# 某部机关电子公文处理系统密码应用方案

## 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》的颁布实施，从法律层面为开展商用密码应用提供了根本遵循,《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。

我部为贯彻落实《密码法》关于信息系统密码应用的要求，结合《国家电子政务建设指导意见》，决定对已经建成的我部电子公文处理系统进行密码应用改造。

通过对我部电子公文处理系统的现状和密码应用需求进行分析，依据 GM/T 0054-2018《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、应用和数据安全等 4 个层面，以及密钥管理、安全管理等方面，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

本系统名称为某部电子公文处理系统，系统建设单位为某部机关，单位地址为 XXXXX，所属密码管理部门为某部办公厅，系统建设单位类型为部机关。

本系统部署在我部局域网，主要服务于我部机关工作人

员，为我部内部业务专网，未与其他系统互联。用户可通过部署在我部业务办公区的 PC 终端浏览器访问登录，也可在互联网通过移动智能终端访问登录。

本系统于 2017 年 5 月 31 日完成网络安全等级保护定级备案（测评机构：XXXXXX，备案编号：XXXXXX），定级等级为第 3 级（S3A3G3），于 2017 年 12 月 1 日上线运行。

## 2.2 系统网络拓扑

本系统采用传统 IT 系统架构，并提供移动智能终端设备在互联网接入所使用的移动互联网络技术，系统网络拓扑如下图 1 所示：

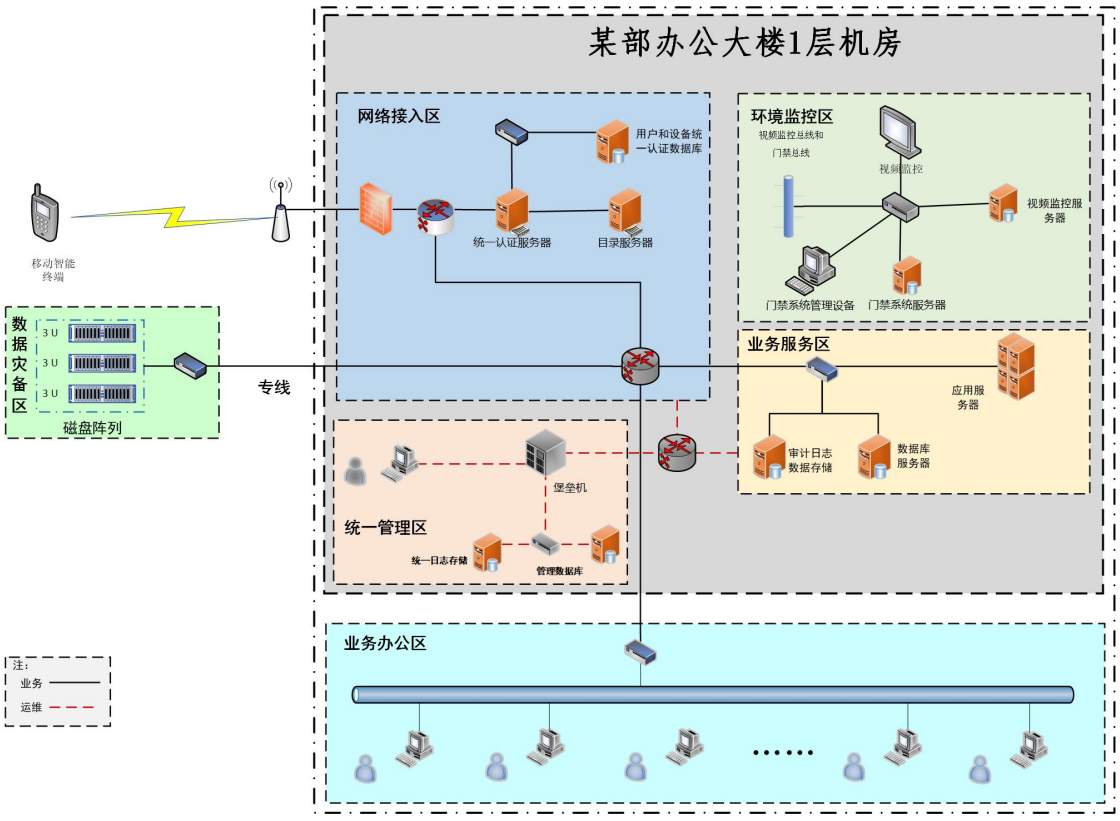


**图 1 某部机关电子公文处理系统网络拓扑图**

系统部署在我部办公大楼 1 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、业务办公区、数据灾备区等六个区。系统网络安全防护符合等保2.0相关要求。

**网络接入区**位于政务网络边界，部署了统一认证服务器、数据库、目录服务器、交换机等设备，实现对接入用户和设备统一认证。

**业务服务区**是电子公文处理系统的核心服务区域，主要部署了电子公文处理系统应用服务器、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。

**运维管理区**主要部署了远程运维管理终端、堡垒机、数据库等设备，实现对系统中的设备集中管理。

**环境监控区**主要部署了门禁系统和视频监控系统，实现对信息系统机房的物理安防管理。

**业务办公区**主要部署了办公终端、交换机等设备，实现我部办公人员通过我部政务办公网访问本系统。

**数据灾备区**主要部署了磁盘阵列等设备，实现重要业务数据的异地备份。

## 2.3 承载的业务情况

电子公文处理系统是我部日常办公的重要信息系统，为我部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。该系统由统一身份认证系统和电子公文处理系统两个应用组成，涉及的关键数据包括用户登录身份鉴别数据、电子公文数据等。

### 2.4 系统软硬件构成

本系统部署有计算机终端、服务器、磁盘阵列、堡垒机、防火墙等硬件设备，机房电子门禁系统通过 ID 卡对进出机房人员进行身份鉴别，使用视频监控系统对机房视频监控数据进行管理，计算机终端通过 IE11 浏览器访问登录电子公文处理系统。

### 2.5 管理制度

本单位根据等保 2.0 管理要求，制定了通用的《某部信息安全管理制度汇编》，该安全管理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 风险控制需求

根据 GM/T 0054-2018《信息系统密码应用基本要求》，从物理和环境安全、设备和计算安全、应用和数据安全、安全管理等层面，对本系统进行风险分析，得出本系统密码应用需求。

#### 3.1.1 物理和环境安全

**1)** 风险分析

（1）目前本系统所在机房使用 ID 卡对进入机房人员进行身份鉴别，未使用密码技术对进入机房人员进行身份鉴别，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。

（2）目前本系统所在机房人员进出记录明文存储在门禁管理系统数据库中，视频监控数据明文存储在磁盘阵列中，未使用密码技术进行存储完整性保护，存在物理进出记录和视频记录遭到非授权篡改，以掩盖非授权人员进出情况的风险。

**2)密码应用需求**

在本系统所在机房部署符合 GM/T 0036-2014 标准要求的电子门禁系统对进出机房人员进行身份鉴别。并在环境监控区部署符合密码相关国家、行业标准要求的服务器密码机，对门禁进出记录和视频监控数据进行完整性保护。

### 3.1.2 网络和通信安全

**1)风险分析**

（1）目前本系统业务服务区和数据灾备区之间使用专线进行灾备数据传输，通信前未使用密码技术对通信双方进行验证，未使用密码技术对灾备数据传输通道进行机密性和完整性保护，存在非法设备从外部接入内部网络，通信数据在信息系统外部被非授权截取、非授权篡改风险。

（2）目前本系统移动端 App 使用 HTTP 协议建立数据传

输通道，未使用密码技术建立安全的数据传输通道，实现数据传输通道机密性和完整性保护，存在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)目前本系统管理员用户在政府办公网通过 SSH 协议登录堡垒机对系统中的安全设备、安全组件进行集中管理，未使用合规的密码协议建立安全管理通道，存在搭建的集中管理通道被非授权使用，或传输的管理数据被非授权获取和非授权篡改风险。

**2)密码应用需求**

（1）在本系统网络接入区和数据灾备区分别部署符合密码相关国家、行业标准要求的 IPSec VPN，实现在通信前通信双方的身份鉴别，建立安全的灾备数据传输通道。

（2）在本系统移动端 App 中部署符合密码相关国家、行业标准要求的移动端密码模块（二级）、在网络接入区边界部署符合密码相关国家、行业标准要求的 SSL VPN 安全网关，建立安全的移动端 App 数据传输通道。

（3）在本系统统一管理区部署符合密码相关国家、行业标准要求的 SSL VPN 安全网关，建立安全的集中管理通道。

### 3.1.3 设备和计算安全

**1)风险分析**

（1）目前本系统管理员用户在政府办公网通过 IE11 浏览器，使用用户名口令登录堡垒机，使用 SSH 协议与堡垒机

之间建立安全连接，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对管理员登录身份鉴别信息进行传输机密性保护，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）目前本系统应用服务器中所有重要程序或文件在生成时未使用密码技术进行完整性保护，使用或读取这些程序和文件时，未对其进行完整性校验，存在重要程序或文件被非授权篡改、来源不可信风险。

（3）目前本系统应用服务器、数据库服务器等设备日志均明文存储，未使用密码技术进行完整性保护，存在设备日志记录被非授权篡改风险。

**2)密码应用需求**

（1）分别在本系统业务办公区 PC 端部署具有密码模块的浏览器（以下简称“安全浏览器”），在服务端部署 SSL VPN 安全网关，并向系统管理员配发 USB 接口的智能密码钥匙（以下简称“USBKey”），对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护，防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。

（2）在本系统应用服务区部署符合密码相关国家、行业标准要求的服务器密码机，并在应用服务器外挂 USBKey，应用服务器中所有重要程序或文件在生成时通过调用服务器密码机进行完整性保护，使用或读取这些程序和文件时，通

过 USBKey 进行验签以确认其完整性；公钥存放在 USBKey 中。

（3）在本系统应用服务区部署符合密码相关国家、行业标准要求的服务器密码机，对应用服务器、数据库服务器等设备日志进行完整性保护。

### 3.1.4 应用和数据安全

#### 1)风险分析

（1）目前本系统用户在互联网上通过移动端 App 使用用户名口令进行登录身份鉴别；本系统用户在政务办公网中通过 PC 端 IE11 浏览器使用用户名口令进行登录身份鉴别；均未使用密码技术对登录用户进行身份鉴别，存在应用被非授权人员登录风险。

（2）目前本系统通过统一身份认证系统对登录用户进行身份鉴别，统一身份认证系统未使用密码技术对本系统用户访问权限控制列表进行完整性保护，存在应用资源被非授权用户获取的风险。

（3）目前本系统用户登录身份鉴别信息、在系统中流转的电子公文数据均明文传输、存储，未使用密码技术进行传输、存储机密性、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。

（4）目前本系统应用日志记录明文存储在应用服务器中，未使用密码技术进行完整性保护，存在应用日志记录被

非授权篡改风险。

（5）目前本系统中流转的电子公文数据均未使用密码技术进行操作不可否认性保护，存在数据发送者或接收者不承认发送或接受到数据，或者否认所做的操作风险。

**2)密码应用需求**

（1）在本系统移动端 App 中部署符合密码相关国家、行业标准要求的移动端密码模块（二级）、在网络接入区边界部署符合密码相关国家、行业标准要求的安全认证网关，在新设置的系统基础设施区部署证书认证系统，通过证书认证系统分别向移动端密码模块（二级）、安全认证网关配置数字证书，实现移动端登录应用用户的安全身份鉴别，防止非授权人员登录；在本系统业务办公区 PC 端部署安全浏览器，在业务服务区部署 SSL VPN 安全网关，并向政务内网用户配发 USBKey，实现对 PC 端登录应用用户的安全身份鉴别，防止非授权人员登录。

（2）在网络接入区部署符合密码相关国家、行业标准要求的签名验签服务器，对统一身份认证系统应用用户访问权限控制列表进行完整性保护，防止应用资源被非授权用户篡改。

（3）在业务服务区部署符合密码相关国家、行业标准要求的服务器密码机，应用通过调用服务器密码机，对移动端登录用户身份鉴别数据、PC 端登录用户身份鉴别数据、系统

中流转的电子公文数据进行传输、存储机密性、完整性保护，实现身份鉴别数据、电子公文数据防窃取和防篡改保护。

（4）通过调用部署在业务服务区的服务器密码机，对应用日志记录进行完整性保护，防止应用日志记录被非授权篡改。

（5）在基础设施区部署符合密码相关国家、行业标准要求的电子签章系统、时间戳服务器，使用密码技术对在系统中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。

### 3.1.5 安全管理

#### 1)风险分析

本系统为已建在运行系统，在系统建设阶段，未依据密码相关国家、行业标准，制定密码应用方案，规划建设密码保障系统，系统上线前和运行后，均未开展过密码应用安全性评估，未依据《基本要求》中的安全管理要求，制定密码相关管理制度，不利于在本系统中落实密码相关国家政策要求，发挥密码在信息系统安全中的基础支撑作用。

#### 2)密码应用需求

依据《基本要求》，制定本系统密码应用改造方案，并委托密评机构对密码应用改造方案进行评估，评估通过后，建设密码保障系统，制定密码相关的管理制度，系统改造完成后，依据密码应用改造方案对本系统进行密码应用安全性评

估，评估通过后上线运行。

## 3.2 需求分析

**表 1 系统密码应用需求分析清单**

| 安全层面 | 指标要求 | 系统密码应用需求 | 不适用说明 |
|---|---|---|---|
| 物理和环境安全 | 身份鉴别 | 确认进入机房人员的身份真实性，防止假冒人员进入 | 无 |
| | 电子门禁记录数据完整性 | 保护电子门禁系统进出记录和视频监控音像记录的完整性，防止被非授权篡改 | 无 |
| | 视频记录数据完整性 | | |
| | 密码模块实现 | 采用符合要求的密码模块实现密码运算和密钥管理 | |
| 网络和通信安全 | 身份鉴别 | 确认业务服务区和数据灾备区之间通信实体的身份真实性，防止与假冒实体进行通信 | 无 |
| | 访问控制信息完整性 | 保护业务服务区和数据灾备区之间网络边界设备中的访问控制信息的完整性，防止被非授权篡改 | 无 |
| | 通信数据完整性 | 保护通信过程中灾备数据的完整性和机密性，防止数据被非授权篡改，防止敏感数据泄露 | 无 |
| | 通信数据机密性 | | |
| | 集中管理通道安全 | 建立安全的集中管理通道，对安全设备、安全组件进行集中管理，防止集中管理通道被非授权使用，防止传输的管理数据被非授权获取和非授权篡改 | 无 |
| | 密码模块实现 | 采用符合要求的密码模块实现密码运算和密钥管理 | |
| 设备和计算安全 | 身份鉴别 | 对使用政务办公网 PC 端浏览器登录的管理员的身份真实性进行识别和确认，防止假冒人员登录 | 无 |
| | 远程管理身份鉴别信息机密性 | 在远程管理时，对管理员的身份鉴别信息进行加密保护，防止鉴别信息泄漏 | |
| | 敏感标记的完整性 | 不适用 | 本系统无重要信息资源敏感标记 |
| | 访问控制信息完整性 | 保护计算机、服务器等设备中的系统资源访问控制信息、日志记录和重要可执行程序的完整性，防止被非授权篡改 | 无 |
| | 日志记录完整性 | | 无 |
| | 重要程序或文件完整性 | | 无 |

| 安全层面 | 指标要求 | 系统密码应用需求 | 不适用说明 |
| --- | --- | --- | --- |
| | 密码模块实现 | 采用符合要求的密码模块实现密码运算和密钥管理 | |
| 应用和数据安全 | 身份鉴别 | 确认互联网移动端 App、政务办公网 PC 端浏览器登录用户的身份真实性，防止假冒人员登录 | 无 |
| | 访问控制信息和敏感标记完整性 | 对统一身份认证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 |
| | 数据传输机密性 | 保护在客户端与服务器之间、应用系统之间的非安全网络信道中传输的和存储的用户登录身份鉴别信息、电子公文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 | 无 |
| | 数据存储机密性 | | |
| | 数据传输完整性 | | |
| | 数据存储完整性 | | |
| | 日志记录完整性 | 保护应用日志记录的完整性，防止被非授权篡改 | 无 |
| | 重要应用程序的加载和卸载 | 保护重要应用程序的加载和卸载，防止重要应用程序在加载过程中被非授权篡改 | 无 |
| | 抗抵赖 | 保护电子公文数据发送和接收操作的不可否认性，确保发送方和接收方对已经发生的操作行为无法否认 | 无 |
| | 密码模块实现 | 采用符合要求的密码模块实现密码运算和密钥管理 | |

# 4 设计目标及原则

## 4.1 设计目标

围绕《国家政务信息化项目建设管理办法》中关于政务信息系统在系统规划阶段的密码应用要求，综合考虑电子公文系统物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的电子公文处理系统密码应用方案，满足《基本要求》中三级指标要求，并为通过密码应用安全性评估奠定基础。

## 4.2 设计原则与依据

电子公文处理系统密码应用设计应遵循以下原则：

**（1）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，并与本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，为在本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，设计本系统密码改造方案。

**（3）经济性原则。**结合本系统规模，在合理、够用的前提下，设计满足《基本要求》的密码应用改造方案，确保本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。

**主要依据**

- GM/T 0054-2018《信息系统密码应用基本要求》
- GM/T 0071-2019《电子文件密码应用指南》
- 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 0023-2014《IPSec VPN 网关产品规范》
- GM/T 0024-2014《SSL VPN 技术规范》

- GM/T 0025-2014《SSL VPN 网关产品规范》
- GM/T 0026-2014《安全认证网关产品规范》
- GM/T 0030-2014《服务器密码机技术规范》
- GM/T 0031-2014《安全电子签章密码技术规范》
- GM/T 0027-2014《智能密码钥匙技术规范》
- GM/T 0014-2012《证书认证系统密码协议规范》
- GM/T 0028-2014《密码模块安全技术要求》
- GM/T 0033-2014《时间戳接口规范》
- GM/T 0029-2014《签名验签服务器技术规范》
- GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》

# 5 技术方案

## 5.1 密码应用技术框架

系统密码应用技术框架如下图 2 所示。根据我部电子公文处理系统的部署方式和实现业务功能，在满足总体性、完备性、经济性原则的基础上，要通过部署 USBKey、服务器密码机、签名验签服务器、SSL VPN 安全网关、安全认证网关、IPSec VPN、浏览器密码模块（二级）、移动端密码模块（二级）、电子签章系统、证书认证系统、安全门禁系统、时间戳服务器等密码产品，并正确部署配置，以满足本系统的密码应用需求。

其中，基础设施区是在原网络接入区、环境监控区、业务服务区等基础上，根据本次相关密码设备和系统部署的需

要新设置的，用于存放服务器密码机、证书认证系统、时间戳服务器、电子签章系统、签名验签系统等。

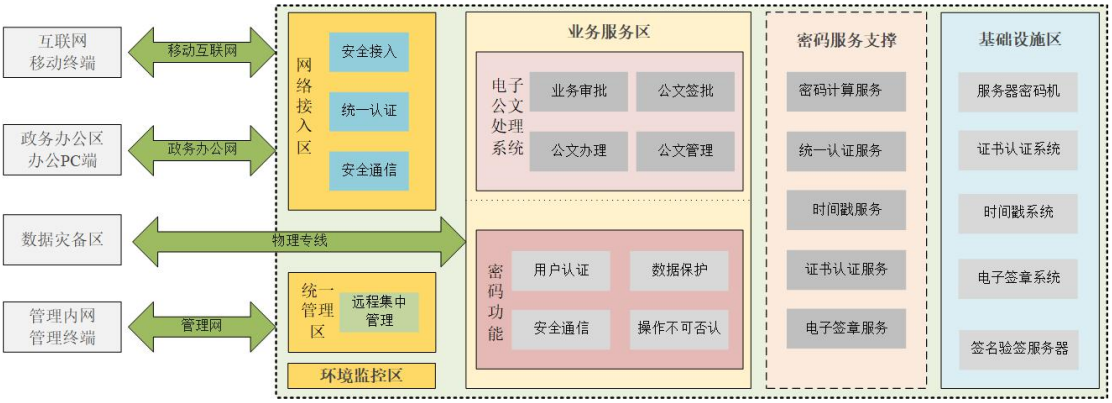


**图 2 电子公文处理系统密码应用技术框架**

其中：

**（1）USBKey：**主要提供签名验签、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书或电子印章等用户数据。根据用途的不同，USBKey又细分为身份鉴别Key和电子印章Key。1）身份鉴别Key中存放标识用户身份的数字证书，主要用于对用户身份真实性的鉴别。2）电子印章USBKey中存放遵循GM/T 0031《安全电子签章密码技术规范》的电子印章数据。本示例电子公文系统中用到的电子印章指单位公章，用于对电子公文进行签章，实现电子公文真实性和不可否认性保护。

**（2）服务器密码机：**主要为应用系统提供数据加解密、签名验签、杂凑等密码运算服务，实现信息的机密性、完整

性、真实性和不可否认性保护，同时提供安全、完善的密钥管理功能。

**（3）SSL VPN安全网关：**主要用于在网络上建立安全的信息传输通道，通过对数据包的加密和数据包目标地址的转换实现远程访问，进行加密通信。

**（4）电子签章系统：**为各级政务部门提供电子公章的签章、验章服务，有效保障电子文件的真实性、完整性和签章行为的不可否认性，是实现电子公文流转，部门协同办公的重要信任支撑。

**（5）移动端密码模块（二级）：**主要提供签名验签、加密解密、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书。

**（6）时间戳服务器：**时间戳能够唯一地标识某一时刻（通常为一段字符序列），从而可用于应用系统用户证明某些数据的产生时间，支撑公钥基础设施的“不可否认”服务。

**（7）安全门禁系统：**满足GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》标准要求，使用SM4算法进行密钥分散，实现门禁卡的“一卡一密”，并基于SM4算法对人员身份进行鉴别鉴别。

**（8）证书认证系统：**主要为设备/用户的身份鉴别提供真实性、身份验证、签名验签等信任服务。

**（9）签名验签服务器：**提供基于PKI体系和数字证书的数字签名、验证签名等运算功能，保证用户身份的真实性、完整性和关键操作的不可否认性。

**（10）IPSec VPN：**提供通信前通信双方身份鉴别、通信数据传输机密性、完整性保护等功能，对设备在通信前进行双向身份鉴别，保证通信通道的机密性、完整性。

**（11）安全认证网关：**采用数字证书为电子公文处理系统提供用户管理、身份鉴别、单点登录、传输加密、访问控制和安全审计等服务。

**（12）浏览器密码模块（二级）：**主要提供签名验签、加密解密、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书。

## 5.2 物理和环境安全

在系统所在机房部署符合 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，使用 SM4 算法进行密钥分散，实现门禁卡的“一卡一密”，并基于 SM4 算法对人员身份进行鉴别。

在系统环境监控区部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，使用 HMAC-SM3 技术对电子门禁系统进出记录和视频监控系统视频记录等数据进行完整性保护，其中 HMAC-SM3 密钥由环境监控区服务器密码机

生成，存储在服务器密码机中，不涉及密钥分发、导入与导出，密钥的备份与恢复、归档和销毁由密码设备管理员负责。

物理和环境安全层面使用的密码算法、密码技术、密钥管理由符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》、GM/T 0030-2014《服务器密码机技术规范》、GM/T 0028-2014《密码模块安全技术要求》的电子门禁系统和服务器密码机实现。

### 5.3 网络和通信安全

在本系统网络接入区和数据灾备区分别部署符合 GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》的 IPSec VPN，对进行数据备份的设备在通信前进行身份鉴别；并建立安全的数据备份传输通道。

在本系统统一管理区部署符合 GM/T 0025-2014《SSL VPN 网关产品规范》的 SSL VPN 安全网关，建立安全的集中管理通道。

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 GM/T 0025-2014《SSL VPN 网关产品规范》、GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》、GM/T 0028-2014《密码模块安全技术要求》的 SSL VPN 安全网关、IPSec VPN 实现。

### 5.4 设备和计算安全

在本系统业务办公区 PC 端部署安全浏览器，并向系统管

理员配发 USBKey，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护，防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。

在本系统应用服务区部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，并在应用服务器外挂符合 GM/T 0027-2014《智能密码钥匙技术规范》的 USBKey，应用服务器中所有重要程序或文件在生成时通过调用服务器密码机使用 SM2 数字签名技术进行完整性保护；使用或读取这些程序和文件时，通过 USBKey 进行验签以确认其完整性；公钥存放在 USBKey 中。

调用部署在应用服务区中的服务器密码机，使用 HMAC-SM3 对应用服务器、数据库服务器等设备日志进行完整性保护。

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、密钥管理由安全浏览器、符合 GM/T 0030-2014《服务器密码机技术规范》、GM/T 0027-2014《智能密码钥匙技术规范》、GM/T 0028-2014《密码模块安全技术要求》的 USBKey、服务器密码机实现。

### 5.5 应用和数据安全

在本系统移动端 App 中部署符合 GM/T 0028-2014《密码模块安全技术要求》的移动端密码模块（二级），在网络接入区边界部署符合 GM/T 0026-2014《安全认证网关产品规范》

的安全认证网关，在系统基础设施区部署符合 GM/T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》的证书认证系统，通过证书认证系统分别向移动端密码模块（二级）、安全认证网关配置数字证书，实现移动端登录应用用户的安全身份鉴别，防止非授权人员登录；在本系统业务办公区 PC 端部署安全浏览器，在业务服务区部署符合 GM/T 0025-2014《SSL VPN 网关产品规范》的 SSL VPN 安全网关，并向相关用户配发 USBKey，实现对 PC 端登录应用用户的安全身份鉴别，防止非授权人员登录。

在网络接入区部署符合 GM/T 0029-2014《签名验签服务器技术规范》的签名验签服务器，使用数字签名技术对统一身份认证系统应用用户访问权限控制列表进行完整性保护，防止应用资源被非授权用户获取。

在业务服务区分别部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机和符合 GM/T 0025-2014《SSL VPN 网关产品规范》的 SSL VPN 安全网关，应用通过调用服务器密码机，对移动端登录用户身份鉴别数据、PC 端登录用户身份鉴别数据、系统中流转的电子公文数据进行传输、存储机密性、完整性保护，实现身份鉴别数据、电子公文数据防窃取和防篡改保护；PC 端安全浏览器与 SSL VPN 安全网关之间使用合规的 SSL 协议，建立安全的数据传输通道，实现数据传输机密性、完整性保护。

应用通过调用部署在业务服务区的服务器密码机，使用HMAC-SM3对应用日志记录进行完整性保护，防止应用日志记录被非授权篡改。

在基础设施区部署符合GM/T 0031-2014《安全电子签章密码技术规范》、GM/T 0033-2014《时间戳接口规范》的电子签章系统、时间戳服务器，使用密码技术对在系统中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。

应用和数据安全层面所要求的密码算法、密码技术、密码服务、密钥管理由安全浏览器、符合GM/T 0027-2014《智能密码钥匙技术规范》、GM/T 0026-2014《安全认证网关产品规范》、GM/T 0029-2014《签名验签服务器技术规范》、GM/T 0030-2014《服务器密码机技术规范》、GM/T 0031-2014《安全电子签章密码技术规范》、GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》、GM/T 0033-2014《时间戳接口规范》、GM/T 0014-2012《证书认证系统密码协议规范》、GM/T 0028-2014《密码模块安全技术要求》等标准要求的移动端密码模块（二级）、USBKey、安全认证网关、签名验签服务器、服务器密码机、电子签章系统、时间戳服务器和证书认证系统实现。

## 5.6 密钥管理安全

本系统无独立的对称密钥管理系统，使用的数字证书由

本系统中部署的证书认证系统颁发。考虑到本系统独立部署在我部办公大楼内部，用户仅有我部内部人员，不与其他机构进行用户身份互认，系统证书规模较小，故采用自建CA为部署在本系统中的IPSec/SSL VPN、USBKey、安全认证网关颁发数字证书，并制定严格的CA管理操作规程，保证密钥等信息和系统的部署、使用安全。

本系统选用通过检测认证的USBKey、SSL VPN安全网关、安全认证网关、IPSec VPN、签名验签服务器、服务器密码机、时间戳服务器、安全门禁系统、安全电子签章系统、证书认证系统、移动端密码模块（二级）、浏览器密码模块（二级）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。

## 5.7 密码应用部署

本系统部署和使用了SSL VPN安全网关、安全认证网关、USBKey、移动端密码模块（二级）、浏览器密码模块（二级）、签名验签服务器、服务器密码机、IPSec VPN、电子签章系统、时间戳服务器、证书认证系统、安全门禁系统等密码产品，均选自《商用密码产品认证目录（第一批）》，通过了具备资质的商用密码认证机构认证。系统密码应用部署拓扑如下图3所示。

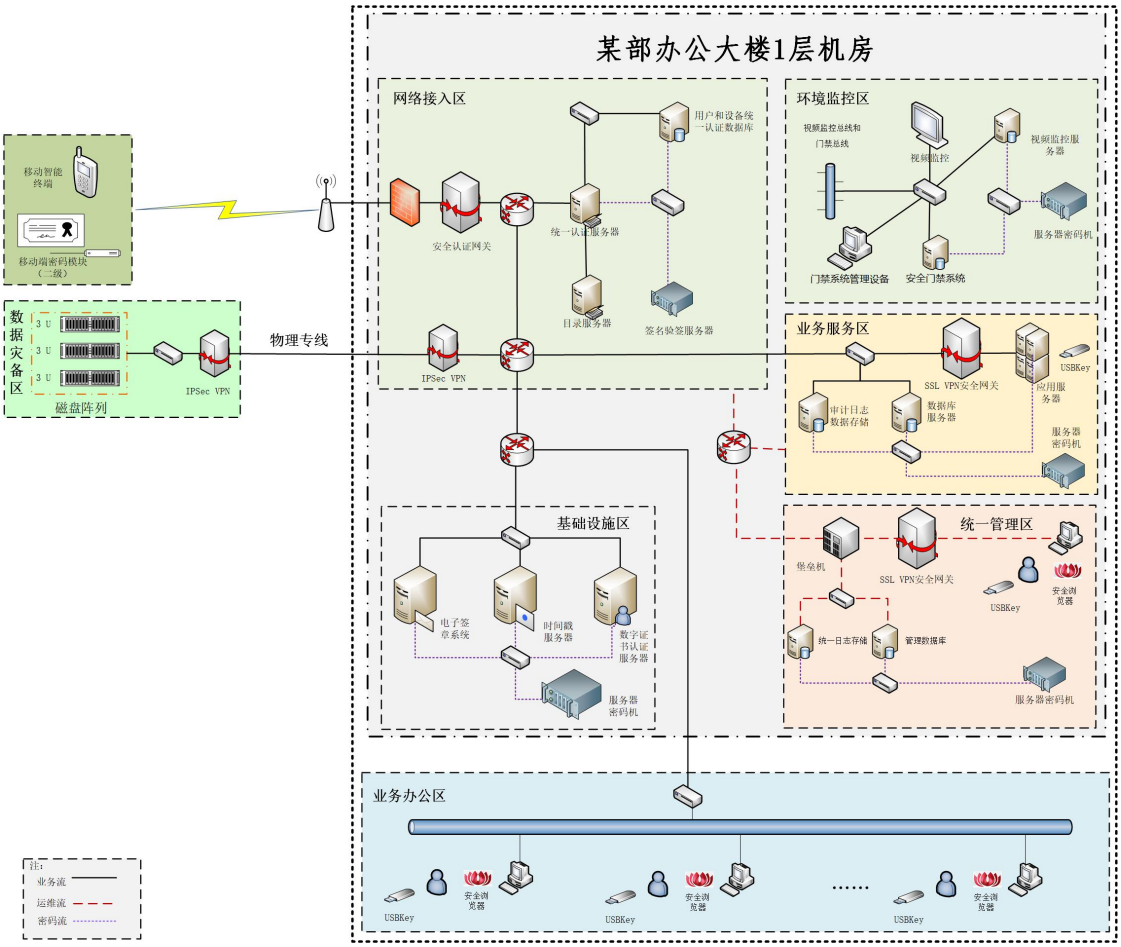


图 3 电子公文处理系统密码部署图

**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、身份鉴别等的过程及相关数据流转。

## 5.8 密码软硬件产品清单

表 2 系统密码软硬件产品清单

| 序号 | 产品名称 | 部署位置 | 使用的密码算法 | 数量 | 用途 |
|---|---|---|---|---|---|
| 1 | USBKey | 业务办公区 | SM2/3/4 | 按需配置 | 系统用户/管理员登录身份鉴别 |
| 2 | 浏览器密码模块（二级） | 业务办公区 | SM2/3/4 | 按需配置 | 部机关内部人员安全登录系统 |
| 3 | 移动端密码 | 移动智能终 | SM2/3/4 | 按需配置 | 移动端用户安全接 |

| | | | | | |
|---|---|---|---|---|---|
| | 模块（二级） | 端 | | | 入身份鉴别 |
| 4 | 证书认证系统 | 基础设施区 | SM2/3/4 | 1 | 为设备/用户的身份鉴别提供真实性服务 |
| 5 | 电子签章系统 | 基础设施区 | SM2/3/4 | 1 | 提供电子公章的签章、验章服务 |
| 6 | 时间戳服务器 | 基础设施区 | SM2/3/4 | 1 | 提供可靠的时间 |
| 7 | 服务器密码机 | 基础设施区 | SM2/3/4 | 1 | 为数字证书系统提供高性能密码计算 |
| 8 | 安全认证网关 | 网络接入区 | SM2/3/4 | 1 | 为移动办公人员提供安全接入通道 |
| 9 | 签名验签服务器 | 网络接入区 | SM2/3/4 | 1 | 供统一身份认证系统调用，鉴别用户身份 |
| 10 | 服务器密码机 | 环境监控区 | SM2/3/4 | 1 | 对电子门禁数据和视频监控音像记录等进行完整性保护 |
| 11 | 安全门禁系统 | 环境监控区 | SM4 | 1 | 对进入机房人员进行身份鉴别 |
| 12 | 服务器密码机 | 业务服务区 | SM2/3/4 | 1 | 对重要业务数据进行存储机密性、完整性保护 |
| 13 | USBKey | 业务服务区 | SM2/3/4 | 按需配置 | 在使用或读取应用服务器中的重要程序和文件进行验签以确认其完整性 |
| 14 | SSL VPN 安全网关 | 业务服务区 | SM2/3/4 | 1 | 配合 PC 端部署的安全浏览器，实现 PC 端到服务端之间数据传输机密性保护 |
| 15 | IPSec VPN | 网络接入区 | SM2/3/4 | 1 | 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 |

| | | | | | |
|---|---|---|---|---|---|
| 16 | USBKey | 统一管理区 | SM2/3/4 | 按需配置 | 应用/设备管理员登录堡垒机 |
| 17 | 服务器密码机 | 统一管理区 | SM2/3/4 | 1 | 对审计日志记录进行完整性保护 |
| 18 | 浏览器密码模块（二级） | 统一管理区 | SM2/3/4 | 1 | 管理员安全登录堡垒机 |
| 19 | SSL VPN 安全网关 | 统一管理区 | SM2/3/4 | 1 | 建立安全的集中管理通道 |
| 20 | IPSec VPN | 数据灾备区 | SM2/3/4 | 1 | 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 |

## 5.9 安全与合规性分析

**表 3 密码应用合规性对照表**

| 指标要求 | 密码技术应用点 | 采取措施 | 标准符合性（符合/不适用） | 说明（针对不适用项说明原因及替代性措施） |
|---|---|---|---|---|
| 物理和环境安全 | 身份鉴别 | 在系统所在机房部署安全电子门禁系统，使用 SM4 算法进行密钥分散，实现门禁卡的一卡一密，并基于 SM4 算法对人员身份进行鉴别鉴别 | 符合 | 无 |
| | 电子门禁记录数据完整性 | 在系统环境监控区部署服务器密码机，使用 HMAC-SM3 技术对电子门禁系统进出记录和视频监控系统视频记录等数据进行完整性保护 | 符合 | 无 |
| | 视频记录数据完整性 | | 符合 | 无 |
| | 密码模块实现 | 在安全电子门禁系统和服务器密码机中实现密码算法、密码技术、密钥管理 | 符合 | 无 |
| 网络和通信安全 | 身份鉴别 | 在本系统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 | 符合 | 无 |

| 指标要求 | 密码技术应用点 | 采取措施 | 标准符合性（符合/不适用） | 说明（针对不适用项说明原因及替代性措施） |
|---|---|---|---|---|
| | | 智能移动终端接入本系统的身份鉴别在“应用和数据安全”层面实现 | | |
| | 访问控制信息完整性 | 在本系统网络接入区和数据灾备区分别部署IPSec VPN，对访问控制信息进行完整性保护<br>智能移动终端接入本系统所涉及的访问控制信息的完整性在“应用和数据安全”层面实现 | 符合 | 无 |
| | 通信数据完整性<br>通信数据机密性 | 在本系统业务服务区和数据灾备区分别部署IPSec VPN，建立安全的备份数据传输通道<br>智能移动终端与本系统的通信数据机密性和完整性在“应用和数据安全”层面实现 | 符合 | 无 |
| | 集中管理通道安全 | 在本系统统一管理区部署SSL VPN安全网关，建立安全的集中管理通道 | 符合 | 无 |
| | 密码模块实现 | 在SSL VPN安全网关中实现密码算法、密码技术、密钥管理 | 符合 | 无 |
| 设备和计算安全 | 身份鉴别<br>远程管理身份鉴别信息机密性 | 在本系统业务办公区PC端部署安全浏览器，并向系统管理员配发USBKey，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护 | 符合 | 无 |
| | 访问控制信息完整性 | 仅有管理员可以访问应用服务器、数据库服务器，管理员身份鉴别通过USBKey实现，使用数字签名技术对应用服务器、数据库服务器管理员用户访问权限控制列表进 | 符合 | 无 |

| 指标要求 | 密码技术应用点 | 采取措施 | 标准符合性（符合/不适用） | 说明（针对不适用项说明原因及替代性措施） |
| --- | --- | --- | --- | --- |
| | | 行完整性保护 | | |
| | 敏感标记的完整性 | 无 | 不适用 | 本系统不涉及重要信息资源的敏感标记 |
| | 日志记录完整性 | 在本系统应用服务区部署服务器密码机，调用服务器密码机，使用HMAC-SM3对应用服务器、数据库服务器等设备日志进行完整性保护 | 符合 | 无 |
| | 重要程序或文件完整性 | 在本系统应用服务区部署服务器密码机，并在应用服务器外挂USBKey，应用服务器中所有重要程序或文件在生成时通过调用服务器密码机使用SM2数字签名技术进行完整性保护，使用或读取这些程序和文件时，通过USBKey进行验签以确认其完整性；公钥存放在USBKey中 | 符合 | 无 |
| | 密码模块实现 | 由密码模块（二级）、USBKey、服务器密码机实现密码算法、密码技术、密码服务、密钥管理 | 符合 | 无 |
| 应用和数据安全 | 身份鉴别 | 1.在本系统移动端App中部署移动端密码模块（二级），在网络接入区边界部署安全认证网关，在系统基础设施区部署证书认证系统，通过证书认证系统分别向移动端密码模块（二级）、安全认证网关配置数字证书，实现移动端登录应用用户的安全身份鉴别；<br>2.在本系统业务办公区PC端部署安全浏览器，在业务服务区部署SSL | 符合 | 无 |

| 指标要求 | 密码技术应用点 | 采取措施 | 标准符合性（符合/不适用） | 说明（针对不适用项说明原因及替代性措施） |
| --- | --- | --- | --- | --- |
| | | VPN 安全网关，并向政务内网用户配发 USBKey，实现对 PC 端登录应用用户的安全身份鉴别 | | |
| | 访问控制信息和敏感标记完整性 | 在网络接入区部署签名验签服务器，使用数字签名技术对统一身份认证系统应用用户访问权限控制列表进行完整性保护 | 符合 | 本系统不涉及重要信息的敏感标记 |
| | 数据传输机密性<br>数据存储机密性<br>数据传输完整性<br>数据存储完整性 | 在业务服务区部署服务器密码机和 SSL VPN 安全网关，应用通过调用服务器密码机，对移动端登录用户身份鉴别数据、PC 端登录用户身份鉴别数据、系统中流转的电子公文数据进行传输、存储机密性、完整性保护，实现身份鉴别数据、电子公文数据防窃取和防篡改保护；<br>PC 端安全浏览器与 SSL VPN 安全网关之间使用合规的 SSL 协议，建立安全的数据传输通道，实现数据传输机密性、完整性保护。 | 符合 | 无 |
| | 日志记录完整性 | 调用部署在业务服务区的服务器密码机，使用 HMAC-SM3 对应用日志记录进行完整性保护 | 符合 | 无 |
| | 重要应用程序的加载和卸载 | 仅有管理员可以进行重要应用程序的加载和卸载，而管理员的身份鉴别在“设备和计算安全”层面完成 | 符合 | 无 |
| | 抗抵赖（四级） | 在基础设施区部署电子签章系统、时间戳服务器，使用密码技术对在系 | 符合 | 无 |

| 指标要求 | 密码技术应用点 | 采取措施 | 标准符合性（符合/不适用） | 说明（针对不适用项说明原因及替代性措施） |
|---|---|---|---|---|
| | | 统中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 | | |
| | 密码模块实现 | 由安全浏览器、USBKey、SSL VPN 安全网关、移动端密码模块（二级）、电子签章系统、服务器密码机、时间戳服务器和证书认证系统实现密码算法、密码技术、密码服务、密钥管理 | 符合 | 无 |

# 6 安全管理方案

## 6.1 制度

根据《基本要求》中安全管理制度方面的要求，制定与本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 6 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，在我部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

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。

一是设置内部密码专题培训机制，每6个月组织一次，由内部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和标准规范、商用密码应用、商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的法律和法规，掌握密码基本原理，并遵照执行；

二是在本系统完成密码应用改造后，安排项目建设单位、相关密码设备厂商对本系统部署使用的所有密码产品进行操作培训，确保相关人员能够正确配置使用本系统中部署的密码产品；

三是结合本系统情况，分别设立密钥管理员、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；

四是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，每年对密钥管理人员、安全审计人员、密码操作人员组织一次考核，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；密钥管理人员、安全审计人员、密码操作人员与单位订保密协议，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 实施

完成本方案编制后，委托密评机构对本方案进行评估，评估通过后，将本系统密码应用改造方案向我部密码管理部门备案，并同步对本系统进行密码应用改造，选用通过检测认证合格的USBKey、服务器密码机、签名验签服务器、SSL VPN安全网关、安全认证网关、IPSec VPN、浏览器密码模块（二级）、移动端密码模块（二级）、电子签章系统、证书认证系统、安全门禁系统、时间戳服务器等商用密码产品，合规、正确、有效的建设密码保障系统。

依据评估通过的密码应用方案改造完成后，委托密评机构对本系统进行密评，密评通过后上线运行，上线运行后，每年对本系统进行一次密码应用安全性评估，并根据评估意见进行整改。当本系统在运行过程中发现重大密码应用安全隐患时，将停止系统运行，制定整改方案，按照整改方案对系统进行整改和密码应用安全性评估，评估通过后重新上线运行。

## 6.4 应急

根据《基本要求》中安全管理应急方面的要求，对本系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施；针对密码安全方面的应急响应措施包括：当本系统发生密码相关安全事件时，在事发后3小时内向我部办公厅进行报告；事件处置完成后2个工作日内，向我部

办公厅汇报安全事件发生情况及处置情况。

# 7 实施保障方案

略。