

崇左市退役军人事务局

边境英烈云祭扫小程序

密码应用方案

建设单位：

崇左市退役军人事务局

编制时间：

2025年12月



目录

1 背景 -----	1
1.1 项目概况 -----	1
1.2 政策依据 -----	1
2 系统概述 -----	3
2.1 基本情况 -----	3
2.2 计算平台现状 -----	3
2.2.1 物理环境 -----	3
2.2.2 网络环境 -----	4
2.2.3 计算环境 -----	4
2.3 业务应用现状 -----	5
2.3.1 关键业务应用 -----	5
2.3.2 被保护对象 -----	6
3 密码应用需求分析 -----	7
3.1 物理和环境安全 -----	7
3.2 网络和通信安全 -----	7
3.3 设备和计算安全 -----	10
3.4 应用和数据安全 -----	10
3.5 管理制度 -----	11
3.6 人员管理 -----	12
3.7 建设管理 -----	13
3.8 应急处置 -----	13
4 安全目标及设计原则 -----	13
4.1 安全目标 -----	13
4.2 设计原则与依据 -----	14
4.2.1 信息系统密码应用方案设计原则： -----	14
4.2.2 设计依据 -----	14
5 密码应用设计 -----	17
5.1 密码应用技术框架 -----	17

5.2 计算平台密码应用方案 -----	18
5.2.1 物理和环境安全 -----	18
5.2.2 网络和通信安全 -----	18
5.2.3 设备和计算安全 -----	20
5.3 密码支撑平台方案 -----	21
5.3.1 身份鉴别服务 -----	22
5.3.2 数据传输机密性和传输完整性保护服务 -----	22
5.3.3 数据存储机密性和存储完整性保护服务 -----	22
5.4 业务应用的密码应用方案 -----	23
5.5 密钥管理安全 -----	25
5.6 密码应用部署 -----	26
5.7 密码产品清单 -----	27
5.7.1 已有密码产品清单 -----	27
5.7.2 需新增密码产品清单 -----	28
6 安全管理方案 -----	28
6.1 管理制度 -----	29
6.2 人员管理 -----	29
6.3 建设运行 -----	30
6.4 应急处置 -----	30
7 安全与合规性分析 -----	32
8 实施保障方案 -----	38
8.1 实施内容 -----	38
8.1.1 实施目标 -----	38
8.1.2 项目责任单位 -----	38
8.1.3 项目实施地点 -----	39
8.1.4 实施原则 -----	39
8.1.5 实施内容 -----	39
8.1.6 重要难点问题和风险控制 -----	39
8.2 实施计划 -----	39
8.2.1 实施路线 -----	40

8.2.2 实施进度计划 -----	40
8.3 保障措施 -----	41
8.3.1 组织保障 -----	41
8.3.2 人员保障 -----	41
8.3.3 经费保障 -----	41
8.3.4 技术保障 -----	42
8.3.5 质量保障 -----	42
8.3.6 监督检查 -----	43
附录 A 系统定级匹配证明 -----	44

1背景

1.1项目概况

为贯彻落实《中华人民共和国密码法》关于信息系统密码应用的要求，决定对该系统进行商用密码应用改造。

根据 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“《基本要求》”），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、安全管理等层面，对该平台进行风险分析，得出该平台密码应用需求。

1.2政策依据

本方案的内容及相关密码产品，符合国家相关指导思想及行业标准，主要参考以下依据：

序号	类型	政策法规（标准）名称
1	指导思想	《中华人民共和国密码法》
		《中华人民共和国电子签名法》
		《中华人民共和国网络安全法》
		《中华人民共和国数据安全法》
		《商用密码管理条例》
		《国家政务信息化项目建设管理办法》
		《国家网络空间安全战略》
		中共中央办公厅、国务院办公厅联合印发《关于加强重要领域密码应用的指导意见》（中办、国办发〔2015〕4号）
		国家密码局管理印发《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）
		广西壮族自治区人民政府办公厅关于印发《广西政务信息化项目建设管理办法（试行）》的通知（桂政办发〔2021〕21号）
2	密码应用改造参考标准	《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）
		《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）
		《信息安全技术 信息系统密码应用设计指南》（GBT 43207-2023）

		《商用密码应用安全性评估量化评估规则》（2023 版）
		《信息系统密码应用高风险判定指引》
3	产品（服务） 设计标准	《SM4 分组密码算法》（GM/T 0002-2014）
		《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）
		《SM3 密码杂凑算法》（GM/T 0004-2012）
		《SM2 密码算法使用规范》（GM/T 0009-2012）
		《数字证书认证系统密码协议规范》（GM/T 0014-2023）
		《基于 SM2 密码算法的数字证书格式规范》（GM/T 0015-2023）
		《智能密码钥匙应用接口规范》 GM/T 0016-2023
		《密码设备应用接口规范》（GM/T 0018-2023）
		《通用密码服务接口规范》（GM/T 0019-2023）
		《IPSec VPN 网关产品规范》（GM/T 0023-2023）
		《SSL VPN 技术规范》（GM/T 0024-2023）
		《SSL VPN 网关产品规范》（GM/T 0025-2023）
		《安全认证网关产品规范》（GM/T 0026-2023）
		《智能密码钥匙技术规范》（GM/T 0027-2014）
		《密码模块安全技术要求》（GM/T 0028-2024）
		《签名验签服务器技术规范》（GM/T 0029-2014）
		《服务器密码机技术规范》 GM/T 0030-2014
		《时间戳接口规范》（GM/T 0033-2023）
		《采用非接触卡的门禁系统密码应用技术指南》（GM/T 0036-2014）
		《证书认证密钥管理系统检测规范》（GM/T 0038-2014）
		《电子文件密码应用指南》（GM/T 0071-2019）
		《云服务器密码机技术规范》（GM/T 0104-2021）

2系统概述

2.1基本情况

本系统为：崇左市退役军人事务局边境英烈云祭扫小程序。

系统责任单位：崇左市退役军人事务局。

项目目标：通过“崇左市退役军人事务局边境英烈云祭扫小程序”的建设，通过打造官方、权威、公益的“边境英烈云祭扫小程序”，为社会公众、英烈家属及部队官兵提供一个便捷、庄严、绿色的数字化祭扫渠道，营造崇尚英烈、缅怀英烈、学习英烈、捍卫英烈的浓厚社会氛围，让红色基因与英雄精神在新时代得以永续传承。

所属密码管理部门为广西密码管理局。

系统上线运行时间：待定

应用系统未进行商用密码应用安全性评估相关工作，本系统已完成网络安全等级保护预定级备案，定级等级为第二级（S2A2G2），材料见附录 A

序号	应用系统 (子系统)	访问用户	访问网络及终端类型
1	边境英烈云祭扫 小程序管理平台	电子政务外网用户、单位 内部人员	互联网、电子政务外网的电脑终端
2	边境英烈云祭扫 小程序	互联网公众用户	手机终端

2.2计算平台现状

该平台部署环境情况具体如下：

2.2.1物理环境

表 2-1 物理环境

序号	物理环境名称	物理位置	重要程度
1	政务云平台机房	中国电信崇左政务云服务系统（二期）	非常 重要

其中系统部署在中国电信崇左政务云服务系统（二期），中国电信崇左政务云服务系统（二期）目前正在建设（以下简称云平台），建设根据 GB/T

39786—2021《信息安全技术 信息系统密码应用基本要求》第三级要求开展并通过密码应用评估。

2.2.2 网络环境

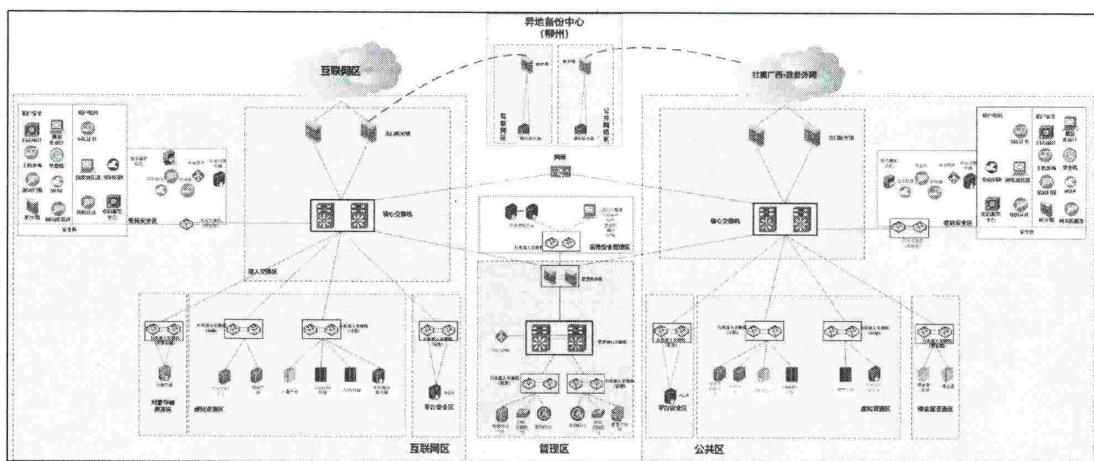


图 2-1 网络拓扑图

崇左市退役军人事务局边境英烈云祭扫小程序对互联网和电子政务外网提供服务。网络区域主要分为互联网接入区、政务外网接入区。

互联网接入区：部署有互联网网络安全防护设备，对互联网提供服务。

政务外网接入区：部署有政务外网网络安全防护设备，对政务外网提供服务。

PC 端用户在政务外网或互联网访问边境英烈云祭扫小程序管理平台，移动用户在互联网访问边境英烈云祭扫小程序。

2.2.3 计算环境

2.2.3.1 密码产品

系统为新建系统，目前没有使用密码产品。

2.2.3.2 服务器/存储设备

表 2-4 服务器/存储设备

序号	设备名称	生产厂商	型号	操作系统版本	是否为虚拟设备	用途	数量	重要程度

1	应用服务器	/	/	/	是	部署业务系统 应用程序	-	重要
2	数据库服务器	/	/	/	是	部署数据库、 存储业务数据	-	重要

2.2.3.3 网络及安全设备

表 2-5 网络及安全设备

序号	设备名称	生产厂商	型号	用途 (包括涉及的密码技术)	数量	重要程度
1	防火墙	依托云平台资源池提供		访问控制	/	重要
2	Web 应用防火墙	依托云平台资源池提供		应用层防护	/	重要
3	堡垒机	依托云平台资源池提供		设备管理	/	重要
4	数据库审计	依托云平台资源池提供		数据库行为审计	/	重要
5	漏洞扫描	网络基础安全		安全基线检查	/	重要
6	日志审计	网络基础安全		日志分析	/	重要
7	态势感知	网络基础安全		安全运维	/	重要
8	堡垒机	依托云平台资源池提供		集中运维管理	/	重要

2.2.3.4 数据库管理系统

表 2-6 数据库管理系统

序号	数据库管理系统 名称	版本	部署位置	主要功能	重要 程度
1	PolarDB 数据库	V2	数据库服务器	存储业务数据	重要
2	Redis 数据库	V5.0.4	数据库服务器	存储缓存数据	一般

2.3 业务应用现状

应用系统主要业务为：在线预约入园、云祭奠先烈、墓园 VR 全景展示。

2.3.1 关键业务应用

表 2-7 关键业务应用

序号	应用名称	版本	部署位置	主要功能
1	边境英烈云祭扫小程序	V1.0	应用服务器	为运维人员、运营人员、系统管

	程序管理平台			理员提供系统管理平台。
2	边境英烈云祭扫小程序	V1.0	应用服务器	为用户提供系统核心业务的操作界面与功能服务，包括信息查询、业务办理、交互反馈等。

2.3.2 被保护对象

表 2-8 被保护对象

序号	应用系统名称	数据	描述	安全需求
1	边境英烈云祭扫小程序 程序管理平台	应用用户	普通用户	真实性
2			管理员用户	真实性
3		鉴别数据	应用系统的用户口令	传输机密性 传输完整性 存储机密性 存储完整性
4		访问控制信息	权限数据，如用户和角色关联表、角色和菜单关联表	存储完整性
5		个人信息	用户个人信息（姓名、身份证件、家庭住址、电话、联系人）等	传输机密性 传输完整性 存储机密性 存储完整性
6			日志数据	包括系统中涉及的重要操作日志、登录日志等
7		业务数据	烈士信息、陵园信息、客服聊天信息	传输完整性 存储完整性
8		应用用户	普通用户	真实性
9			鉴别数据	传输机密性 传输完整性 存储机密性 存储完整性
10		访问控制信息	应用系统的用户口令	存储完整性
11			权限数据，如用户和角色关联表、角色和菜单关联表	传输完整性 存储完整性
12		个人信息	用户个人信息（姓名、身份证件、家庭住址、电话、联系人）等	传输完整性 存储完整性
13			日志数据	包括系统中涉及的重要操作日志、登录日志等
		业务数据	预约入园信息、云祭奠留言信息、客服聊天信息	传输完整性 存储完整性

3密码应用需求分析

根据 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“《基本要求》”），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、安全管理等层面，对该平台进行风险分析，得出该平台密码应用需求。

3.1物理和环境安全

1) 安全风险分析

1、身份鉴别

信息机房未采用密码技术对进出人员进行身份鉴别。

2、电子门禁记录数据存储完整性

信息机房未采用密码技术对电子门禁记录数据进行完整性保护。

2) 密码应用需求

1、身份鉴别

信息机房有采用密码技术对进出人员进行身份鉴别的需求。

2、电子门禁记录数据存储完整性

信息机房有采用密码技术对电子门禁记录数据进行完整性保护的需求。

机房应采用经商用密码认证机构认证合格的密码产品或遵循密码相关国家标准、行业标准的密码技术对重要物理区域出入人员的身份进行鉴别，防止被非授权实体进入侵害内部信息。

机房应使用经商用密码认证机构认证合格的密码产品或遵循密码相关国家标准、行业标准的密码技术对物理进出记录数据完整性进行保护，防止被非授权篡改。

3.2网络和通信安全

1) 安全风险分析

序号	安全层面	保护对象	说明
1	网络和通信安全	互联网移动端与边境英烈云祭扫小程序之间的业务通道	业务用户在互联网通过手机终端访问小程序或边境英烈云祭扫小程序。

序号	安全层面	保护对象	说明
2		互联网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道	运维人员、运营人员、系统管理员浏览器访问边境英烈云祭扫小程序管理平台。
3		政务外网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道	运维人员、运营人员、系统管理员浏览器访问边境英烈云祭扫小程序管理平台。
4		互联网 VPN 客户端与综合安全网关的通信信道	运维人员在互联网通过 VPN 访问运维管理系统。

1、互联网移动端与边境英烈云祭扫小程序之间的业务通道：互联网移动端与边境英烈云祭扫小程序之间的业务通道采用非国密 HTTPS 协议通信，没有采用合规的密码技术对通信实体进行身份鉴别，没有采用合规的密码技术保证通信数据的机密性和完整性，没有采用密码技术保证网络边界访问控制信息的完整性。

2、互联网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：没有采用密码技术对通信实体进行身份鉴别，没有采用密码技术保证通信数据的机密性和完整性，没有采用密码技术保证网络边界访问控制信息的完整性。

3、政务外网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：没有采用密码技术对通信实体进行身份鉴别，没有采用密码技术保证通信数据的机密性和完整性，没有采用密码技术保证网络边界访问控制信息的完整性。

4、互联网 VPN 客户端与综合安全网关的通信信道：VPN 运维通道未采用合规的密码技术对运维访问实体进行身份鉴别，未采用合规的密码技术保证运维数据的机密性和完整性，未采用密码技术保证 VPN 边界访问控制信息的完整性。

2) 密码应用需求

序号	安全层面	保护对象	说明
1	网络和通信安全	互联网移动端与边境英烈云祭扫小程序之间的业务通道	采用合规的密码技术对经互联网移动端接入的社会公众进行身份鉴别，采用合规的密码技术保证云祭扫业务数据的机密性和完整性，采用合规的密码技术保证网络边界访问控制信息的完整性。

序号	安全层面	保护对象	说明
2		互联网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道	采用合规的密码技术对经互联网浏览器接入的业务管理员进行身份鉴别，采用合规的密码技术保证管理平台数据的机密性和完整性，采用合规的密码技术保证网络边界访问控制信息的完整性。
3		政务外网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道	采用合规的密码技术对经政务外网浏览器接入的业务管理员进行身份鉴别，采用合规的密码技术保证管理平台数据的机密性和完整性，采用合规的密码技术保证网络边界访问控制信息的完整性。
4		互联网 VPN 客户端与综合安全网关的通信信道	采用合规的密码技术对经互联网拨入 VPN 访问堡垒机的运维人员进行身份鉴别，采用合规的密码技术保证远程运维数据的机密性和完整性，采用合规的密码技术保证 VPN 边界访问控制信息的完整性。

1、互联网移动端与边境英烈云祭扫小程序之间的业务通道：采用合规的密码技术对经互联网移动端接入的社会公众进行身份鉴别，采用合规的密码技术保证云祭扫业务数据的机密性和完整性，采用合规的密码技术保证网络边界访问控制信息的完整性。

2、互联网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：采用合规的密码技术对经互联网浏览器接入的业务管理员进行身份鉴别，采用合规的密码技术保证管理平台数据的机密性和完整性，采用合规的密码技术保证网络边界访问控制信息的完整性。

3、政务外网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：采用合规的密码技术对经政务外网浏览器接入的业务管理员进行身份鉴别，采用合规的密码技术保证管理平台数据的机密性和完整性，采用合规的密码技术保证网络边界访问控制信息的完整性。

4、采用合规的密码技术对经互联网拨入 VPN 访问堡垒机的运维人员进行身份鉴别，采用合规的密码技术保证远程运维数据的机密性和完整性，采用合规的

密码技术保证 VPN 边界访问控制信息的完整性。

3.3设备和计算安全

1) 安全风险分析

1、身份鉴别

用户通过用户名口令登录服务器、数据库进行运维管理，未使用密码技术对运维人员登录进行身份鉴别，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、系统资源访问控制信息完整性

服务器、数据库均未使用密码技术进行数据的完整性保护，存在访问控制信息被篡改的风险。

3、日志记录完整性

服务器、数据库均未使用密码技术进行完整性保护，存在设备日志记录被非法篡改、非法操作等风险。

2) 密码应用需求

1、身份鉴别

采用合规密码技术对登录用户进行身份鉴别的需求，防止非授权人员登录。

2、系统资源访问控制信息完整性

采用合规密码技术对系统资源访问控制信息进行完整性保护的需求。

3、日志记录完整性

有采用合规密码技术对服务器、数据库等设备日志记录进行完整性安全保护的需求。

3.4应用和数据安全

1) 安全风险分析

1、身份鉴别

普通用户：使用用户名、口令进行登录，未使用密码技术进行身份鉴别，存在无法确保登录用户身份真实性的风险；

管理员用户：使用用户名、口令进行登录，未使用密码技术进行身份鉴别，存在无法确保登录用户身份真实性的风险。

2、访问控制信息完整性

系统内的访问控制信息未做完整性保护，存在导致访问控制信息被攻击者篡改，且无法及时发现，攻击者通过修改后的访问控制信息访问敏感信息的风险。

3、重要数据传输机密性

采用无效的密码技术对鉴别信息进行传输机密性保护，存在数据被攻击者截获，造成数据泄露的风险。

4、重要数据存储机密性

采用无效的密码技术对鉴别信息进行存储机密性保护，可能会导致重要数据的数据被攻击者获取，造成数据泄露。

5、重要数据传输完整性

未采用密码技术对鉴别信息、重要业务信息进行传输完整性保护，可能导致重要数据被攻击者篡改，且无法及时发现的风险。

6、重要数据存储完整性

未采取密码技术对鉴别信息、日志信息、重要业务信息进行存储完整性保护，可能会导致重要数据被攻击者篡改，且无法及时发现的风险。

2) 密码应用需求

1、身份鉴别

对登录应用系统用户采用密码技术进行身份鉴别。

2、访问控制信息完整性

系统对不同角色的访问控制信息，采用密码技术对控制信息进行存储完整性保护。

3、重要数据传输机密性

采用合规的密码技术保障重要数据其传输过程中的机密性。

4、重要数据存储机密性

采用合规的密码技术保障重要数据其存储后的机密性；

5、重要数据传输完整性

采用合规的密码技术保障重要数据其传输过程中的完整性；

6、重要数据存储完整性

采用合规的密码技术保障重要数据其存储后的完整性；

3.5管理制度

1) 安全风险分析

目前本系统没有制定密码应用安全管理制度，没有包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；没有建立密钥管理规则，没有对密码相关管理人员或操作人员的日常管理操作建立操作规程，没有定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，没有修订记录，没有明确制度的发布流程和版本控制，没有密码应用操作规程执行过程中留存的相关执行记录文件。

3) 密码应用需求

根据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）制定密码应用安全管理制度，密码应用安全管理制度包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；建立相应的密钥管理规则，对密码相关管理人员或操作人员的日常管理操作建立操作规程，定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，并形成修订记录，明确制度的发布流程和版本控制，密码应用操作规程执行过程中应留存相关执行记录文件。

3.6 人员管理

1) 安全风险分析

没有核查系统相关人员是否了解并遵守密码相关法律法规和密码应用安全管理制度，没有建立密码应用岗位责任制度，没有设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位，没有定义岗位职责，没有对关键岗位建立多人共管机制，没有确认密码安全审计员岗位人员不兼任密钥管理员、密码操作员等关键安全岗位，没有核查相关设备与系统的管理和使用账号是否有多人共用的情况，没有建立上岗人员培训制度，没有定期进行安全岗位人员考核，没有建立关键岗位人员保密制度和调离制度。

2) 密码应用需求

定期核查系统相关人员是否了解并遵守密码相关法律法规和密码应用安全管理制度，建立密码应用岗位责任制度，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位并定义岗位职责，对关键岗位建立多人共管机制，确认密码安全审计员岗位人员不兼任密钥管理员、密码操作员等关键安全岗位，核查

相关设备与系统的管理和使用账号是否有多人共用的情况，建立上岗人员培训制度，定期进行安全岗位人员考核，建立关键岗位人员保密制度和调离制度。

3.7建设管理

1) 安全风险分析

在系统规划阶段，没有依据密码相关标准和信息系统密码应用需求制定密码应用方案，没有制定密钥安全管理策略，没有制定密码实施方案，没有在系统投入运行前进行密码应用安全性评估，没有定期开展密码应用安全性评估及攻防对抗演习。

3) 密码应用需求

在系统规划阶段，依据密码相关标准和信息系统密码应用需求制定密码应用方案并通过评审，制定密钥安全管理策略，根据密码应用方案制定密码实施方案，在系统投入运行前应进行密码应用安全性评估，定期开展密码应用安全性评估及攻防对抗演习。

3.8应急处置

1) 安全风险分析

没有根据密码应用安全事件等级制定相应的密码应用应急策略，没有明确密码应用安全事件发生时的应急处理流程及其他管理措施；没有制定事件处置制度，当密码应用安全事件发生后无法及时向信息系统主管部门进行报告；没有制定上报制度，无法及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

4) 密码应用需求

根据密码应用安全事件等级制定相应的密码应用应急策略并进行评审，明确密码应用安全事件发生时的应急处理流程及其他管理措施；制定事件处置制度，当密码应用安全事件发生后及时向信息系统主管部门进行报告；制定上报制度，当密码应用安全事件处置完成，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

4安全目标及设计原则

4.1安全目标

按照《密码应用基本要求》中第二级密码应用基本要求，综合考虑本系统物理和环境、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，设计合规、正确、有效的密码应用方案，为后续密码保障体系建设、密码应用安全性评估奠定坚实基础，降低或消除应用系统中存在的安全风险，提升应用系统的安全防护水平，实现使用密码技术对本项目进行保护的目的。

4.2设计原则与依据

4.2.1信息系统密码应用方案设计原则：

1、自主可控、安全合规

健全安全管理制度，强化数据安全管理，落实主体责任，加强综合防范，积极运用自主可控、信创的密码技术产品，确保各系统运行和数据信息安全。

2、总体性原则

通过从整体层面，对本系统的密码应用开展顶层设计，明确密码应用需求和预期目标，并与各系统网络安全保护等级相结合，通过系统的设计形成涵盖技术、管理、实施保障的整体方案，为在各系统中落实密码应用相关要求奠定基础。

3、完备性原则

围绕本系统实际业务应用与安全保护等级，站在整体角度，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，设计各系统密码改造方案。

4、经济性原则

结合本系统规模，在合理、够用的前提下，满足 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》的密码应用改造方案，确保各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。

4.2.2设计依据

密码应用方案设计参考以下法律、法规及规范性文件：

- 1、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》；
- 2、《信息系统密码应用高风险判定指引》；
- 3、《商用密码应用安全性评估量化评估规则》；
- 4、《商用密码应用安全性评估 FAQ》；
- 5、《SM4 分组密码算法》（GM/T 0002-2014）
- 6、《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）
- 7、《SM3 密码杂凑算法》（GM/T 0004-2012）
- 8、《SM2 密码算法使用规范》（GM/T 0009-2012）
- 9、《数字证书认证系统密码协议规范》（GM/T 0014-2023）
- 10、《基于 SM2 密码算法的数字证书格式规范》（GM/T 0015-2023）
- 11、《智能密码钥匙应用接口规范》 GM/T 0016-2023
- 12、《密码设备应用接口规范》（GM/T 0018-2023）
- 13、《通用密码服务接口规范》（GM/T 0019-2023）
- 14、《IPSec VPN 网关产品规范》（GM/T 0023-2023）
- 15、《SSL VPN 技术规范》（GM/T 0024-2023）
- 16、《SSL VPN 网关产品规范》（GM/T 0025-2023）
- 17、《安全认证网关产品规范》（GM/T 0026-2023）
- 18、《智能密码钥匙技术规范》（GM/T 0027-2014）
- 19、《密码模块安全技术要求》（GM/T 0028-2024）
- 20、《签名验签服务器技术规范》（GM/T 0029-2014）
- 21、《服务器密码机技术规范》 GM/T 0030-2014
- 22、《时间戳接口规范》（GM/T 0033-2023）

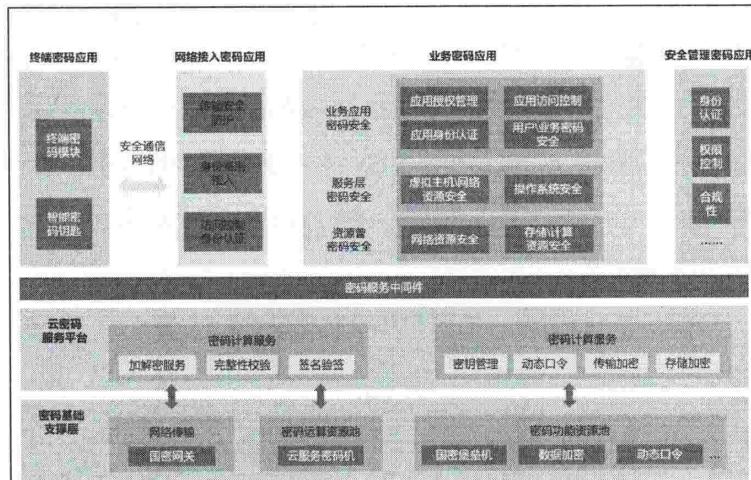
- 23、《采用非接触卡的门禁系统密码应用技术指南》（GM/T 0036-2014）
- 24、《证书认证密钥管理系统检测规范》（GM/T 0038-2014）
- 25、《电子文件密码应用指南》（GM/T 0071-2019）
- 26、《云服务器密码机技术规范》（GM/T 0104-2021）。

5密码应用设计

5.1 密码应用技术框架

通过采用符合密码相关国家标准和行业标准要求的密码产品，为系统提供身份认证服务、数据加解密服务、签名验签服务、电子签名服务等，保障系统用户身份的真实性、数据的机密性、数据的完整性。

根据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021），



结合系统的实际情况，系统的密码应用技术框架图如下图所示：

图 5-1 密码应用技术框架图

基于密码技术的统一服务体系架构，遵循国家相关管理要求，采用硬件专用设备加虚拟化、物理主机进行融合的模式，实现了密码运算资源的应用，使之在符合密钥使用管理要求的同时实现统一密码服务体系架构。通过应用和密码计算服务分离、密码计算和密钥管理分离的设计，应用可在密码支撑层获得安全的密码服务。

密码体系架构：从架构上，密码体系由密码基础支撑层、云密码服务平台、应用层三部分组成，可以为应用系统提供数据加解密、签名验签、时间戳验证、传输加密等安全服务。

密码基础支撑层：由专用物理设备和云服务密码机、国密网关、国密堡垒机等组成。

密码服务层：以已有密码产品为主，为应用系统国密改造提供标准化服务能力，包括加解密服务、完整性校验、签名验签、密钥管理、传输存储加密等。

密码应用层：系统调用下层的接口层实现安全功能应用。

5.2 计算平台密码应用方案

5.2.1 物理和环境安全

物理和环境安全是信息系统安全的基础层面。如果信息系统的物理和环境安全得不到保障，则设备、数据、应用等都将直接暴露在威胁之下，信息系统的安全就无从谈起。利用密码技术确保信息系统的物理和环境安全，可以有效阻断外界对信息系统各类重要场所、监控设备的直接入侵，并确保监控记录信息不被恶意篡改。对于物理和环境安全性的要求主要有两方面：一是对于物理和环境的访问控制，即未授权人员无法访问重要场所、重要设备和监控设备；二是对各类物理和环境的监控信息的完整性保护，包括人员进入记录、监控记录等，实现事前威慑、事中监控、事后追责。

物理和环境安全要求对照表：

表 5-1 物理和环境安全要求对照表

指标要求		一级	二级	三级	四级
物理和环境安全	身份鉴别*	可	宜	宜	应
	电子门禁记录数据存储完整性	可	可	宜	应
	视频记录数据存储完整性	--	--	宜	应
	密码服务	应	应	应	应
	密码产品	--	一级及以上	二级及以上	三级及以上

机房部署符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》的电子门禁系统，通过国密 CPU 卡和国密门禁读卡器，采用基于 SM4 国密算法的对称加解密技术，实现用户身份鉴别，同时采用基于 SM3 的 HMAC 或 SM2 技术，实现对电子门禁进出记录数据的完整性保护。

5.2.2 网络和通信安全

网络和通信安全要求对照表：

表 5-2 网络和通信安全要求对照表

指标要求		一级	二级	三级	四级
网络和通信安全	身份鉴别*	可	宜	应	应
	通信数据完整性	可	可	宜	应
	通信过程中重要数据的机密性*	可	宜	应	应

指标要求	一级	二级	三级	四级
网络边界访问控制信息的完整性	可	可	宜	应
安全接入认证	--	--	可	宜
密码服务	应	应	应	应
密码产品	--	一级及以上	二级及以上	三级及以上

1、互联网移动端与边境英烈云祭扫小程序之间的业务通道：通过云平台部署符合 GM/T 0025-2023《SSL VPN 网关产品规范》、GM/T 0028-2024《密码模块安全要求》的 SSL VPN 安全认证网关进行流量代理，采用基于 RSA（2048）算法的密码技术对通信实体进行身份鉴别，采用基于 AES_GCM 算法的密码技术保证通信数据的机密性，采用基于 AES_GCM 算法的密码技术保证通信数据的完整性，合规的 SSL VPN 安全认证网关内部可保证网络边界访问控制信息的完整性，SSL 证书由国家密码管理局许可的电子政务电子认证服务机构颁发。

2、互联网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：通信信道采用双协议兼容方式，即 TLS（非高风险）与 TLCP 双协议兼容方式；通过云平台部署符合 GM/T 0025-2023《SSL VPN 网关产品规范》的 SSL VPN 安全认证网关设备，采用基于 RSA（2048）算法或 SM2 算法的密码技术对通信实体进行身份鉴别，采用基于 AES_GCM 算法或 SM4 算法的密码技术保证通信数据的机密性，采用基于 AES_GCM 算法或 HMAC-SM3 算法的密码技术保证通信数据的完整性，数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发，合规的 SSL VPN 安全认证网关内部可保证网络边界访问控制信息的完整性。

3、政务外网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：通信信道采用双协议兼容方式，即 TLS（非高风险）与 TLCP 双协议兼容方式；通过云平台部署符合 GM/T 0025-2023《SSL VPN 网关产品规范》的 SSL VPN 安全认证网关设备，采用 RSA（2048）算法或 SM2WithSM3 算法的密码技术对通信实体进行身份鉴别，采用基于 AES_GCM 算法或 SM4 算法的密码技术保证通信数据的机密性，采用基于 AES_GCM 算法或 HMAC-SM3 技术的密码技术保证通信数据的完整性，数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发，合规的 SSL VPN 安全认证网关内部可保证网络边界访问控制

信息的完整性。

4、互联网 VPN 客户端与综合安全网关的通信信道：运维人员通过互联网使用 VPN 访问堡垒机进行运维管理，通过部署符合 GM/T 0025-2023《SSL VPN 网关产品规范》的综合安全网关，采用基于 SM2 算法对运维访问实体进行身份鉴别，采用基于 SM4 算法保证通信数据的机密性，采用基于 HMAC-SM3 算法保证通信数据的完整性，合规的 SSL VPN 安全认证网关可保证 VPN 边界访问控制信息的完整性，数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发。

网络和通信安全层面使用的密码算法、密码技术、密钥管理由符合国家相关标准和行业标准的安全认证网关、综合认证网关等密码产品实现。

5.2.3 设备和计算安全

设备和计算安全要求对照表：

表 5-3 设备和计算安全要求对照表

指标要求		一级	二级	三级	四级
设备和 计算安 全	身份鉴别	可	宜	应	应
	远程管理通道安全	--	--	应	应
	系统资源访问控制信息完整性	可	可	宜	应
	重要信息资源安全标记完整性	--	--	宜	应
	日志记录完整性	可	可	宜	应
	重要可执行程序完整性、重要可执行程序来源真实性	--	--	宜	应
	密码服务	应	应	应	应
	密码产品	--	一级及以上	二级及以上	三级及以上

1、身份鉴别

由于服务器等设备的身份鉴别改造难度大、成本高、周期长，暂不考虑对其进行国密改造，服务器等设备仍采用用户名+静态口令的方式进行身份鉴别。

当用户在互联网使用 VPN 进行运维时，使用智能密码钥匙基于 SM2 算法的数字签名机制进行综合安全网关实现身份鉴别，搭建 TLCP 国密通道后再通过用户名+静态口令的方式登录堡垒机，登录堡垒机后对服务器、数据库等进行统一运维管理，可降低服务器、数据库身份鉴别的安全风险，智能密码钥匙中用户数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发。

2、系统资源访问控制信息完整性

由于服务器等设备本身的限制，要在服务器等设备上应用国密算法，改造难度大、成本高、周期长，故暂不考虑采用密码技术保证服务器等设备系统资源访问控制信息的完整性，对于合规的密码产品，其本身可保证系统资源访问控制信息的完整性。

3、日志记录完整性

由于服务器等设备本身的限制，要在服务器等设备上应用国密算法，改造难度大、成本高、周期长，故暂不考虑采用密码技术保证服务器等设备日志记录的完整性，对于合规的密码产品，其本身可保证日志记录的完整性。

设备和计算安全层面所使用的密码算法、密码技术、密码服务、密钥管理由符合 GM/T 0030《服务器密码机技术规范》、GM/T 0027《智能密码钥匙技术规范》、GM/T 0028《密码模块安全技术要求》的智能密码钥匙、服务器密码机实现。

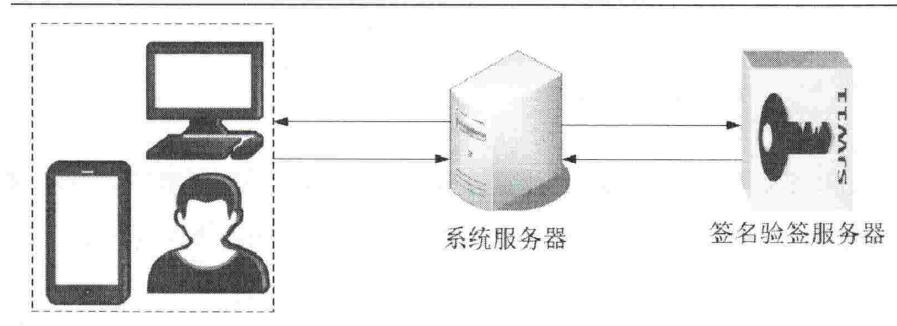
5.3 密码支撑平台方案

目前业务应用系统设计所采用的密码产品均具有商用密码产品认证证书且密码模块为安全二级及以上，所采用的密码产品及遵循的标准如下表：

序号	密码产品名称	产品标准	支持的密码算法	密码功能	部署方式
1	智能密码钥匙	GM/T 0027《智能密码钥匙技术规范》 GM/T 0028《密码模块安全技术要求》	SM2/SM3/SM4	实体鉴别	统一部署
2	SSL VPN 安全认证网关	GM/T 0025《SSL VPN网关产品规范》 GM/T 0028《密码模块安全技术要求》	SM2/SM3/SM4	实体鉴别、签名验签、加密解密	统一部署
3	云服务器 密码机	GM/T 0030《服务器密码机技术规范》 GM/T 0028《密码模块安全技术要求》	SM2/SM3/SM4	签名验签、加密解密	统一部署
4	签名验签 服务器	GM/T 0029《签名验签服务器技术规范》 GM/T 0028《密码模块安全技术要求》	SM2/SM3/SM4	签名验签、加密解密	统一部署
5	身份认证 网关	GM/T 0026《安全认证网关产品规范》 GM/T 0028《密码模	SM2/SM3/SM4	实体鉴别、签名验签、加密解密	统一部署

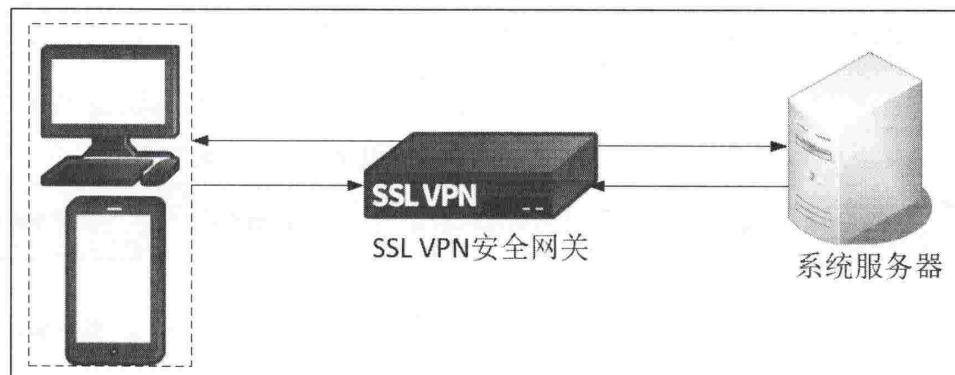
		块安全技术要求》		
--	--	----------	--	--

5.3.1身份鉴别服务



业务应用系统采用智能密码钥匙+数字证书进行身份鉴别，调用签名验签服务器进行签名验证，保证用户身份的真实性。

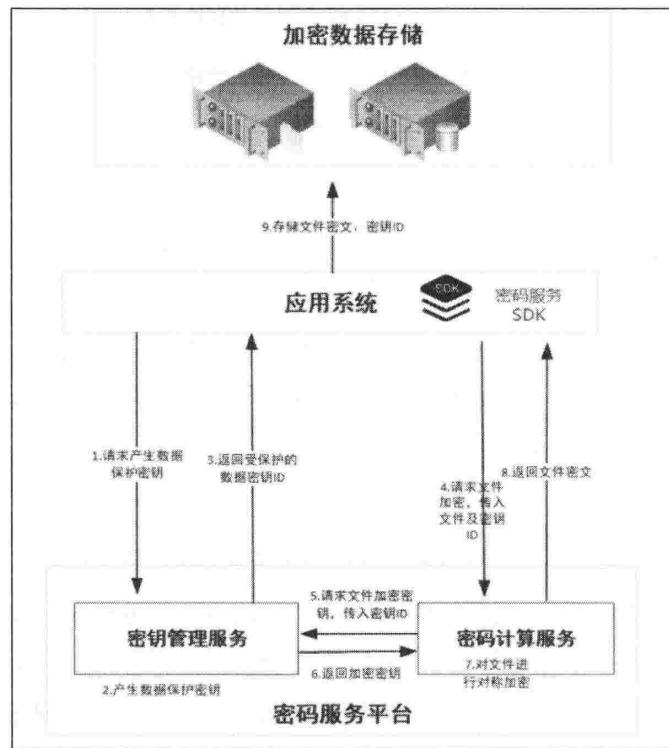
5.3.2数据传输机密性和传输完整性保护服务



SSL VPN安全网关将业务应用系统的通信协议代理成TLCP协议，保证业务应用系统数据的传输机密性和传输完整性。

5.3.3数据存储机密性和存储完整性保护服务

系统的重要数据包括平台鉴别信息、访问控制信息、日志数据、业务数据、个人敏感信息等数据，均需要做存储完整性保护。



应用系统调用密码服务平台接口，由平台中的密码运算服务模块对重要数据进行SM4加密运算、HMAC-SM3摘要运算处理后，存储到系统后台数据库指定加密位置，实现对重要数据的存储机密性和完整性保护。

5.4 业务应用的密码应用方案

应用和数据安全要求对照表：

表 5-4 应用和数据安全要求对照表

指标要求		一级	二级	三级	四级
应用 和数 据安 全	身份鉴别*	可	宜	应	应
	访问控制信息完整性	可	可	宜	应
	重要信息资源安全标记完整性	--	--	宜	应
	重要数据传输机密性*	可	宜	应	应
	重要数据存储机密性*	可	宜	应	应
	重要数据传输完整性	可	宜	宜	应
	重要数据存储完整性*	可	宜	宜	应
	不可否认性*	--	--	宜	应
	密码服务	应	应	应	应
	密码产品	--	一级及以上	二级及以上	三级及以上

1、身份鉴别

应用系统普通用户和移动端普通用户由于用户量大、范围广、改造难度大、

成本高、周期长，经研讨后，应用系统普通用户和移动端普通用户采用用户名+静态口令+短信验证码的方式进行身份鉴别，并且严格控制普通用户和移动端普通用户的操作权限，仅授予用户角色当前拥有的最小权限，及建立完善的审计记录功能，对用户重要操作行为进行审计记录，并定期审查日记操作记录，从而在一定程度上降低普通用户和移动端普通用户身份鉴别的安全风险。

系统管理员用户采用智能密码钥匙+数字证书的方式进行身份鉴别，采用基于SM3WithSM2算法的数字签名机制实现管理员用户身份鉴别，服务端调用身份认证网关或签名验签服务器进行签名验证，其中数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发。

当管理员用户登录系统时，在验证 PIN 码和智能密码钥匙绑定的帐号后，由系统服务端向身份认证网关发送生成随机数的请求，身份认证网关或签名验签服务器生成随机数并返回随机数给系统服务端后，由系统服务端将随机数发送至系统前端，在系统前端调用智能密码钥匙中的用户私钥进行签名并将签名值、公钥、随机数等签名数据发送至系统服务端，再由系统服务端调用身份认证网关或签名验签服务器的接口对签名值、公钥、随机数进行验签，验证用户数字证书的有效性和签名数据的正确性，验证完毕后将验签结果响应返回给系统服务端，从而完成登录认证闭环，实现登录用户的身份认证。

2、访问控制信息完整性

应用系统用户的权限由管理员进行分配，在对用户进行权限分配或修改时系统服务端调用信创云平台已部署符合密码相关国家标准、行业标准要求的云服务器密码机或签名验签服务器提供的“签名接口”，使用基于SM3WithSM2数字签名算法的密码技术对访问控制信息进行签名，云服务器密码机或签名验签服务器对其进行签名后将响应报文返回给系统服务端，系统服务端从返回的报文得到的签名值存储到数据库中。在系统用户登录环节或查看访问控制信息环节，系统调用云服务器密码机或签名验签服务器提供的“验签接口”，使用公钥对访问控制信息数据、存储在数据库中的签名值进行进行验签，如果验签通过，说明访问控制信息未被篡改；如果验签未通过，说明当前访问控制信息已经被篡改，并系统在前端弹框提示数据已经被篡改。

3、重要数据传输机密性

重要数据明文传输，依托“网络和通信安全”层面建立的 SSL 通道实现重要数据在传输过程中的机密性保护。

4、重要数据存储机密性

通过符合 GM/T 0030-2014《服务器密码机技术规范》标准的服务器密码机等密码产品，采用 SM4 算法 CBC 模式保证重要数据在存储过程中的机密性。

5、重要数据传输完整性

重要数据明文传输，在传输过程中的完整性依托“网络和通信安全”层面建立的 SSL 通道实现通信数据的完整性保护。

6、重要数据存储完整性

本系统中的重要数据需要存储完整性保护，存储机密性保护包括数据录入/修改、数据校验两部分。

重要数据在录入或修改时，系统服务端调用信创云平台已部署符合密码相关国家标准、行业标准要求的云服务器密码机或签名验签服务器提供的“签名接口”，使用基于 SM3withSM2 算法的数字签名技术对重要数据进行签名或使用 HMAC-SM3 生成 HMAC 值，云服务器密码机或签名验签服务器对其进行签名后将响应报文返回给系统服务端，系统服务端从返回的报文得到的签名值存储到数据库中。当系统用户在前端查看或校验重要数据时，系统调用云服务器密码机或签名验签服务器提供的“验签接口”，使用公钥对重要数据的原文数据、存储在数据库中的签名值进行验签，如果验签通过，说明重要数据未被篡改；如果验签未通过，说明当前重要数据已经被篡改，并系统在前端弹框提示数据已经被篡改。

5.5 密钥管理安全

本系统使用的数字证书均由国家密码管理局许可的电子政务电子认证服务机构颁发，系统所使用的密钥均保存在合规的密码产品中，系统涉及的密钥包括服务器密码机对称密钥、签名验签服务器签名密钥对、智能密码钥匙签名密钥对、SSL VPN 签名密钥对。

本系统采用符合密码相关国家标准和行业标准要求的智能密码钥匙、签名验签服务器、服务器密码机等商用密码产品，根据这些商用密码产品提供的安全策略，制定密钥管理方案，并严格遵照该方案进行使用和实施。

表 5-5 业务应用系统非对称密钥全生命周期管理

密钥名称	生成	存储	分发	更新	使用	备份和恢复	归档	销毁	撤销
智能密码钥匙签名私钥	在智能密码钥匙内部生成	在智能密码钥匙内部存储	不涉及	通过智能密码钥匙进行更新	在智能密码钥匙内部使用	不涉及	不涉及	在智能密码钥匙内部销毁	不涉及
智能密码钥匙签名公钥	在智能密码钥匙内部生成	在智能密码钥匙内部以证书的形式存储	通过CA机构以证书的形式分发	通过CA机构以证书的形式进行更新	以证书的形式使用	不涉及	不涉及	在智能密码钥匙内部销毁	不涉及
签名验签服务器签名密钥对	在签名验签服务器内部生成	在签名验签服务器内部存储	不涉及	通过签名验签服务器进行更新	在签名验签服务器内部使用	不涉及	不涉及	在签名验签服务器内部销毁	不涉及
SSL VPN签名私钥	在SSL VPN内部生成	在SSL VPN内部存储	不涉及	通过SSL VPN进行更新	在SSL VPN内部使用	不涉及	不涉及	在SSL VPN内部销毁	不涉及
SSL VPN签名公钥	在SSL VPN内部生成	在SSL VPN内部以证书的形式存储	通过CA机构以证书的形式分发	通过SSL VPN进行更新	以证书的形式使用	不涉及	不涉及	在SSL VPN内部销毁	不涉及

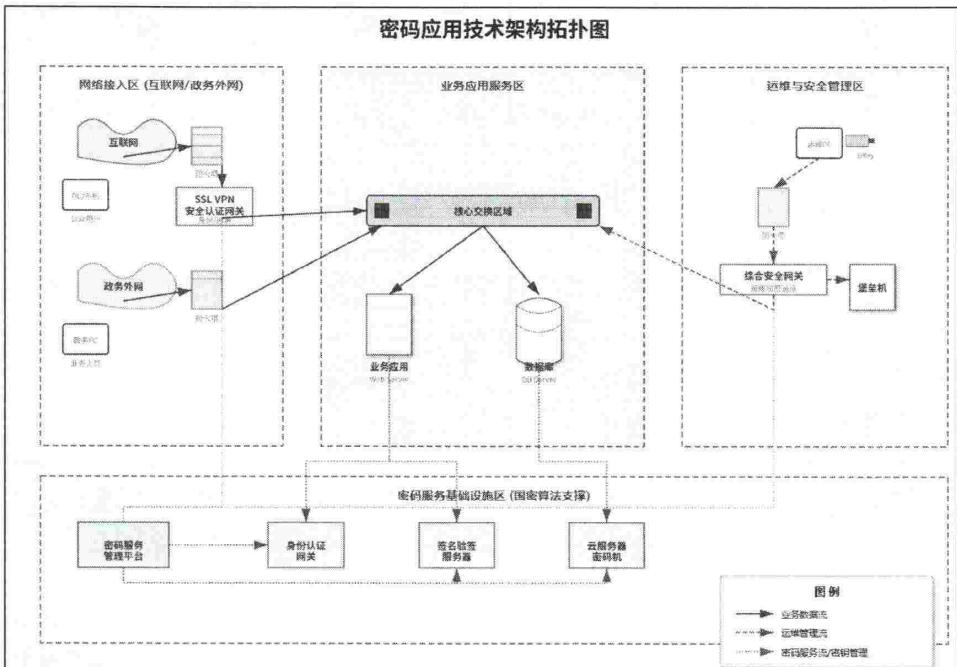
表 5-6 业务应用系统对称密钥全生命周期管理

密钥名称	生成	存储	分发	更新	使用	备份和恢复	归档	销毁	撤销
服务器密码机对称密钥	在服务器密码机内部生成	在服务器密码机内部存储	不涉及	通过服务器密码机进行更新	在服务器密码机内部使用	不涉及	不涉及	在服务器密码机内部销毁	不涉及

5.6 密码应用部署

本系统使用的智能密码钥匙、签名验签服务器、服务器密码机、SSL VPN、等密码产品均具有商用密码产品认证证书。密码应用部署图如下图 5-2 所示：

图 5-2 密码应用部署图



业务流：系统用户登录系统并执行业务操作的过程及相关数据流转；

运维流：系统运维人员对系统中的相关设备进行运维管理操作的过程及相关数据流转；

密码应用流：系统中的应用和设备调用密码保障系统实现数据安全传输、存储、身份鉴别等过程及相关数据流转。

5.7 密码产品清单

5.7.1 已有密码产品清单

云平台支持的密码产品清单：

表 5-7 云平台可提供密码产品清单

序号	产品名称	部署位置	使用的密码算法	数量	用途
1	SSL VPN 安全认证网关	/	SM2/SM3/SM4	/	建立用户访问业务应用系统的安全数据传输通道。
2	综合安全网关	/	SM2/SM3/SM4	/	建立运维用户远程运维的安全数据传输通道
3	云服务器密码机	/	SM2/SM3/SM4	/	提供数据加解密服务、数据完整性保护服务。

序号	产品名称	部署位置	使用的密码算法	数量	用途
4	签名验签服务器	/	SM2/SM3/SM4	/	提供数字签名服务。
5	身份认证网关	/	SM2/SM3/SM4	/	提供应用系统身份鉴别验签服务。
6	密码服务管理平台	/	SM2/SM3/SM4	/	提供密钥管理服务。

5.7.2 需新增密码产品清单

序号	产品名称	部署位置	使用的密码算法	数量	用途
1	国密 SSL 证书	SSL VPN 安全认证网关 / 综合安全网关	SM2/SM3	/	部署于网关设备上，用于标识服务端身份，并建立基于国密算法的加密传输通道。
2	非国密 SSL 证书	SSL VPN 安全认证网关 / 综合安全网关	RSA-2048/AES/SHA-256	/	部署于网关设备上，用于标识服务端身份，并建立基于国密算法的加密传输通道。
2	智能密码钥匙	运维终端 / 管理员电脑	SM2/SM3/SM4	/	硬件密码模块（UKey），用于安全存储用户数字证书及私钥，提供边境英烈云祭扫小程序的密码运算环境。
3	国密浏览器	运维终端 / 管理员电脑	SM2/SM3/SM4	/	支持国密 SSL 协议及国密算法的浏览器，用于与 SSL VPN 网关建立合规的国密通信信道。
4	用户证书	智能密码钥匙 内部	SM2	/	存储在智能密码钥匙中，用于标识运维/管理人员的身份，实现强身份鉴别和数字签名。

6 安全管理方案

6.1管理制度

在管理制度方面，本单位将按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的相关要求，制定符合本单位实际情况的相关密码应用安全管理制度，制度包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度管理内容，并在单位内部进行正式发布；建立相应的密钥管理规则并对密钥的全生存周期进行管理；对密码相关管理人员或操作人员的日常管理操作建立操作规程；定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和评审审定，并留存相关修订记录以及评审记录；明确密码应用安全管理制度的发布流程和版本控制，并留存相关发布流程文件或记录；密码操作人员在密码应用操作规程执行过程中要填写的相关执行记录文件并留存记录文件。

6.2人员管理

根据《基本要求》中安全管理人员方面的要求，对本系统现有的人员管理制度进行补充和完善。

在人员管理方面，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中实施管理要求，本单位将对系统相关人员进行密码相关法律法规和密码应用安全管理制度培训，通过培训确保系统相关人员知悉和掌握密码应用安全管理制度、法律法规内容，并能遵照执行，单位内部留存相关培训记录文件；结合本单位的实际状况，制定严格且有效的密码应用岗位责任制度，并根据密码应用的实际情况设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位，对密钥管理员、密码安全审计员、密码操作员等关键安全岗位建立多人共管机制，并为人员开通对应的管理帐户，使得密钥管理员、密码安全审计员、密码操作员职责之间相互制约相互监督，并且在密码应用岗位责任制度中明确密码安全审计员岗位不与密钥管理员、密码操作员兼任，明确相关设备与系统的管理和使用账号不得多人共用；制定上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能，制定涉及密码的操作和管理的人员的培训计划，培训后形成相应的培训记录文件并留存，培训记录包括密码培训人员、密码培训内容、密码培训结果等描述；建立关键岗位人员的保密制度和调离制度，关键岗位人员在上岗前要签署保密协议，保密协议的内容包括保密范围、

保密责任、违约责任、协议的有效期限和责任人的签字等内容，当关键岗位人员离岗前要办理离岗手续，收回其所有权限，进行离岗安全审查，在审查合格后，方可调离。

6.3建设运行

在建设运行方面，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中实施管理要求，做好密码应用方案设计与评审、密码保障系统建设与商用密码应用安全性评估、以及相关闭环管理工作，保证密码应用方案的有效落地，设置合理的实施运行保障方案，包括以下内容：

根据系统实际情况制定相应密码应用方案。应用规划阶段，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》及 GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》等标准的相关要求制定密码应用方案，委托密评机构对密码应用方案进行评估，确保其评估结论为通过。

制定密钥安全管理策略。根据已通过评审的密码应用方案，确定涉及的密钥种类、体系及其生存周期环节，制定对应的密钥安全管理策略，留存相应的密钥管理过程记录。

制定实施方案。根据密码应用方案制定密码实施方案，并依据密码应用方案合规、正确、有效进行实施建设，选用通过检测认证合格的商用密码产品实现系统密码保障。

投入运行前进行密码应用安全性评估。密码应用建设完成后，委托密评机构对系统开展商用密码应用安全性评估，评估通过后则系统正式上线运行。

6.4应急处置

在应急处置方面，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中应急管理要求，制定本单位情况的密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时进行处置，根据密码应用安全事件等级制定相应的密码应用应急策略并对应急策略进行评审，应急策略中明确密码应用安全事件发生时的应急处理流程及其他管理措施，并遵照执行，若发生密码应用安全事件，立即启动应急处置措施并形成相应的处置记录并留存；当密码应用安全事件发生后，及时向信息系统主管部门进行报告并留存相应密码应用安全事件报告；当密码应用安全事件处置完成

后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况并留存相应处置情况报告。

7安全与合规性分析

表 7-1 密码应用合规性表（二级）

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/不通过）
物理和环境安全	身份鉴别	宜	适用	机房部署符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》的电子门禁系统，通过国密 CPU 卡和国密门禁读卡器，采用基于 SM4 国密算法的对称加解密技术，实现用户身份鉴别，同时采用基于 SM3 的 HMAC 或 SM2 技术，实现对电子门禁进出记录数据的完整性保护。	/	通过
	电子门禁记录数据完整性	可	适用			通过
网络和通信安全	身份鉴别	宜	适用	1、互联网移动端与边境英烈云祭扫小程序之间的业务通道：通过云平台部署符合 GM/T 0025-2023《SSL VPN 网关产品规范》、GM/T 0028-2024《密码模块安全要求》的 SSL VPN 安全认证网关进行流量代理，采用基于 RSA (2048) 算法的密码技术对通信实体进行身份鉴别，采用基于 AES_GCM 算法的密码技术保证通信数据的机密性，采用基于 AES_GCM 算法的密码技术保证通信数据的完整性，合规的 SSL VPN 安全认证网关内部可保证网络边界访问控制信息的完整性，SSL 证书由国家密码管理局许可的电子政务电子认证服务机构颁发。	/	通过
	通信数据完整性	可	适用	2、互联网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：通信信道采用双协议兼容方式，即 TLS (非高风险) 与 TLCP 双协议兼容方式；通过云平台部署符合 GM/T 0025-2023《SSL VPN 网关产品规范》的 SSL VPN 安全认证网关设备，采用基于 RSA (2048) 算法或 SM2 算法的密码技术对通信实体进行身份鉴别，采用基于 AES_GCM 算法或 SM4 算法的密码技术保证通信数据的机密性，采用基于 AES_GCM 算法或 HMAC-SM3 算法的密码技术保证通信数据的完整性，数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发，合规的 SSL VPN 安全认证网关内部可保证网络边界访问控制信	/	通过
	通信过程中重要数据的机密性	宜	适用	/	/	通过
	网络边界访问控制信息的完整性	可	适用			通过

				<p>息的完整性。</p> <p>3、政务外网浏览器与边境英烈云祭扫小程序管理平台之间的业务通道：通信信道采用双协议兼容方式，即 TLS（非高风险）与 TLCP 双协议兼容方式；通过云平台部署符合 GM/T 0025-2023 《SSL VPN 网关产品规范》的 SSL VPN 安全认证网关设备，采用 AES_GCM 算法或 SM4 算法的密码技术对通信实体进行身份鉴别，采用基于 AES_GCM 算法或 HMAC-SM3 的密码技术保证通信数据的机密性，采用基于非国密（非高风险）算法或国密算法的密码技术保证通信数据的完整性，数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发，合规的 SSL VPN 安全认证网关内部可保证网络边界访问控制信息的完整性。</p> <p>4、互联网 VPN 客户端与综合安全网关的通信信道：运维人员通过互联网使用 VPN 访问堡垒机进行运维管理，通过部署符合 GM/T 0025-2023 《SSL VPN 网关产品规范》的综合安全网关，采用基于 SM2 算法对运维访问实体进行身份鉴别，采用基于 SM4 算法算法保证通信数据的机密性，采用基于 HMAC-SM3 算法保证通信数据的完整性，合规的 SSL VPN 安全认证网关可保证 VPN 边界访问控制信息的完整性，数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发。</p> <p>网络和通信安全层面使用的密码算法、密码技术、密钥管理由符合国家相关标准和行业标准的安全认证网关、综合认证网关等密码产品实现。</p>		
设备和计算安全	身份鉴别	宜	适用	<p>由于服务器等设备的身份鉴别改造难度大、成本高、周期长，暂不考虑对其进行国密改造，服务器等设备仍采用用户名+静态口令的方式进行身份鉴别。</p> <p>当用户在互联网使用 VPN 进行运维时，使用智能密码钥匙基于 SM2 算法的数字签名机制进行综合安全网关实现身份鉴别，搭建 TLCP 国密通道后再通过用户名+静态口令的方式登录堡垒机，登录堡垒机后对服务器、数据库等进行统一运营管理，可降低服务器、数据库身份鉴别的安全风险，智能密码钥匙中用户数字证书由国家密码管理局许可的电子政务电子认证服务</p>	/	通过

				机构颁发。		
系统资源访问控制信息完整性	可	适用		由于服务器等设备本身的限制，要在服务器等设备上应用国密算法，改造难度大、成本高、周期长，故暂不考虑采用密码技术保证服务器等设备系统资源访问控制信息的完整性，对于合规的密码产品，其本身可保证系统资源访问控制信息的完整性。	/	通过
日志记录完整性	可	适用		由于服务器等设备本身的限制，要在服务器等设备上应用国密算法，改造难度大、成本高、周期长，故暂不考虑采用密码技术保证服务器等设备日志记录的完整性，对于合规的密码产品，其本身可保证日志记录的完整性。	/	通过
应用和数据安全	身份鉴别	宜	适用	应用系统普通用户和移动端普通用户由于用户量大、范围广、改造难度大、成本高、周期长，经研讨后，应用系统普通用户和移动端普通用户采用用户名+静态口令+短信验证码的方式进行身份鉴别，并且严格控制普通用户和移动端普通用户的操作权限，仅授予用户角色当前拥有的最小权限，及建立完善的审计记录功能，对用户重要操作行为进行审计记录，并定期审查日记操作记录，从而在一定程度上降低普通用户和移动端普通用户身份鉴别的安全风险。 系统管理员用户采用智能密码钥匙+数字证书的方式进行身份鉴别，采用基于SM3WithSM2算法的数字签名机制实现管理员用户身份鉴别，服务端调用身份认证网关或签名验签服务器进行签名验证，其中数字证书由国家密码管理局许可的电子政务电子认证服务机构颁发。 当管理员用户登录系统时，在验证PIN码和智能密码钥匙绑定的帐号后，由系统服务端向身份认证网关发送生成随机数的请求，身份认证网关或签名验签服务器生成随机数并返回随机数给系统服务端后，由系统服务端将随机数发送至系统前端，在系统前端调用智能密码钥匙中的用户私钥进行签名并将签名值、公钥、随机数等签名数据发送至系统服务端，再由系统服务端调用身份认证网关或签名验签服务器的接口对签名值、公钥、随机数进行验签，验证用户数字证书的有效性和签名数据的正确性，验证完毕后将验签结果响应返回给系统服务端，从而完成登录认证闭环，实现登录用户的	/	通过

			身份认证。		
访问控制信息完整性	可	适用	应用系统用户的权限由管理员进行分配，在对用户进行权限分配或修改时系统服务端调用信创云平台已部署符合密码相关国家标准、行业标准要求的云服务器密码机或签名验签服务器提供的“签名接口”，使用基于SM3WithSM2数字签名算法的密码技术对访问控制信息进行签名，云服务器密码机或签名验签服务器对其进行签名后将响应报文返回给系统服务端，系统服务端从返回的报文得到的签名值存储到数据库中。在系统用户登录环节或查看访问控制信息环节，系统调用云服务器密码机或签名验签服务器提供的“验签接口”，使用公钥对访问控制信息数据、存储在数据库中的签名值进行验签，如果验签通过，说明访问控制信息未被篡改；如果验签未通过，说明当前访问控制信息已经被篡改，并系统在前端弹框提示数据已经被篡改。	/	通过
重要数据传输机密性	宜	适用	/	重要数据明文传输，依托“网络和通信安全”层面建立的SSL通道实现重要数据在传输过程中的机密性保护。	通过
重要数据存储机密性	宜	适用	通过符合GM/T 0030-2014《服务器密码机技术规范》标准的服务器密码机等密码产品，采用SM4算法CBC模式保证重要数据在存储过程中的机密性。	/	通过
重要数据传输完整性	宜	适用	/	重要数据明文传输，在传输过程中的完整性依托“网络和通信安全”层面建立的SSL通道实现通信数据的完整性保	通过

					护。	
管理制度	重要数据存储完整性	宜	适用	<p>本系统中的重要数据需要存储完整性保护，存储机密性保护包括数据录入/修改、数据校验两部分。</p> <p>重要数据在录入或修改时，系统服务端调用信创云平台已部署符合密码相关国家标准、行业标准要求的云服务器密码机或签名验签服务器提供的“签名接口”，使用基于SM3withSM2算法的数字签名技术对重要数据进行签名或使用HMAC-SM3生成HMAC值，云服务器密码机或签名验签服务器对其进行签名后将响应报文返回给系统服务端，系统服务端从返回的报文得到的签名值存储到数据库中。当系统用户在前端查看或校验重要数据时，系统调用云服务器密码机或签名验签服务器提供的“验签接口”，使用公钥对重要数据的原文数据、存储在数据库中的签名值进行验签，如果验签通过，说明重要数据未被篡改；如果验签未通过，说明当前重要数据已经被篡改，并系统在前端弹框提示数据已经被篡改。</p>	/	通过
	具备密码应用安全管理制度	应	适用	<p>本单位将按照GB/T 39786-2021《信息技术 信息系统密码应用基本要求》的相关要求，制定符合本单位实际情况的相关密码应用安全管理制度，制度包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度管理内容，并在单位内部进行正式发布；定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和评审审定，并留存相关修订记录以及评审记录；明确密码应用安全管理制度的发布流程和版本控制，并留存相关发布流程文件或记录。</p>	/	通过
	密钥管理规则	应	适用	建立相应的密钥管理规则并对密钥的全生存周期进行管理。	/	通过
	建立操作规程	应	适用	对密码相关管理人员或操作人员的日常管理操作建立操作规程；密码操作人员在密码应用操作规程执行过程中要填写的相关执行记录文件并留存记录文件。	/	通过
人员管	了解并遵守密码相	应	适用	对系统相关人员进行密码相关法律法规和密码应用安全管理制度培训，确保系统相关人员已了解并遵守密码相关法律法规和密码应用安全	/	通过

理	关法律法 规和密 码管理 制度			管理制度。		
	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，并根据密码应用的实际情况设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位，对密钥管理员、密码安全审计员、密码操作员等关键安全岗位建立多人共管机制，密钥管理员、密码安全审计员、密码操作员职责互相制约互相监督，其中密码安全审计员岗位不与密钥管理员、密码操作员兼任，明确相关设备与系统的管理和使用账号不得多人共用。	/	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，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能，制定涉及密码的操作和管理的人员的培训计划，培训后形成相应的培训记录，培训记录包括密码培训人员、密码培训内容、密码培训结果等描述。	/	通过
	建立关键 岗位人员 保密制 度和调 离制 度	应	适用	建立关键岗位人员的保密制度和调离制度，关键岗位人员签署保密协议，保密协议的内容包括保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容，当关键岗位人员调离时办理调离手续，收回其所有权限，进行离岗安全审查，在审查合格后，方可调离。	/	通过
	制定密码 应用方案	应	适用	系统责任单位在信息系统规划阶段，依据密码相关标准和信息系统密码应用需求制定密码应用方案，并对方案进行评估并通过。	/	通过
建设运 行	制定密 钥安全 管理策 略	应	适用	根据密码应用方案的密钥管理制度确定系统涉及的密钥种类、体系及其生存周期环节，密钥管理制度根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的附录 B 进行制定。	/	通过
	制定实施	应	适用	根据密码应用方案制定密码实施方案。	/	通过

	方案					
	投入运行前进行密码应用安全性评估	宜	适用	在信息系统投入运行前组织进行密码应用安全性评估并通过评估。	/	通过
应急处置	应急策略	应	适用	依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中应急管理要求，制定情况的密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时进行处置，根据密码应用安全事件等级制定相应的密码应用应急策略并对应急策略进行评审，应急策略中明确密码应用安全事件发生时的应急处理流程及其他管理措施，并遵照执行，若发生密码应用安全事件，立即启动应急处置措施并形成相应的处置记录并留存；当密码应用安全事件发生后，及时向信息系统主管部门进行报告并留存相应密码应用安全事件报告；当密码应用安全事件处置完成后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况并留存相应处置情况报告。	/	通过

8实施保障方案

8.1实施内容

8.1.1实施目标

本项目严格按照《中华人民共和国密码法》及商用密码有关规范，以落实 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》第二级信息系统密码应用相关标准为原则，通过部署国产商用密码软硬件产品，提供身份真实性、数据机密性、数据完整性和抗抵赖性等安全服务，健全密码应用项目的网络安全保障体系。

8.1.2项目责任单位

崇左市退役军人事务局。

8.1.3项目实施地点

政务云平台机房

8.1.4实施原则

项目严格遵循国家主管部门制定的密码安全管理等技术标准与规范，保障能够有效地控制风险。方案中所采用的产品技术和部署方式必须具有足够的安全性，充分考虑可能的安全威胁和风险，并制定相应的对策。关键数据必须有可靠的备份与恢复措施。采用具有足够安全性的产品技术，以杜绝不单点故障。

8.1.5实施内容

本系统商用密码应用改造与实施内容具体如下：

- 1、调研应用现状，通过现状分析存在的商用密码应用问题或与《基本要求》不符的应用情况；
- 2、编写密码应用方案，依据调研应用现状情况以及《基本要求》第二级密码应用要求，编写密码应用方案；
- 3、密码应用方案评估，将编制完成的密码应用方案交由具备测评资质的商用密码应用测评机构进行评审（或组织专家评审），依据评审意见进行方案修改，直至拿到方案评审报告（或会议评审通过）；
- 4、密码应用设备采购，依据商用密码应用方案进行设备采购；
- 5、商用密码应用改造实施，依据密码应用方案中的具体细节实施，包括但不限于设备调试安装、应用系统密码应用改造、数据库存储测试等；
- 6、测评机构进行商用密码应用测评，由商用密码应用实施单位配合，由测评机构组织进行测评，测评后对不符合密码应用方案或者测评要求的内容进行整改；
- 7、出具测评报告，当测评无异议后，由测评机构出具测评报告。

8.1.6重要难点问题和风险控制

密码管理体系和运维体系的建立，密码管理和运维工作专业性比较强，需要保证制定完善的管理体系和运维管理体系，确保密码应用安全。

8.2实施计划

8.2.1实施路线

根据本项目的项目需求，编制《项目密码应用实施方案》，组织专家进行评审论证，并报领导小组备案，报请甲方用户批准；在《项目密码应用实施方案》被批准后，将严格按照实施方案、时间进度要求，组织工程建设，完成工程建设任务，组织工程验收，系统投入运行。

本项目具体实施包括以下几个步骤：

- 1、组建项目实施团队；
- 2、制定实施计划、编制《项目密码应用实施方案》；
- 3、项目实施，进行软硬件的安装与调试；
- 4、项目培训；
- 5、系统试运行与交付；
- 6、系统正式运行；
- 7、日常运维。

8.2.2实施进度计划

本项目实施计划如下：

序号	阶段	工作内容	所需时间	责任主体
1	现状调研	密码应用情况及应用现状调研。	5天	密码应用方案编写方，用户方参与
2	方案编制	密码应用方案编制。	3天	密码应用方案编写方
3	方案评审	对编写的密码应用方案进行评审及整改。	7天	密码应用方案编写方组织，测评机构参与
4	方案评审报告出具	出具密码应用方案评审报告。	7天	测评机构组织，密码应用方案编写方参与
5	实施采购	依据通过的方案采购所需设备。	14天	密码应用改造实施方
6	改造实施	依据通过的方案实施改造	35天	密码应用改造实施方组织，用户方、密码应用方案编写方参与

序号	阶段	工作内容	所需时间	责任主体
7	测评	对实施内容进行测评。	10 天	测评机构组织，用户方、密码应用改造实施方参与。
8	出具报告	出具测评报告。	5 天	测评机构

8.3保障措施

项目的组织和管理是保证一个项目实施成功的重要环节，本项目采用先进的管理手段、配置经验丰富的工程技术人员，从组织、实施以及技术服务等各方面入手进行管理，保证项目的质量，有序、按时、顺利地完成，并最终实现系统目标。

8.3.1组织保障

切实发挥好建设工作领导小组牵头协调作用，加强宏观指导，及时研究解决工作推进中的重大问题，推动工作高效开展。统筹规划、统一部署、协调推进，不断提高项目建设工作水平。各部门、项目组要高度重视，建立主要领导负责制，加强项目工作力量的协调，构建统一领导、上下衔接、统筹有力组织体系，充分落实项目建设工作，保障项目建设顺利推进。

8.3.2人员保障

营造良好的学习实践环境，加强项目人才队伍建设，积极培养既精通业务又能运用互联网技术和信息化手段开展工作的综合型人才。将项目建设列入各部门和项目组成员学习培训内容，建立普及性与针对性相结合的培训机制，提高建设意识和素质。强化互联网宣传，提升公众参与度，充分利用电视、广播、报刊、互联网等各类媒体，广泛宣传项目建设、服务新理念、新做法，加强对项目建设的舆论引导，积极协调高水平人才参与项目建设过程中。

8.3.3经费保障

项目组积极配合建设单位对各类资金进行统一管理，制定资金使用的相关规范、制度、流程，确保资金的合理使用。将项目预算纳入政府财政，规范化政务信息化服务项目经费预算编制和资金使用管理。

8.3.4技术保障

一是要确保商用密码应用运行所需的网络环境、网络资源等运行环境保障和技术支撑，满足应用需求；二是要打造系统化的商用密码安全体系，确保在建设中的技术优势。

8.3.5质量保障

1、进度管理

为了有效管理项目的进度，确保项目的进程。项目经理及有关工作人员需借助一些手段去了解工作的进展，及早察觉出现问题或脱期的环节。常用的手段包括：

- 每周项目进度报告；
- 项目任务制定表；
- 问题清单、尚待处理事项清单等。

2、质量控制

为了确保整个项目成功地实施，在整个项目周期内，项目经理所担当的角色相当重要。需要委派有多年成功项目管理经验的项目经理承担此项目，在客户全面积极配合下，确保人力、物力的定量投入。双方合作从以下几个方面保障项目的质量：

(1) 严格执行质量管理体系规范

- 质量控制管理体系规范的质量管理表格有：
- 日程表；
 - 人力资源分配表；
 - 各阶段的文档；
 - 各种表格式样。

(2) 保证人员的稳定

在项目实施过程中，人员的稳定和工作态度对项目的质量是非常重要的，为了保证系统的成功实施，需要做到以下几点：

- 派遣经验丰富的项目经理负责监督、统筹及协调各项开发事宜；
- 派遣经验丰富的实施人员完成项目实施工作；
- 提供足够的测试人员负责软件的综合测试及验收支持。

(3) 采用有效的质量监控手段

项目经理将通过定期质量管理会议，掌握项目的质量情况，及时发现并纠正质量上存在的问题，保证项目的质量。

明确工作目标；

明确每个成员的任务；

合理可行的项目时间表；

严谨的用户验收过程。

3、项目交付项

包括但不限于《系统用户手册》《技术白皮书》《接口说明》等文档。

8.3.6 监督检查

健全监督检查机制，建立涵盖整个项目过程、进度、质量的监督检查制度、规范等，保障项目顺利实施，达到预期成效。

附录 A 系统定级匹配证明

系统备案名称	边境英烈云祭扫小程序
系统备案时间	2025年12月10日

广西壮族自治区崇左市公安局

**关于对边境英烈云祭扫小程序网络安全等级
保护预定级审核意见的函**

崇左市退役军人事务局：

贵单位发来《关于审核边境英烈云祭扫小程序网络安全等级保护预定级的函》（崇退役军人函〔2025〕27号）收悉。经审核，贵单位拟建设的“边境英烈云祭扫小程序”的网络安全保护等级预定级为第二级，基本符合《信息安全等级保护管理办法》及《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）的规定，可以根据系统对应的网络安全等级实施项目安全建设。在项目建设完成后，请按规定及时办理正式的信息系统网络安全等级保护定级、备案和开展相关的安全等级测评工作。

崇左市公安局网络安全保卫支队
2025年12月10日

(公开前需经政府信息公开审查)