# 2 系统概述

## 2.1基本情况

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：系统基本情况包括系统名称、系统责任主体单位情况(名称、地址、所属密码管理部门和单位类型等)、系统上线运行时间、系统用户情况(使用单位、使用人员和使用场景等)、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以及密码应用安全性评估情况等。根据系统实际情况，示例写法如下：**

### 2.1.1系统名称

{{sysname}}

### 2.1.2系统责任主体单位

建设单位名称：{{sysunit}}

地址：{{jsdwdz}}

所属密码管理部门：{{ssmmglbm}}

单位类型：{{dwlx}}

### 2.1.3系统上线运行时间

{{xtsxyxsj}}

### 2.1.4系统用户情况

| **序号{{table21}}** | **用户角色** | **业务场景** | **网络访问位置** |
| --- | --- | --- | --- |
|  | [yh] | [ywyy] | [szwl] |

### 2.1.5关键基础设施说明

{{gjjcsssm}}

### 2.1.6网络安全等级保护情况

{{dbcp}}

### 2.1.7密码应用安全性评估情况

{{mmaqpg}}

### 2.1.8部署情况

{{bsqk}}

## 2.2计算平台现状

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：如果密码应用方案包括计算平台密码应用方案设计,则包括以下具体描述。**

1. **物理环境:包括机房或重要场所地点、系统部署位置、内外部环境和管理责任主体。**
2. **网络环境: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. **计算环境: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)。**

**如果密码应用方案不包括计算平台密码应用方案设计,则描述计算平台的场所地点和密码应用安全性评估情况。**

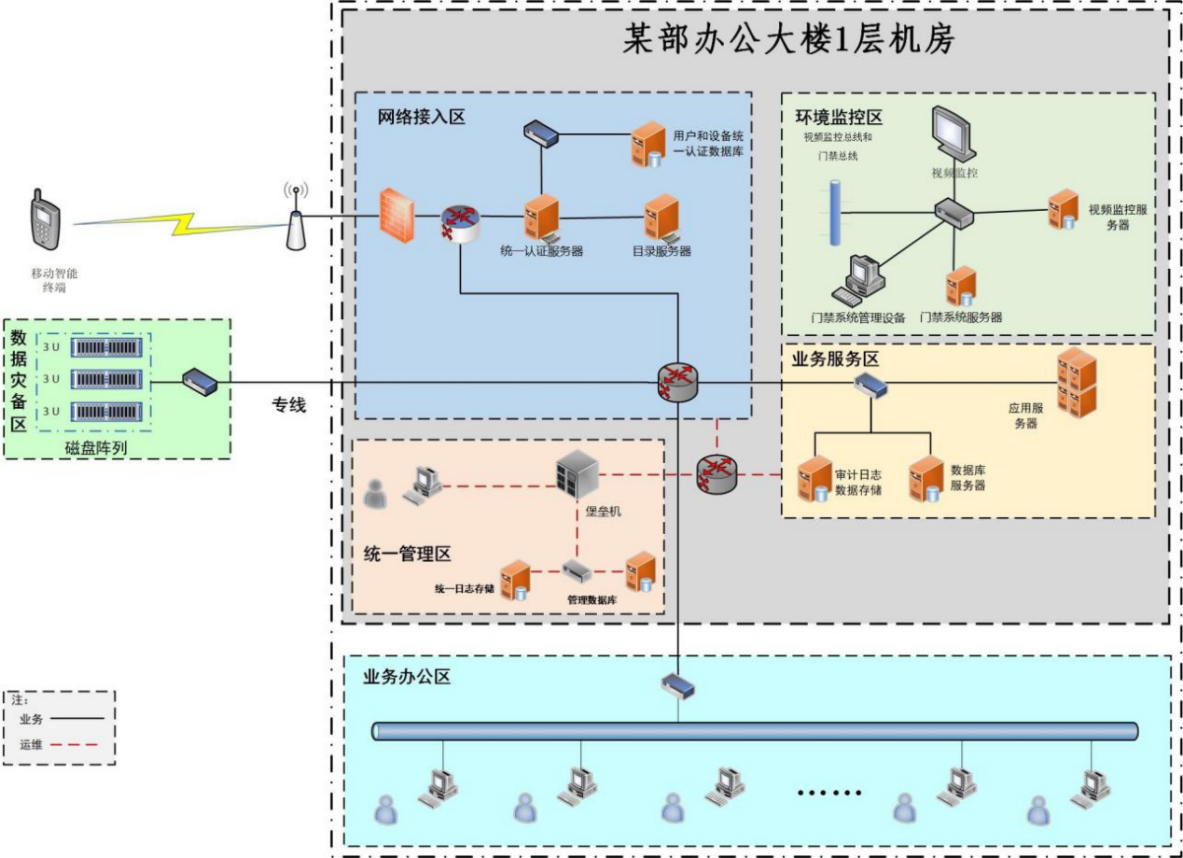
**计算平台密码应用方案设计的根据系统实际情况，示例写法如下：**

### 2.2.1物理环境现状

本系统部署在{{jfmclist}}，地址为{{jfdzlist}}。机房安装有门禁和视频监控系统，门口有专人值守，且进出机房需要实名登记。机房管理责任主体单位为{{jfzrztdwlist}}，机房外部所在大楼（园区）为运营商所有，由运营商管理。

### 2.2.2网络环境现状

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。系统网络拓扑如下图1所示：



**图 1 系统网络拓扑图**

**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。

**统一管理区**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。

**内外部数据交互情况：**在内部数据交互过程中，用户在办公大楼局域网环境下，可通过部署在我部业务办公区的PC终端浏览器访问登录应用系统。运维人员使用运维终端在局域网，通过堡垒机实现统一集中运维管理。在外部数据交互过程中，用户在互联网环境下可通过移动智能终端访问登录应用系统；办公大楼1层机房业务服务器区通过专线将数据传输至灾备机房实现数据级灾备。

根据网络结构划分及数据交互情况，系统跨网络访问的信道有两个：①内部用户PC浏览器与业务系统之间的通信信道；②系统业务服务区和数据灾备区之间的专线通信信道；③公众用户移动端 APP与业务系统之间的通信信道；④XXX系统与业务系统之间的通信信道。

服务通道采用HTTPS方式，通过政务外网/互联网/内网对内部用户提供XXX服务，现阶段对内部PC端用户采用用户名+口令方式进行身份鉴别，未使用密码技术进行身份鉴别，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，未使用密码技术对该条信道的网络边界访问控制信息进行完整性保护。

目前系统业务服务区和数据灾备区之间的专线通信信道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实体双方进行验证， 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，未使用密码技术对该条信道的网络边界访问控制信息进行完整性保护。

目前互联网系统移动端 APP的通信信道使用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，未使用密码技术对该条信道的网络边界访问控制信息进行完整性保护。

### 2.2.3计算环境现状

{{sysname}}系统的软硬件设备情况如表2.7所示：

表 2.7 通用设备调查表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **设备名称{{table25}}** | **品牌型号** | **数量** | **操作系统** | **数据库** | **登录方式** |
| [sbmc] | [ppxh] | [sl] | [czxt] | [sjk] | [sfrz] |

{{sysname}}系统的其他软硬件设备情况如表2.8所示：

表 2.8 专用设备调查表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **设备类型** | **设备名称** | **品牌型号** | **数量** | **是否支持国密算法** | **是否有商密证书** | **是否支持远程运维** | **身份认证方式** | **是否过堡垒机** |
| **密码产品/**  **密码设备{{table261}}** | [sbmc] | [ppxh] | [sl] | [gmsf] | [smzs] | [ycyw] | [sfrz] | [blj] |
|  | | | | | | | |
| **具有密码功能的网络及安全设备(含云平台提供的虚拟VPN、堡垒机等) {{table262}}** | [sbmc] | [ppxh] | [sl] | [gmsf] | [smzs] | [ycyw] | [sfrz] | [blj] |
|  | | | | | | | |
| **采用密码技术的其他产品{{table263}}** | [sbmc] | [ppxh] | [sl] | [gmsf] | [smzs] | [ycyw] | [sfrz] | [blj] |
|  | | | | | | | |
| **没有密码功能的网络及安全设备{{table264}}** | [sbmc] | [ppxh] | [sl] | [gmsf] | [smzs] | [ycyw] | [sfrz] | [blj] |
|  | | | | | | | |
| **虚拟设备和系统{{table265}}** | [sbmc] | [ppxh] | [sl] | [gmsf] | [smzs] | [ycyw] | [sfrz] | [blj] |
|  | | | | | | | |

目前本系统运维管理员用户通过PC浏览器，使用账号+口令登录堡垒机，使用http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进行远程管理的进行安全保护。

目前运维管理员接入堡垒机后，由堡垒机使用SSH协议与服务器之间建立远程管理通道，使用账号+口令登录服务器实现服务器及数据库的远程管理。未使用密码技术对登录服务器人员进行身份鉴别，未使用合规的密码技术对进行远程管理的进行安全保护。

目前堡垒机、服务器、数据库设备的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。设备的系统资源访问控制信息和日志记录均由设备自身明文存储，未使用密码技术进行完整性保护。

## 2.3业务应用现状

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：**

**业务应用现状包括以下具体描述。**

1. **业务应用的基本情况,包括承载的业务情况和责任主体等。**
2. **承载的业务情况,包括系统承载的业务应用、业务功能和关键数据类型等**
3. **对于多个子应用的信息系统,对每个子应用分别描述。根据系统实际情况，示例写法如下：**

### 2.3.1业务应用基本情况

XXX系统由A系统和B系统两个应用组成，其中A系统主要实现系统用户的统一身份认证。认证通过后用户进XXX系统应用，该应用主要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。XXX系统责任主体为我部，由我部对该系统进行运维管理。

### 2.3.2承载业务情况

#### 2.3.2.1业务应用

描述业务系统逻辑架构图和对应文字介绍。

（需提供逻辑架构图）

系统管理员和普通用户在政务办公网中通过PC浏览器，使用用户名+口令登录应用系统；在互联网通过移动端App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。

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。

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、日志数据、访问控制信息数据均明文传输、存储，未使用密码技术进行传输、存储机密性、完整性保护。

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。

#### 2.3.2.2业务功能

描述业务系统功能，如子模块介绍等。

#### 2.3.2.3关键数据类型

{{sysname}}的应用层用户包括XXXXX员、XXXXX员、XXXXX用户、XXXXX用户。涉及的重要数据包括日志数据、鉴别数据和重要业务数据。重要业务数据包括：XXXX数据、XXXX数据、XXXX数据、XXXX数据。

系统涉及的关键操作有XXX。

XXXX系统的被保护对象信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号{{tableTest}} | 应用名称 | 类别 | 具体保护对象 | 安全需求 |
| [index] | [yymc] | [lb] | [jtbhdx] | [aqxq] |
| 1 | XXXXX系统 | 应用用户 | 系统管理员 | 真实性 |
| XXXX员 | 真实性 |
| XXXX员 | 真实性 |
| 重要数据 | 鉴别数据 | ☑传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 业务数据（XXXXXXX） | □传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 日志数据（用户登录、退出、操作日志等） | □传输机密性  □传输完整性  □存储机密性  ☑存储完整性 |
| 关键操作 | XXXXX行为 | 不可否认性 |
| ... | ... |
| N | XXXXX系统（根据实际，有子系统的按需求添加） | 应用用户 | 系统管理员 | 真实性 |
| XXXX员 | 真实性 |
| XXXX员 | 真实性 |
| 重要数据 | 鉴别数据 | ☑传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 业务数据（XXXXXXX） | ☑传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 日志数据（用户登录、退出、操作日志等） | □传输机密性  □传输完整性  □存储机密性  ☑存储完整性 |
| 关键操作 | XXXXX行为 | 不可否认性 |
| ... | ... |

## 2.4密码应用现状

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：信息系统部署密码设施设备的基本情况、责任主体和密码支撑情况(如密码中间件的部署情况和密码功能的提供模式)等。根据系统实际情况，示例写法如下：**

系统当前未部署相关密码软硬件设施设备，未形成密码支撑功能供上层应用系统调用。本次密码应用方案通过后，我部将会依据方案部署相应密码密码软硬件设施设备，按照密码应用策略配置相关形成密码支撑功能。

### 2.4.1物理和环境安全现状

{{wlhhjaqxz}}

### 2.4.2网络和通信安全现状

{{wlhtxaqxz}}

### 2.4.3设备和计算安全现状

在运维侧，管理员用户通过堡垒机访问所需运维设备，使用用户名口令的方式对运维人员身份鉴别。通过{{bljfwfs}}方式访问堡垒机，未使用合规的商密VPN技术进行远程管理通道的安全防护，相关日志未做完整性保护。

### 2.4.4应用和数据安全现状

现阶段业务系统包含多个子模块，涉及的系统开发语言是{{kfyy}}，数据库类型是{{sjklx}}，{{sjmwcc}}未采用合规的码技术保证信息系统应用的重要数据在传输和存储过程中的机密性和完整性。

## 2.5密码应用管理现状

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：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。根据系统实际情况，示例写法如下：**

{{mmyyglxz}}