1	计算平台	物理和环境安全	机房电子门禁系统及其数据	无
			机房视频监控数据	

序号	安全层面		保护对象	说明
2		网络和通信安全	互联网访问应用通信信道	从互联网访问应用的通信信道
3			远程运维通信信道	通过远程管理终端对系统内设备进行运维的通信信道
4		设备和计算安全	服务器虚拟机	应用服务器和数据库服务器
5			重要可执行程序和文件	关键业务应用软件安装包、升级包等
6				系统关键组件
7			数据库	无
8			堡垒机	用于集中运维管理
9			密码产品	无
10	业务应用	应用和数据安全	应用用户	互联网用户
11				
12			重要数据	用户登录口令(用户身份鉴别数据)
13				系统中通知、报告、批复等电子公文数据
14				系统业务日志数据
15				系统访问控制信息
16			操作行为	系统重要电子公文数据的签发行为

3.1.2 计算平台安全分析

3.1.2.1 物理和环境安全分析

本系统的物理和环境安全由云平台提供保障，本节略。

3.1.2.2 网络和通信安全分析

互联网用户访问应用时存在通信主体身份被假冒，通信数据在信息系

统外部被非授权截取、非授权篡改风险；

（对于已建信息系统，基于其密码应用现状进行风险分析并给出相应的描述。）

3.1.2.3 设备和计算安全分析

1、系统中服务器虚拟机、数据库、密码服务等存在日志记录和访问控制信息被非授权篡改风险；

2、系统应用服务器中重要可执行程序或文件存在被非授权篡改、来源不可信风险。

（对于已建信息系统，基于其密码应用现状进行风险分析并给出相应的描述。）

3.1.3 业务应用安全分析

1、系统应用存在应用被非授权人员登录风险；

2、用户身份鉴别数据、系统内流转的电子公文数据等重要数据在传输、存储过程中存在被窃取和非授权篡改风险；

3、应用访问控制信息、业务日志数据等重要数据存在被非授权篡改风险；

4、在系统内进行电子公文数据流转时，存在数据发送者否认其操作行为的风险。

（对于已建信息系统，基于其密码应用现状进行风险分析并给出相应的描述。）

3.1.4 安全管理分析

存在密码应用安全管理制度缺失或不合规导致的密钥泄露、数据泄露等风险。

3.2 密码应用需求

根据安全风险分析，并对照《密码应用基本要求》中三级指标要求和《密码应用设计指南》，梳理出本系统密码应用需求清单，如表4所示。

表 4 系统密码应用需求清单

安全层面		指标要求	系统密码应用需求	不适用说明
计算平台安全	物理和环境安全	身份鉴别	已符合密码应用要求。	无
		电子门禁记录数据完整性	已符合密码应用要求。	无
		视频监控记录数据完整性		
		密码服务	不适用。	无密码服务需求
		密码产品	采用的密码产品应达到 GB/T 37092-2018 二级及以上安全要求。	无
	网络和通信安全	身份鉴别	已符合密码应用要求。	无
		通信数据完整性	保护通信过程中重要业务数据的完整性和机密性,防止数据被非授权篡改，防止重要数据泄露。	无
		通信过程中重要数据的机密性		无

安全层面		指标要求	系统密码应用需求	不适用说明
		网络边界访问控制信息的完整性	保护互联网用户访问应用系统的网络边界访问控制信息的完整性，防止被非授权篡改。	无
		安全接入认证	不适用。	无外部设备接入本系统的需求
		密码服务	采用的数字证书由具有电子认证服务资质的机构签发。	无
		密码产品	采用的密码产品应达到 GB/T 37092-2018 二级及以上安全要求。	无
	设备和计算安全	身份鉴别	管理员通过远程运维管理终端访问堡垒机、服务器虚拟机、数据库、密码服务时，对其身份真实性进行识别和确认，防止假冒人员登录。	无
		远程管理通道安全	在设备实施远程运维管理时，对设备的运维管理通道进行保护，防止运维管理数据泄漏。	无
		系统资源访问控制信息完整性	保护系统中服务器虚拟机、数据库、密码服务的访问控制信息的完整性，防止被非授权篡改。	无
		重要信息资源安全标记完整性	不适用。	设备没有安全标记
		日志记录完整性	保护系统中服务器虚拟机、数据库、密码服务的日志记录的完整性，防止被非授权篡改。	无
		重要可执行程序完整性、 来源真实性	保护应用服务器等设备中部署的重要可执行程序的完整性和来源真实性，防止被非授权篡改。	无
		密码服务	不适用。	无密码服务需求
		密码产品	采用的密码产品应达到 GB/T 37092-2018 二级及以上安全要求。	无
业务应用安全	应用和数据安	身份鉴别	确认应用系统用户身份的真实性，防止假冒人员登录。	无

安全层面		指标要求	系统密码应用需求	不适用说明
	全	访问控制信息完整性	对应用系统的访问权限控制列表进行完整性保护，防止被非授权篡改。	无
		重要信息资源安全标记完整性	不适用。	应用没有安全标记。
		数据传输机密性	保护互联网客户端与服务端之间传输和存储的用户登录身份鉴别信息、电子公文数据等重要数据的机密性和完整性，防止数据泄露给非授权的个人、进程等。保护系统业务日志数据的完整性，防止该数据被非授权篡改。	无
		数据存储机密性		
		数据传输完整性		
		数据存储完整性		
		不可否认性	保护系统中流转的电子公文数据的不可否认性，确保发送方对已经发生的操作行为无法否认。	无
		密码服务	采用的数字证书由具有电子认证服务资质的机构签发。	无
		密码产品	采用的密码产品，应达到 GB/T 37092-2018 二级及以上安全要求。	无

4 安全目标及设计原则

4.1 安全目标

综合考虑本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用需求，充分利用已有密码资源，设计合规、正确、有效的密码应用技术方案，以达到《密码应用基本要求》中三级指标要求，并为后续密码保障体系建设、密码应用测评和密码应用安全性评估奠定坚实基础。

4.2 设计原则和依据

本系统密码应用技术方案设计应遵循以下原则：

1、总体性原则。根据本系统密码应用安全要求等级，结合密码应用需求和预期目标，对本系统密码应用开展顶层设计，形成涵盖技术、管理和实施保障的整体方案，为在系统中落实密码应用相关要求奠定基础。

2、完备性原则。围绕本系统实际业务应用与安全要求等级，通过自上而下的体系化设计，综合考虑物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等多个层面密码应用需求，设计本系统密码应用技术方案。

3、经济性原则。结合本系统规模，在合理、够用的前提下，考虑本系统规模、并发数、冗余、部署方式、管理模式等情况，充分利用已有密码资源，设计符合《密码应用基本要求》的密码应用技术方案，确保系统密码应用改造投资合理，规模适度，避免资金浪费和过度保护。

主要设计依据：

●GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》

●GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

●GB/T 32922-2023《信息安全技术 IPSec VPN 安全接入基本要求与实施指南》

●GB/T 38636-2020《信息安全技术 传输层密码协议（TLCP）》

●GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》

●GB/T 38541-2020《信息安全技术 电子文件密码应用指南》

●GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》

●GB/T 37092-2018《信息安全技术 密码模块安全要求》

●GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》

●GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》

●GB/T 33482-2016《党政机关电子公文系统建设规范》

●GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》

●GM/T 0033-2023《时间戳接口规范》

●GM/T 0030-2014《服务器密码机技术规范》

●GM/T 0026-2023《安全认证网关产品规范》

●GM/T 0025-2023《SSL VPN 网关产品规范》

●GM/T 0023-2023《IPSec VPN 网关产品规范》

5 密码应用设计

5.1 密码应用技术框架

本系统密码应用技术框架包含五个方面，如图 2 所示。

图 2 系统密码应用技术框架

1、总体要求：系统调用密码支撑平台提供的密码服务和密码资源，产品实际使用中配置的密码算法、密码技术符合国家密码管理部门的要求。

2、功能要求：机密性，信息不能被非授权者、实体或进程利用或泄露；完整性，数据不能被非授权篡改或非授权使用；真实性，对信息来源的真实身份进行鉴别；不可否认性，发送者或接收者不能事后否认其发送或接收信息的行为。

3、应用要求：本系统涉及物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面，具体的密码功能设计详见 5.2-5.4 节。

4、密钥管理：明确系统涉及的密钥种类及管理环节，设计安全的技术实现方式，确保密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复、销毁等生存周期的安全。密钥管理方案的技术实现需由密码支撑平台提供，未采用该方式的密钥管理方案技术实现可提请国家密码管理部门组织开展安全性审查。

5、安全管理：包括管理制度、人员管理、建设运行、应急处置等，详见第 6 章。

5.2 计算平台密码应用方案

5.2.1 物理和环境安全

本系统部署于云平台，其物理和环境安全已由云平台提供安全保障。云平台机房位于 XX 路 XX 号 XX 层 XX 室，由 XX 负责运维。

5.2.2 网络和通信安全

（一）密码功能设计

调用密码支撑平台提供的安全认证网关服务，在互联网用户与服务端通信前，通过 SM2 密码算法数字证书对服务端进行身份鉴别，并基于 TLCP 通信协议建立安全的数据传输通道。

（二）资源配置估算

本系统面向互联网提供服务，系统性能测算如下：

系统最大并发连接数：1900 个；

系统最大流量：500Mbps；

系统最大每秒事务数（TPS）：3400 次；

系统每秒最大备份数据量：300Mbps。

1、安全认证网关估算

根据密码资源使用现状，结合本系统性能测算数据，对安全认证网关的总体需求进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2,C1/C2)/(1-D)，说明如下：

X：安全认证网关估算数量。

A1：系统最大并发连接数。

A2：安全认证网关支持最大并发连接数。

B1：系统最大流量（Mbps）。

B2：安全认证网关支持最大流量（Mbps）。

C1：最大每秒事务数（TPS）。

C2：安全认证网关支持最大每秒事务数（TPS）。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

安全认证网关一般按最大并发连接数、最大流量、最大每秒事务数这三项指标来计算性能负载，三项中资源使用占比最大的主要性能指标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 5 所示：

表 5 互联网安全认证网关数量估算表

应用系统	系统最大并发连接数（个）A1	安全认证网关最大并发连接数（个）A2	系统最大流量(Mbps)B1	安全认证网关支持最大流量(Mbps)B2	最大每秒事务数(TPS)C1	安全认证网关最大每秒事务数（TPS）C2	密码设备计算荷载冗余边界 D	安全认证网关估算数量 X
人事管理系统	1500	5500	400	2000	3000	25000	0.2	0.34
档案管理系统	2340	5500	300	2000	6000	25000	0.2	0.53
电子公文处理系统	1900	5500	500	2000	3400	25000	0.2	0.43
总计								1.3
安全认证网关基本需求（向上取整）								2
高可用需求数量								1
总计（安全认证网关需求总数）								3

根据上述估算表中安全认证网关服务需求总量（互联网 3 套）与实际数量（互联网 1 套）比较可知，本系统需新增 2 套安全认证网关服务（互联网 2 套）。

2、电子认证服务

本系统采用独立域名发布，原有域名证书无法复用，需申请 1 张域名证书。新增 2 套安全认证网关服务，需申请 2 张设备证书。

5.2.3 设备和计算安全

（一）密码功能设计

1、通过调用密码支撑平台提供的签名验签服务，使用基于SM2密码算法的数字证书及其SM2密码算法对应用服务器中重要可执行程序和文件进行数字签名，使用或读取这些程序和文件时，通过签名验签服务进行验签以确认其完整性和来源真实性。

2、通过调用密码支撑平台提供的签名验签服务，基于SM2密码算法对服务器虚拟机、数据库等设备日志和访问控制信息进行完整性保护。

3、密码服务的设备和计算安全相关指标要求由其配套的密码产品自身实现。

（二）资源配置估算

智能密码钥匙按需配置，签名验签服务复用已有密码资源，SSL VPN 由云平台提供。

5.3 密码支撑平台方案

不涉及密码支撑平台的建设或结构性调整，密码支撑平台方案略。

（对于新建密码支撑平台的情形，需根据新部署的密码设备/密码资源或其他结构性调整进行设计并给出相应的方案。）

5.4 业务应用的密码应用方案

（一）密码功能设计

1、在互联网PC端部署安全浏览器（含密码模块）并向相关用户配发智

能密码钥匙，签发基于SM2密码算法的数字证书，通过调用密码支撑平台的安全认证网关服务，基于SM2密码算法的签名验签机制，对互联网PC端用户进行身份鉴别，防止非授权人员访问应用；通信数据的安全防护由网络和通信层面的安全认证网关及其承载的加密通信信道实现。

2、通过调用密码支撑平台的数据加解密服务，分别使用SM4-CBC算法和基于SM2密码算法的数字信封对互联网PC端用户身份鉴别数据、电子公文数据进行存储机密性保护，实现身份鉴别数据、电子公文数据等重要数据的防泄露。

3、通过调用密码支撑平台的签名验签服务，使用SM2密码算法对应用用户访问权限控制列表、用户身份鉴别数据和业务日志数据进行完整性保护，防止被非授权用户篡改。

4、通过调用密码支撑平台提供的电子签章服务、时间戳服务，基于SM2密码算法对电子公文数据进行数字签名，并加盖时间戳，实现电子公文数据的完整性保护以及文件签发人操作行为的不可否认性。

（二）资源配置估算

本系统面向互联网提供服务，系统性能测算如下：

系统签名验签每秒最大签名次数：800次，每秒最大验签次数：700次；

系统时间戳每秒最大签名次数：800次，每秒最大验签次数：700次；

系统电子签章每秒最大盖章次数：300次，每秒最大验章次数：200次。

1、签名验签服务估算

根据密码资源使用现状，结合本系统性能测算数据，对签名验签服务的使用进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2)/(1-D)，说明如下：

X：签名验签服务估算数量。

A1：系统每秒最大签名次数。

A2：签名验签服务支持每秒最大签名次数。

B1：系统每秒最大验签次数。

B2：签名验签服务支持每秒最大验签次数。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

签名验签服务一般按其支持的每秒最大签名次数和验签次数这两项指标来计算性能负载，两项中资源使用占比较大的主要性能指标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 6 所示：

表 6 签名验签服务数量估算表

应用系统	系统每秒最大签名次数A1	签名验签服务支持每秒最大签名次数A2	系统每秒最大验签次数B1	签名验签服务支持每秒最大验签次数B2	密码设备计算负荷的冗余边界D	签名验签服务估算数量X
人事管理系统	500	9000	1000	6000	0.2	0.21
档案管理系统	1000	9000	3000	6000	0.2	0.63

电子公文处理系统	800	9000	700	6000	0.2	0.15
总计						0.99
签名验签服务基本需求（向上取整）						1
高可用需求数量						1
总计（签名验签服务需求总数）						2

根据上述估算表中签名验签服务需求总量 2 套与实际数量 1 套比较可知，本系统需新增 1 套签名验签服务。

2、时间戳服务估算

根据密码资源使用现状，结合本系统性能测算数据，对时间戳服务估算的使用进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2)/(1-D)，说明如下：

X：时间戳服务估算数量

A1：系统每秒最大签名时间戳次数。

A2：时间戳服务支持每秒最大签名时间戳次数。

B1：系统每秒最大验证时间戳次数。

B2：时间戳服务支持每秒最大验证时间戳次数。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

时间戳服务一般按其支持的每秒最大签名和验证时间戳次数这两项指标来计算性能负载，两项中资源使用占比较大的主要性能指标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 7 所示：

表 7 时间戳服务数量估算表

应用系统	系统每秒最大签名次数A1	时间戳服务支持每秒最大签名时间戳次数A2	系统每秒最大验签次数B1	时间戳服务支持每秒最大验签时间戳次数B2	密码设备计算负荷的冗余边界D	时间戳服务估算数量X
人事管理系统	500	9000	1000	6000	0.2	0.21
档案管理系统	1000	9000	3000	6000	0.2	0.63
电子公文处理系统	800	9000	700	6000	0.2	0.15
总计						0.99
时间戳服务基本需求（向上取整）						1
高可用需求数量						0
总计（时间戳服务需求总数）						1

根据上述估算表中时间戳服务需求总量 1 套与实际数量 1 套比较可知，原有服务可覆盖本系统需求，无需新增服务。

3、电子签章服务估算

根据密码资源使用现状，结合本系统性能测算数据，对电子签章服务的使用进行综合估算。估算公式为 X=MAX(A1/A2,B1/B2)/(1-D)，说明如下：

X：电子签章服务估算数量。

A1：系统每秒最大盖章次数。

A2：电子签章服务支持每秒最大盖章次数。

B1：系统每秒最大验章次数。

B2：电子签章服务支持每秒最大验章次数。

D：密码设备计算负荷的冗余边界，一般设为 20%（注：1-D 即为密码设备计算负荷的水位线）。

电子签章服务一般按其支持的每秒最大盖章和验章次数这两项指标来计算性能负载，两项中资源使用占比较大的主要性能指标是数量估算的主要依据。

按服务于不同网络的设备需独立估算原则，考虑高可用需求，估算如表 8 所示：

表 8 电子签章服务数量估算表

应用系统	系统每秒最大盖章次数A1	电子签章服务支持每秒最大盖章次数A2	系统每秒最大验章次数B1	电子签章服务支持每秒最大验章次数B2	密码设备计算负荷的冗余边界D	电子签章服务估算数量X
档案管理系统	300	800	100	1200	0.2	0.47
电子公文处理系统	300	800	200	1200	0.2	0.47
总计						0.94
电子签章服务基本需求（向上取整）						1
高可用需求数量						0
总计（电子签章服务需求总数）						1

根据上述估算表电子签章服务需求总量 1 套与实际数量 1 套比较可知，

原有服务可覆盖本系统需求，无需新增服务。

4、电子认证服务

本系统新增 1 套签名验签服务，需申请 1 张设备证书。

（三）密钥管理安全

本系统使用的域名证书和设备证书均由具有电子认证服务资质的机构签发并提供服务。

本系统通过调用密码支撑平台提供的安全认证网关、签名验签、电子签章、时间戳、数据加解密等密码服务，为应用系统提供密码应用安全保障。系统所涉及各类密钥由上述密码支撑服务提供密钥生存周期的安全保障。密码服务支撑平台已通过密码应用安全性评估（第三级）。

5.5 密码应用部署

本系统直接调用密码支撑平台提供的密码服务，根据上述密码功能设计，需调用安全认证网关、签名验签、电子签章、时间戳、数据加解密等密码服务。系统密码应用部署拓扑如图3所示。

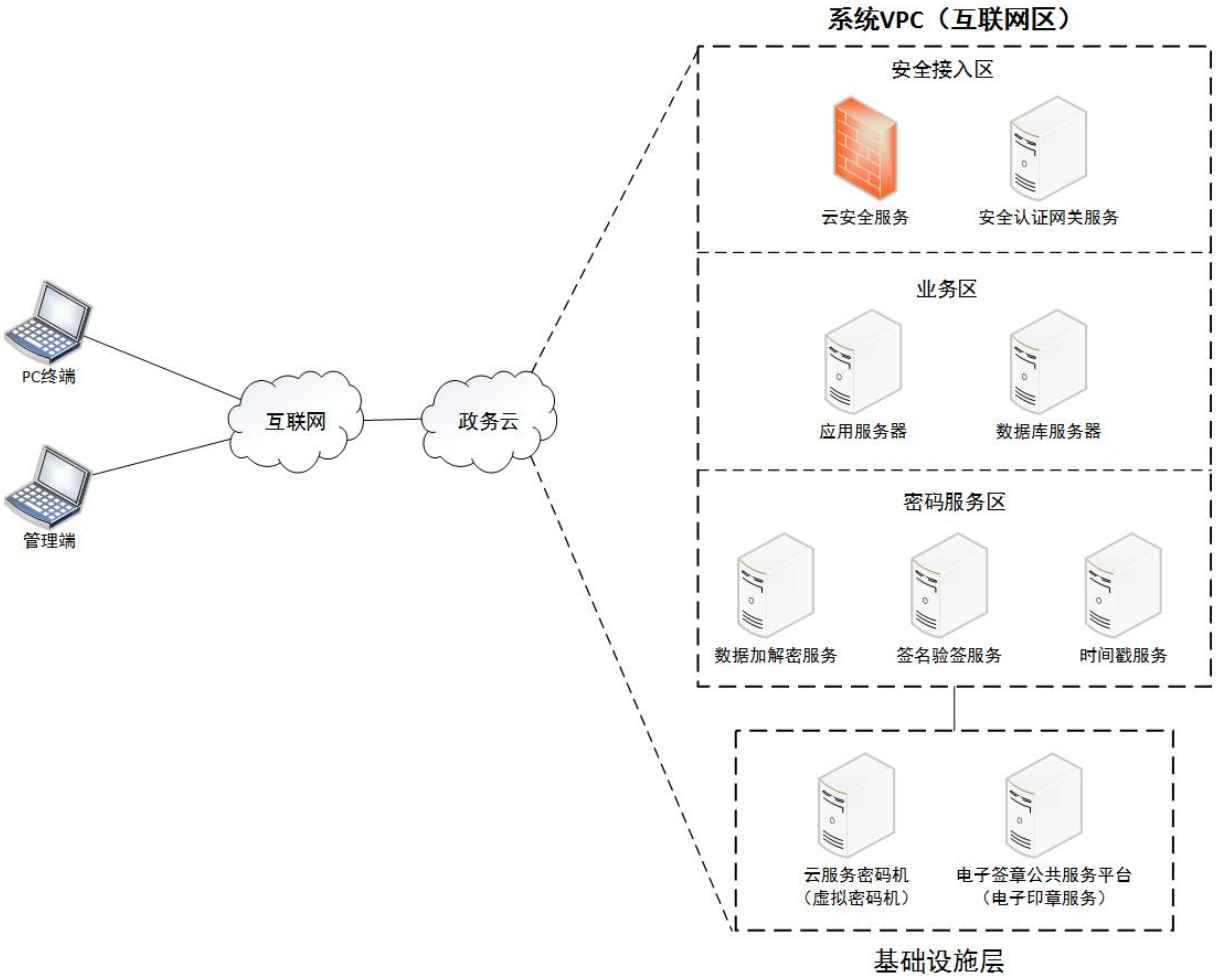


图 3 系统密码应用部署图

本系统需使用的密码服务清单如表9所示。

表 9 密码服务需求清单

序号	密码服务类型	数量	备注说明
1	安全认证网关服务	3	其中 1 套复用已有密码资源，2 套新增。
2	签名验签服务	2	其中 1 套复用已有密码资源，1 套新增。
3	数据加解密服务	/	无
4	时间戳服务	1	复用已有密码资源。

5	电子签章服务	1	复用已有密码资源。
6	电子认证服务（域名证书）	1	新增 1 个域名，需申请 1 张域名证书。
7	电子认证服务（设备证书）	3	新增 2 套安全认证网关服务、1 套签名验签服务，需申请 3 张设备证书。
8	安全浏览器（含密码模块）	xx	互联网 PC 终端 xx 台，需配置 xx 套产品。
9	智能密码钥匙	xx	远程运维管理终端 xx 台、互联网 PC 终端 xx 台，各需配置 xx 套产品。

5.6 密码应用功能模块组成

基于密码支撑平台提供的安全认证网关、签名验签、数据加解密、电子签章、时间戳等密码服务以及系统的应用功能，需开发适配若干密码应用功能模块，以实现网络和通信、设备和计算、应用和数据等层面的密码应用功能。

以下仅为示例,针对具体系统应给出更为详尽的密码应用功能模块建设内容描述,包括模块实现的功能等。

1、用户身份认证机制模块

开发用户身份认证机制模块，通过签名验签等安全机制实现登录用户的身份鉴别。

2、业务重要数据安全传输模块

开发业务重要数据安全传输模块，调用密码支撑平台提供的安全认证网关服务接口，实现应用系统通信数据的机密性和完整性保护。

3、服务器虚拟机设备日志/访问控制信息完整性模块

开发服务器虚拟机设备日志/访问控制信息完整性模块，调用密码支撑平台提供的签名验签服务接口，实现服务器虚拟机、数据库等设备日志/访问控制信息的完整性保护。

4、重要可执行程序签名验签模块

开发重要可执行程序签名验签模块，调用密码支撑平台提供的签名验签服务接口，实现重要可执行程序的完整性、来源真实性保护。

5、用户访问控制信息签名验签模块

开发用户访问控制信息签名验签模块，调用密码支撑平台提供的签名验签服务接口，实现应用系统登录用户的访问控制列表完整性保护。

6、应用系统重要数据加解密模块

开发应用系统重要数据加解密模块，调用密码支撑平台提供的数据加解密服务接口，实现登录用户身份鉴别数据、电子公文数据等结构化、非结构化数据的存储机密性保护。

7、应用系统重要数据签名验签模块

开发应用系统重要数据签名验签模块，调用密码支撑平台提供的签名验签服务接口，实现登录用户身份鉴别数据、电子公文数据、业务日志的存储完整性保护。

8、电子公文电子签章模块

开发电子公文电子签章模块，调用密码支撑平台提供的时间戳服务、电子签章服务接口，实现系统内流转电子公文的公文签批不可否认性。

系统密码应用功能模块的开发适配总体工作量预估为2.5人•月。（注：对于建设投资规模为500万元以下的系统，其密码应用功能模块的开发适配

工作量可大致估计为2.5人·月；若系统功能及业务复杂度较高，则密码应用功能模块的开发适配工作量可相应调增，此时需列明相应的工作量估算明细）。

6 安全管理方案

6.1 管理制度

根据《密码应用基本要求》中安全管理制度方面的要求，制定与系统相适应的密码安全管理制度和操作规范，内容至少包含密码设计、建设、运维、人员、设备、密钥等六个方面，并同步在单位现有的制度发布流程中补充密码相关管理制度发布流程，待新制定的密码安全管理制度和操作规范内部评审通过后，按照密码相关管理制度发布流程予以发布并遵照执行。

密码安全管理制度和操作规范发布后，每年年底，在本单位内部组织专家和密码相关人员对密码安全管理制度和操作规范在使用过程中的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

6.2 人员管理

根据《密码应用基本要求》中人员管理的要求，完善系统现有人员管理制度。

1、设置密码专题培训机制，每六个月组织一次，由内部专业人员或聘请外部专家担任培训讲师，内容涉及密码相关法律法规、标准规范、密码

应用、密码应用安全性评估等多个方面，使相关人员了解密码相关法律法规，掌握密码应用基本原理，并遵照执行。

2、系统完成密码应用改造后，安排项目建设单位、相关密码产品厂商对本系统部署使用的密码产品开展操作培训，确保相关人员能够正确配置使用。

3、结合系统情况，分别设立密钥管理员、密码安全审计员、密码操作员等岗位，明确各岗位职责，每个岗位均由 2 人担任。

4、在现有的安全管理制度中，补充密码相关人员考核、奖惩、保密、调离制度，每年对密钥管理员、密码安全审计员、密码操作员组织一次考核，对考核成绩优异的予以表扬和奖励，考核成绩不合格者，进行批评教育；密钥管理员、安全审计员、密码操作员与单位签订保密协议，承担保密义务，相关人员若要调离岗位时，按照制定的人员调离制度承担相应的保密义务。

6.3 建设运行

完成本方案编制后，我单位将委托检测机构或组织专家评审会对本方案进行评估，并基于通过评估后的方案，合规、正确、有效地建设密码保障系统。

依据评估通过的密码应用方案完成建设后，我单位将委托检测机构对本系统进行密码应用安全评估或密码应用测评，通过后才能上线运行。

系统上线运行后，我单位会定期（每年至少一次）自行或委托检测机构对系统开展密码应用安全性评估，并根据评估意见进行整改。当系统在

运行过程中发现重大密码应用安全隐患时，须停止运行，制定整改方案，按照整改方案对系统进行整改，整改完成后自行或委托检测机构对系统开展密码应用安全性评估，评估通过后重新上线运行。

6.4 应急处置

根据《密码应用基本要求》关于应急处置的要求，完善系统现有应急管理制度，补充制定密码应用应急处置预案，做好应急资源准备，明确密码安全事件处理流程及其它管理措施。

7 安全与合规性分析

对方案的适用情况、采取的密码保障措施、采取的缓解及替代性措施及自评结果进行说明（详见表 10）：

1、若指标为适用，说明采取的密码保障措施或未采取的密码保障措施的情况（如采取的缓解及替代性措施）；

2、针对适用的指标，存在部分保护对象不适用的情况，论证其不适用性；

3、若指标为不适用，说明其不适用的理由。

表 10 密码应用合规性对照表

指标要求	密码技术应用点	GB/T 39786 密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
物理和环境安	身份鉴别	宜	适用	由云平台提供安全保障。复用云平台密评结果。	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
全	电子门禁记录数据存储完整性	宜	适用	由云平台提供安全保障。复用云平台密评结果。	/	通过
	视频监控记录数据存储完整性	宜	适用		/	通过
网络和通信安全	身份鉴别	应	适用	通过调用密码支撑平台部署的安全认证网关服务，对业务通信链路的服务端进行身份鉴别； 通过调用云平台部署的SSL VPN，对运维管理链路的服务端进行身份鉴别。（远程运维通信信道复用云平台密评结果。）	/	通过
	通信数据完整性	宜	适用	通过调用密码支撑平台部署的安全认证网关服务，通过TLCP通信协议实现用户与系统通信数据的机密性和完整性保护； 通过调用云平台部署的SSL VPN,基于TLCP通信协议对运维管理数据进行传输机密性和完整性保护。（远程运维通信信道复用云平台密评结果。）	/	通过
	通信过程中重要数据的机密性	应	适用		/	通过
	网络边界访问控制信息的完整性	宜	适用	由安全认证网关服务、SSL VPN等密码产品提供网络边界访问控制信息完整性保护。（远程运维通信信道复用云平台密评结果。）	/	通过

指标要求	密码技术应用点	GB/T 39786 密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	安全接入认证	可	不适用	/	无外部设备接入本系统的需求。	通过
设备和计算安全	身份鉴别	应	适用	向远程运维管理员配发智能密码钥匙，对访问堡垒机、服务器、数据库的用户进行身份鉴别，并通过调用云平台部署的 SSL VPN 建立安全的远程管理信息传输通道。	堡垒机、服务器虚拟机、数据库登录时的身份鉴别未使用密码技术，通过云平台部署的 SSL VPN 双向鉴别降低风险。	通过
	远程管理通道安全	应	适用			通过
	系统资源访问控制信息完整性	宜	适用	通过调用密码支撑平台提供的签名验签服务，基于 SM2 密码算法对服务器虚拟机、数据库等设备的访问控制信息进行完整性保护。密码服务访问控制信息的完整性保护由其配套的密码产品自身实现。	/	通过
	重要信息资源安全标记完整性	宜	不适用	/	本系统不涉及重要信息资源的安全标记。	通过
	日志记录完整性	宜	适用	通过调用密码支撑平台提供的签名验签服务，基于 SM2 密码算法对服务器虚拟机、数据库等设备的日志进行完整性保护。密码服务日志记录完整性保护由其配套的密码产品自身实现。	/	通过
	重要可执行程序完整性、重	宜	适用	通过调用密码支撑平台提供的签名验签服务，使用基于 SM2 密	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	要可执行程序来源真实性			码算法的数字证书及其SM2密码算法对应用服务器中重要可执行程序和文件进行数字签名，实现应用服务器中重要可执行程序和文件完整性保护和来源真实性保护。		
应用和数据安全	身份鉴别	应	适用	在系统互联网和PC端部署安全浏览器（含密码模块），并向相关用户配发智能密码钥匙，通过调用密码支撑平台的身份鉴别服务，基于SM2密码算法的签名验签机制，对互联网PC端用户进行身份鉴别。	/	通过
	访问控制信息完整性	宜	适用	通过调用密码支撑平台的签名验签服务，使用SM2密码算法对应用用户访问权限控制列表进行完整性保护。	/	通过
	重要信息资源安全标记完整性	宜	不适用	/	本系统不涉及重要信息资源的安全标记。	通过
	重要数据传输机密性	应	适用	通过调用密码支撑平台的数据加解密服务，分别使用SM4-CBC算法和基于SM2密码算法的数字信封对互联网PC端用户身份鉴别数据、	通过网络和通信层面的密码技术，对重要数据的传输机密性和完整性进行弥补和降	通过
	重要数据存储机密性	应	适用			通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	重要数据传输完整性	宜	适用	电子公文数据进行存储机密性保护。 通过调用密码支撑平台的签名验签服务，使用SM2密码算法对用户身份鉴别数据和业务日志数据进行存储完整性保护。 通过调用密码支撑平台的安全认证网关服务实现身份鉴别数据、电子公文数据、业务日志数据等重要数据的安全传输防护。	低风险。	通过
	重要数据存储完整性	宜	适用			通过
	不可否认性	宜	适用	通过调用密码支撑平台提供的电子签章服务、时间戳服务，基于SM2密码算法对电子公文数据进行数字签名,并加盖时间戳，实现电子公文数据的完整性保护以及文件签发人操作行为的不可否认性。	/	通过
管理制度	具备密码应用安全管理制度	应	适用	制定密码应用安全管理制度	/	通过
	密钥管理规则	应	适用	制定密钥管理规则	/	通过
	建立操作规程	应	适用	建立操作规程	/	通过
	定期修订安全管理制度	应	适用	定期修订安全管理制度	/	通过
	明确管理制度发布流程	应	适用	明确管理制度发布流程	/	通过
	制度执行	应	适用	留存制度执行过程记	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
	过程记录留存			录		
人员管理	了解并遵守密码相关法律法规和密码管理制度	应	适用	对密码相关法律法规和密码管理制度进行定期培训	/	通过
	建立密码应用岗位责任制度	应	适用	建立密码应用岗位责任制度	/	通过
	建立上岗人员培训制度	应	适用	建立上岗人员培训制度	/	通过
	定期进行安全岗位人员考核	应	适用	定期对安全岗位人员进行考核	/	通过
	建立关键岗位人员保密制度和调离制度	应	适用	建立关键岗位人员保密制度和调离制度	/	通过
建设运行	制定密码应用方案	应	适用	制定密码应用方案	/	通过
	制定密钥安全管理策略	应	适用	制定密钥安全管理策略	/	通过
	依据密码应用方案实施建设	应	适用	依据密码应用方案实施建设	/	通过
	投入运行前进行密码应用安全性评估	应	适用	系统投入运行前进行密码应用安全性评估	/	通过
	定期开展密码应用安全性评估及攻防对抗演习	应	适用	定期开展密码应用安全性评估及攻防对抗演习	/	通过
应急	应急策略	应	适用	制定密码应用应急策	/	通过

指标要求	密码技术应用点	GB/T 39786密码应用基本要求	适用情况（适用/不适用）	采取的密码保障措施	说明（如采取的缓解及替代性措施）	自评结果（通过/未通过）
处置				略		
	事件处置	应	适用	制定密码应用事件处置规范	/	通过
	向有关主管部门上报处置情况	应	适用	向有关主管部门上报处置情况	/	通过

8 实施保障方案

8.1 实施内容

1、项目实施内容

本项目主要对我单位电子公文处理系统进行密码应用改造，以达到《密码应用基本要求》对信息系统密码应用安全第三级的要求，合规、正确、有效地使用商用密码对系统进行保护，并通过密码应用安全性评估。

本项目将依据方案中确定的密码应用需求、密码应用设计方案，使用经检测认证合格的密码产品、服务，对现有的应用进行开发改造、系统集成、联调测试等方式建设密码技术体系；依据安全管理方案，制定密码安全相关人员、制度、业务、运维、应急等方面的管理措施，同步建立密码安全管理体系。

2、可能存在的风险点及应对措施

密码应用改造可能会给系统带来一定风险，主要风险及其规避方法如下：

1）影响系统正常运行的风险：应用系统密码模块开发改造、联调测试、

试运行等环节。

规避方法：在测试系统中进行充分测试，选择夜间或休息日进行线上联调测试，确保系统运行稳定性和可用性。

2）项目延期：方案编制、招标、改造、验收测试等环节。

规避方案：制定细致的实施计划，并严格遵照执行，设立周报制度，每周汇报进度，进度不达标的地方及时进行督促，确保项目进度。

8.2 实施计划

本项目实施周期为XX个月，自20XX年XX月开始，至20XX年XX月。

1、项目总体进度及阶段性节点如下：

1）20XX年XX月，完成密码应用方案设计，并通过评估；

2）20XX年XX月，完成密码应用改造；

3）20XX年XX月，完成系统改造后的密码应用安全性评估或密码应用测评，并上线试运行；

4）20XX年XX月，完成系统运行效率、使用效果的后评价工作，并通过项目验收。

2、项目详细进度计划如表11所示。

表 11 项目详细进度计划

阶段	时间节点	工作内容	实施主体	阶段性节点
密码应用改造方案设计	20XX 年 XX 月	密码应用方案沟通研讨，确定改造内容和范围。	系统建设单位	
		开展密码应用方案设计，确定项目总体整体架构，明确项目实施周期和关键时间节点。		
		开展详细的密码应用方案编制，完成系		

		统现状分析、密码应用需求分析、技术方案、安全管理方案和实施保障方案等内容的编制。		
		根据密码应用的场景及方案设计内容。		
		对方案进行评估。	检测机构	密码应用方案通过评估
选择集成商	20XX 年 XX 月	选择集成商，负责系统的密码应用改造。	系统建设单位	选择密码应用改造集成商
密码应用改造	20XX 年 XX 月 -20XX 年 XX 月	根据密码应用技术方案中的软硬件密码产品/服务清单，采购密码产品或申请密码服务。	系统建设单位、系统集成商	完成本系统密码保障体系中的技术体系建设
		根据密码应用技术方案，复用系统所在机房电子门禁系统、视频监控系统。		
		根据密码应用技术方案，对系统网络和通信层面的身份鉴别、网络传输通道、集中管理通道等方面的安全需求进行密码应用改造。		
		根据密码应用技术方案，对系统设备和计算层面的管理员登录身份鉴别、远程管理身份鉴别信息传输、访问控制信息、重要应用程序、日志记录等方面的安全需求进行密码应用改造。		
		根据密码应用技术方案，对系统应用和数据层面的访问用户身份鉴别数据、电子公文数据、业务日志数据等方面的安全需求进行密码应用。		
		根据安全管理方案，设计密码安全管理制度、人员管理、设备管理、应急处置等方面的管理体系。		完成本系统密码保障体系中的管理体系设计
测评	20XX 年 XX 月	选择检测机构。	系统建设单位	选择检测机构
		检测机构依据评估通过的密码应用方案对改造后的系统进行密码应用安全性评估或密码应用测评。	检测机构	完成系统密码应用改造后的密码应用安全性评估或密码应用测评
试运行	20XX 年 XX 月	开展系统试运行、收集试运行期间的性能，效率、安全状态等数据，根据试运行情况做进一步评估和优化。	系统建设单位	开始试运行
项目验收	20XX 年 XX 月	完成系统运行效率、使用效果的后评价工作，根据评价结果进行项目验收。	系统建设单位	通过项目验收

8.3 保障措施

8.3.1 组织和人员保障

我单位将该项目作为重点任务，在项目组织上本着“统一领导、健全组织、合理分工、密切协作”的原则，明确项目组织形式，设置项目组织架构，按照职责分工开展工作，为顺利实施密码应用改造项目，高质量、高效率完成密码应用改造提供组织保障。

项目组织形式见图4，各组工作实行组长负责制。

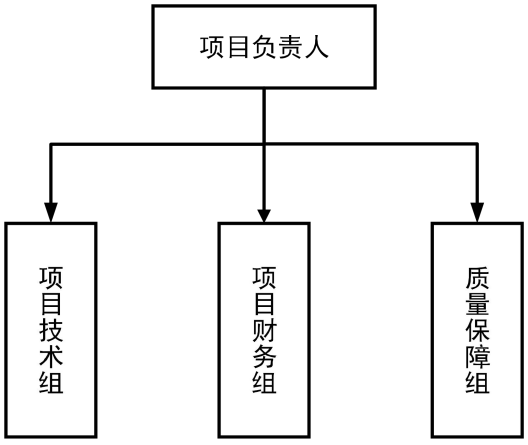


图 4 组织结构图

各组人员组成及工作职责如表12所示。

表 12 组织人员构成表

序号	名 称	人员组成	工作职责
1	项目负责人	张三	总体负责项目的技术、组织和财务等方面工作，宏观把握项目改造内容和建设目标。
2	项目技术组	组长：李四 组员：	由项目负责人及项目骨干组成，负责项目总体管理、各部分工作协调、项目进展情况和项目完成情况的监督检查、项目改造后的质量把关。
3	项目财务组	组长：李四 组员：	由本单位财务部门负责人和骨干组成，负责项目执行过程中的经费管理。
4	质量保障组	组长：李四 组员：	负责按照本项目制定的质量保障措施，落实质量监督和管理。

8.3.2 经费保障

本项目执行过程中，将严格按照单位资金使用管理办法，进行经费使用，确保经费使用合规。

8.3.3 质量保障

在项目建设实施过程中，通过组织项目定期会议，保障实施工作按计划进行；同时对于项目实施过程中出现的偏差或问题，及时沟通协调，必要时通过项目技术组向项目负责人进行汇报，并形成相应的决策意见和修订方案。

1、项目例会制度

项目通过定期例会和不定期会议来跟踪项目进度，反馈和讨论项目实施过程中的问题，对项目技术方案进行评审，对计划完成情况进行总结和说明，同时对后续计划进行确认。在遇到技术障碍或方案涉及重大变更时，通过不定期会议，由项目技术组或质量保障组讨论决策，针对出现的变更或重大问题进行及时修正，并制定相应的措施和方案。

2、项目周报机制

由项目技术组制定项目进展周报机制，每周五提交本周的项目进展、阶段成果、遗留问题和下周计划，质量保障组对项目进度进行统筹跟踪，协调相关人员和资源，保障项目如期完成。

3、风险管理机制

项目在实施过程中，建立完善的风险管理机制，包括项目风险的识别、评估和管理，从资金、成本控制、采购合规、技术、人才、管理等多个方面进行风险管控，包括确定风险发生时的备选方案、资金、设备和人员等；

定期检查和评估风险消减措施是否有效；定期进行风险排查；制定风险应对的启动机制等措施。

8.3.4 监督检查

监督检查是保证项目实施各阶段的活动顺利开展的重要措施，拟通过如下几类活动开展监督检查工作：

阶段评审：在系统实施过程中，定期地或阶段性地对系统和文档进行评审。在本项目中拟进行以下三次评审：第一次评审方案合理性、确认验收方法；第二次评审方案的实施计划，实施步骤、测试方法，试运行方案等，并对第一次评审结果复核；第三次评审功能和综合检查。阶段评审要组织专门的评审小组，评审小组原则上由实施小组成员、用户项目管理小组成员、我公司代表等构成。

日常检查：在本项目实施过程中，督促各子系统填写项目进展报告，即各个设备调试进展报告、软件安装部署阶段进度表、项目完成情况表等三张表格。项目管理人员可以通过项目进展报告发现有关项目实施过程中的问题。

8.4 经费概算

8.4.1 密码产品/服务费用列表

密码产品/服务费用详见表 13。

表 13 密码产品/服务费用列表（仅为示例）

序号	类别	在示例中提供的密码功能	单价（万元）	数量	总价（万元）
1	安全认证网关服务（含	为互联网用户提供安全接入通道；配合 PC 端部署的安全	/	3（其中，复用 1 套，	/

	虚拟密码机）	浏览器（含密码模块），实现PC端到服务端之间数据传输机密性和完整性保护。		新增2套。）	
2	签名验签服务（含虚拟密码机）	供系统调用，通过数字签名技术对系统重要数据进行完整性保护。	/	2（其中，复用1套，新增1套。）	/
3	数据加解密服务（含虚拟密码机）	对互联网PC端用户身份鉴别数据、电子公文数据进行存储机密性保护。	/	/	/
4	时间戳服务（含虚拟密码机）	基于SM2密码算法对电子公文数据进行数字签名，并加盖时间戳，实现电子公文文件签发人操作行为的不可否认性。	/	1（复用）	/
5	电子签章服务（含虚拟密码机）	基于SM2密码算法对电子公文数据进行数字签名，并加盖电子签章，实现电子公文数据的完整性保护以及文件签发人操作行为的不可否认性。	/	1（复用）	/
6	电子认证服务（域名证书）	为域名申请数字证书，用于保证信息传输的机密性，确认网站的真实性。	1	1（新增）	1
7	电子认证服务（设备证书）	为安全认证网关服务、签名验签服务等设备申请数字证书，用来证明设备的身份信息。	0.6	3（新增）	1.8
8	安全浏览器（含密码模块）	确保设备管理员安全登录堡垒机，互联网用户安全访问系统。	/	XX	/
9	智能密码钥匙	为设备管理员登录堡垒机、系统用户/管理员登录系统进行身份鉴别。	/	XX	/

8.4.2 密码应用功能模块开发费列表

密码应用功能模块开发费用详见表14。

表14 密码应用功能模块开发费列表（仅为示例）

序号	类别	人·月	单价（万元）	总价（万元）
1	密码应用功能模块	2.5	2	5

附录 4

密钥管理策略设计指南

1、密钥产生

密码在符合 GB/T 37092 规定的密码产品中产生。明确信息系统中密钥的产生方式和来源，密钥产生的同时记录密钥关联信息，包括密钥种类、长度、拥有者、使用起始时间和使用终止时间等。

2、密钥分发

密钥分发时保证密钥的机密性、完整性以及分发者、接收者身份的真实性等，确定密钥与实体的关联关系，并建立密钥介质的管理规范。

3、密钥存储

明确各类型密钥存储的位置和方式，如密钥在符合 GB/T 37092 的密码产品中存储或在对密钥进行机密性和完整性保护后，存储在通用设备或系统中。除公钥外，密钥不以明文方式存储在密码产品外部并采取严格的安全防护措施，防止密钥被非授权的访问或篡改。公钥可以明文方式存储在密码产品外部，但有必要采取安全防护措施，防止公钥被篡改。

4、密钥使用

明确各类型密钥的使用要求并按要求使用密钥，包括使用条件、时间和用途等。密钥一般在符合 GB/T 37092 规定的密码产品内部产生，且每个密钥一般只有单一的用途。公钥使用前需要验证其完整性，以及与实体的关联关系，确保公钥来源的真实性。

5、密钥更新

设定密钥更新策略，包括密钥的更新周期、更新机制、更新流程，以及保障密钥更新前后业务连续性的措施，并指定密钥更新人员。在密钥超过使用期限、泄露或存在泄露风险时，根据相应的密钥更新策略进行更新。

6、密钥归档

如果信息系统有密钥归档需求，明确密钥归档的条件、人员和流程，并确定归档密钥的存储位置、存储方式以及管理者。根据安全需求采取有效的安全措施，保证归档密钥的安全性和正确性。归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。执行密钥归档时，生成审计信息，包括归档的密钥和归档的时间等。

7、密钥撤销

明确密钥的撤销条件、撤销流程、撤销机制和撤销人等，以及撤销后密钥的处理方式等。

8、密钥备份

指定备份操作人员、备份密钥管理人员，制定备份密钥管理机制、备份密钥恢复流程以及备份密钥存档要求等。明确密钥备份的机密性、完整性以及与实体和其他信息的关联关系。对密钥备份过程进行记录，并生成审计信息，审计信息包括备份的主体和备份的时间等。

9、密钥恢复

制定密钥恢复要求与机制，确定密钥恢复流程，指定密钥恢复操作员。对密钥恢复过程进行记录，并生成审计信息，审计信息包括恢复的主体和恢复的时间等。

10、密钥销毁

制定密钥销毁相关要求，根据密钥存储介质情况确定密钥销毁模式，明确密钥销毁机制、销毁启动条件（设备失控、丢弃时进行密钥销毁），以及销毁操作方法、操作流程和操作人员。

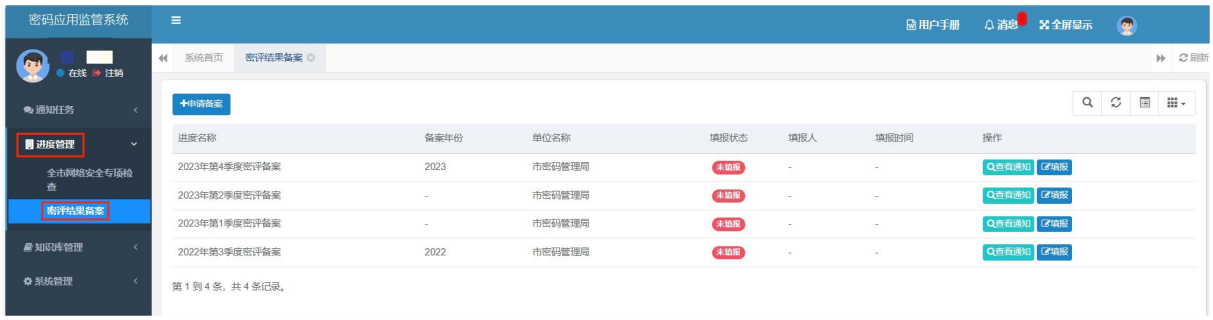
附录 5

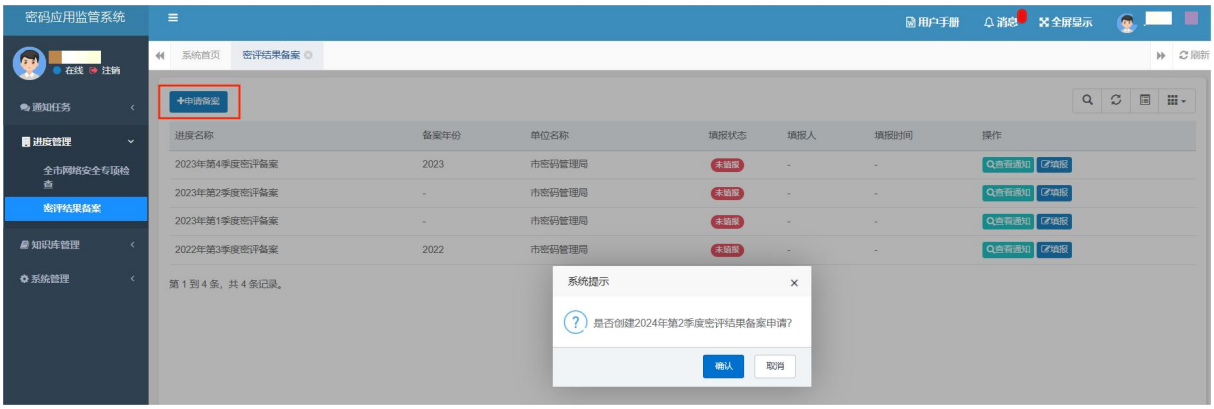
密码应用安全性评估（密评）结果备案流程

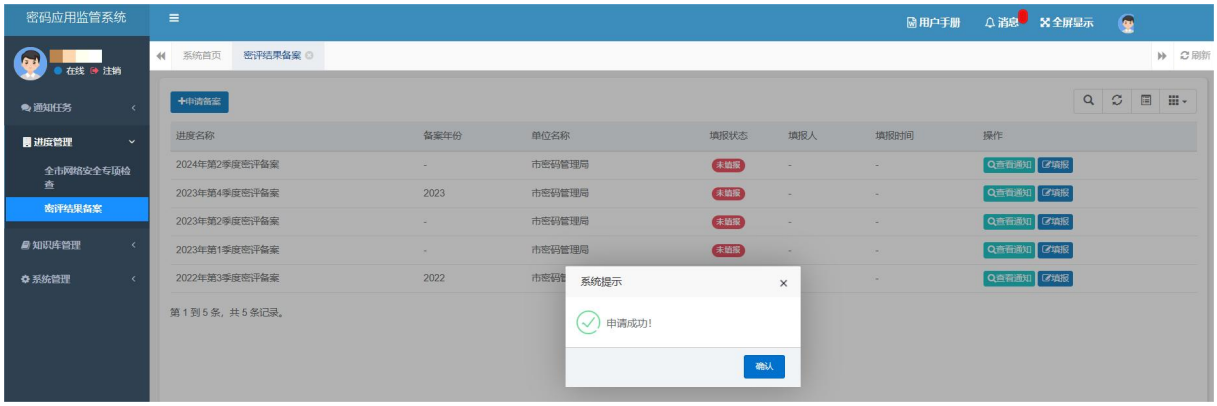
信息系统建设、使用、管理单位（以下简称责任单位）应自密评报告形成之日起 30 日内通过密码应用监管平台进行密评结果备案，具体流程如下：

1、责任单位登录访问密码应用监管平台（互联网 https://mgj.sh.gov.cn:2003，政务外网 https://10.86.129.166:2003）。新用户需先进行注册，管理员审核后，平台将注册成功或失败信息通过邮件和短信发送至用户注册时填写的邮箱和手机号，注册成功后方可登录平台。

2、责任单位登录密码应用监管平台后，选择“进度管理”-“密评结果备案”，点击“申请备案”，根据平台提示操作。

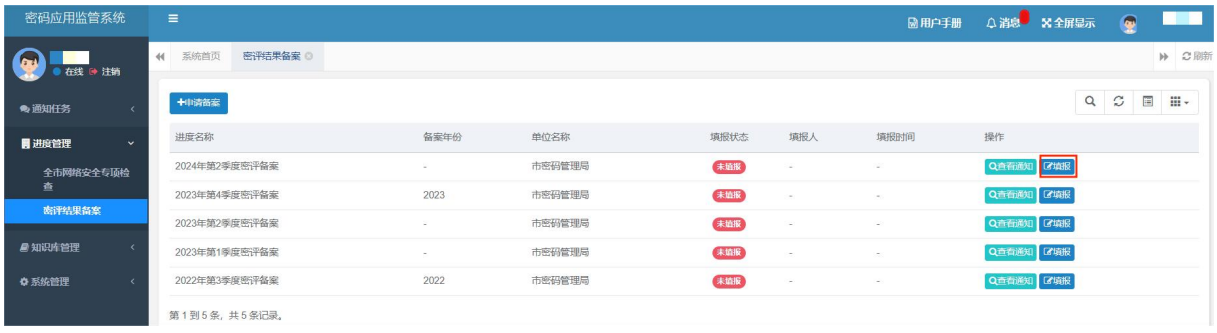


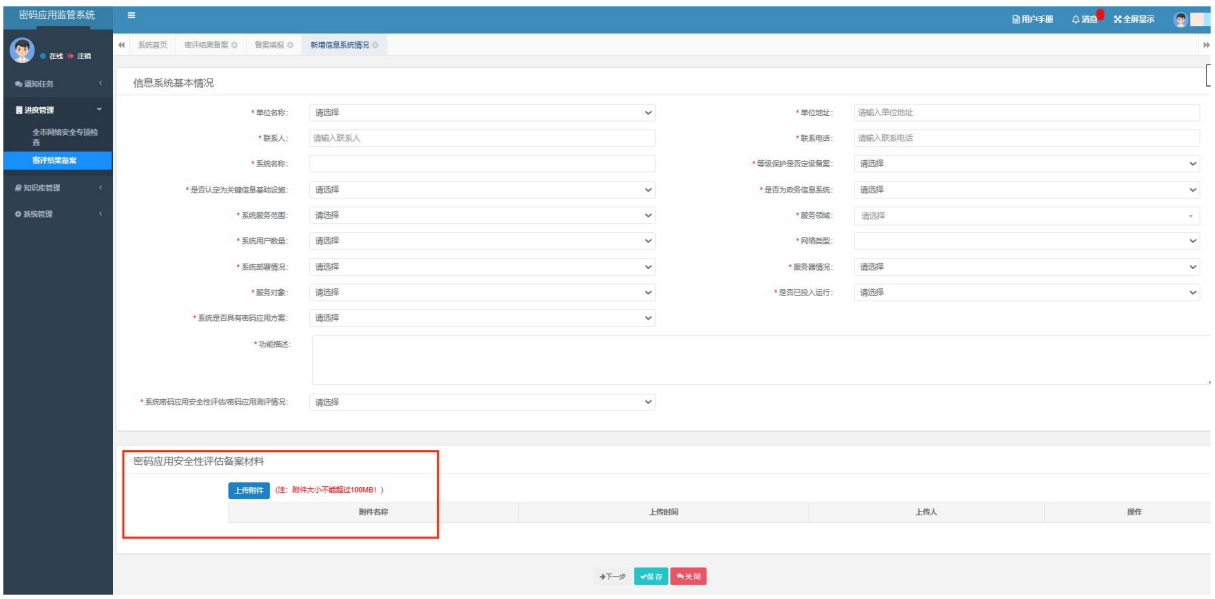




3、密评结果备案进度建立后，点击进度栏中的“填报”。若申请备案的信息系统首次在平台填报，选择“新建”，进入填报页面。若申请备案的信息系统之前已在平台有填报记录，则该系统会自动显示在页面上，点击“操作”栏中的“添加”，按平台提示点击“确认”，再点击“编辑”，进入填报页面。一个（套）信息系统需填写“信息系统基本情况”“密码应用情况”两个页面（相关操作请阅读页面右上角的“用户手册”），并在“信息系统基本情况”页面最下方上传“XX 系统商用密码应用安全性评估报告”（报告模板请参见上海市密码管理局互联网门户网站

（https://mgj.sh.gov.cn）--通知公告--商用密码应用安全性评估报告（2023 版））。





4、完成信息系统填写后，在“备案填报”页面点击“操作”栏中的“提交”，完成提交。

5、市密码管理局审核后给出“审核通过”或者“审核拒绝”。备案单位通过查看“审核状态”了解审核进度。若“审核状态”显示为“审核拒绝”，点击“审核拒绝”获知具体修改意见。

6、密评结果备案材料通过审核后，责任单位点击该备案系统“操作”栏中的“查看”，在“信息系统基本情况”页面最下方选择需要的回执类型：无章版回执、盖章版回执（扫描件）、盖章版回执（纸质件）。“盖章版回执（纸质件）”需填写收件人、手机号、收件地址，市密码管理局通过快递到付方式寄送。责任单位可通过“回执状态”了解进度，“回执状态”显示为已办理后，若申请的是“盖章版回执（扫描件）”，点击“盖章版回执（扫描件）”下载；若申请的是“盖章版回执（纸质件）”，等待快递送达。

附录 6

商用密码检测机构

相关机构信息请参见国家密码管理局门户网站《商用密码应用安全性评估试点机构目录》。上海市商用密码检测机构相关信息见下表。

序号	机构名称	联系人	联系方式
1	智巡密码（上海）检测技术有限公司	史为国	15618089855 021-60700168
2	上海市信息安全测评认证中心	朱少辉	18521525799
3	公安部第三研究所	杨元原	18721525396 021-64336810-1807

附录 7

电子认证服务机构

相关机构信息请参见工业和信息化部门户网站。上海市电子认证服务机构相关信息见下表。

序号	机构名称	联系电话
1	上海市数字证书认证中心有限公司	021-962600 021-36393170
2	亚数信息科技（上海）有限公司	4008808600

电子政务电子认证服务机构

相关机构信息请参见国家密码管理局门户网站《电子政务电子认证服务机构目录》。上海市电子政务电子认证服务机构相关信息见下表。

序号	机构名称	联系电话
1	上海市数字证书认证中心有限公司	021-962600 021-36393170