# 2 系统概述

首先要确认密码应用的目标信息系统对象，原则上和网络安全等级保护确定的对象、级别一致，分为1-4级，可参考GBT 22240-2020《信息安全技术—网络安全等级保护定级指南》确定目标信息系统，基本原则是1）具有确定的主要安全责任主体；2）承载相对独立的业务应用；3）包含相互关联的多个资源，避免将单个系统组件，如服务器、终端或网络设备作为对象。

根据对目标信息系统的调研整理系统情况，为后续风险分析、密码应用需求、方案设计奠定基础。2.1节介绍系统基本情况，根据GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》，2.2节介绍系统网络拓扑情况，2.3节介绍系统承载的业务情况，2.4节介绍系统软硬件构成情况，2.5节介绍目前的密码管理制度。

## 2.1 系统基本情况

本小节介绍该系统的基本情况，包括系统名称、网络安全保护等级等基本情况，如表2.1所示：

### 2.1.1 基本情况

本系统于XXXX年x月x日完成网络安全等级保护定级备案（测评机构：XXXX，备案编号：XXXXX），定级等级为第3级（S3A3G3），本系统于20XX年X月上线使用，系统的最近一次等级测评时间为\*\*年\*\*月\*\*日，测评机构为：\*\*\*\*\*\*\*\*\*\*，测评结论为：\*\*\*\*\*\*\*\*\*\*。最近一次商用密码安全性评估时间为\*\*年\*\*月\*\*日，测评机构为：\*\*\*\*，测评结论为：\*\*。

{{sysname}}系统基本情况如表2.1所示：

表 2.1 系统基本情况表

|  |  |  |  |
| --- | --- | --- | --- |
| **系统名称** | {{sysname}} | **责任单位** | {{sysunit}} |
| **系统建设** | {{xtjs}} | **单位地址** | {{dwdz}} |
| **密评首次** | {{mpsc}} | **等保级别** | {{dbjb}} |
| **上线时间** | {{sxsj}} | **完成等保定级时间** | {{dbsj}} |
| **定级编号** | {{djbh}} | **测评机构** | {{cpjg}} |
| **系统结构** | {{xtjg}} | **密码制度** | {{mmzd}} |
| **服务端** | {{fwd}} | **移动端** | {{ydd}} |
| **云上部署** | {{ysbs}} | **若在云上** | {{rzys}} |

### 2.1.2 系统架构

{{sysname}}架构，如图2.1所示。其包含四个逻辑层，具体描述如图 2.1所示。



图 2.1 {{sysname}}架构图

（一）展现层：{{sysname}}展现层表现为运维人员操作Web界面、客户端及手机端的操作页面。普通用户、系统管理员通过系统Web界面进行业务操作，公众用户用户通过手机端进行业务操作。

（二）应用层：{{sysname}}应用层核心功能包括XX单位1、2系统、3系统、4系统、5系统、6系统。

（三）数据层：{{sysname}}数据层主要是数据信息的存储，包括业务信息数据库、基础信息数据库。

（四）物理层：{{sysname}}物理层表现为实体的系统载体，包括业务应用服务器、业务数据服务器、数据库服务器。

### 2.1.3 机房情况

{{sysname}}系统机房情况如表2.2所示：

表 2.2 机房调查表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **机房名称{{table22}}** | **机房类型** | **门禁** | **身份认证方式** | **视频监控** | **是否允许增加设备** |
| [jfmc] | [jflx] | [mj] | [sfrz] | [spjk] | [zjsb] |

## 2.2 系统网络拓扑

### 2.2.1 网络拓扑

{{sysname}}系统网络拓扑，如图2.2所示：



图 2.2 网络拓扑图

【最好能根据图补充文字描述，如下所示】

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。

### 2.2.2 网络通信信道

{{sysname}}系统的跨网络访问的通信信道情况如表2.3所示：

表 2.3 通信信道调查表

|  |  |  |
| --- | --- | --- |
| **序号{{table23}}** | **测评对象** | **描述** |
| [index] | [cpdx] | [ms] |

## 2.3 承载的业务情况

### 2.3.1 业务应用

{{sysname}}系统所具有的功能及业务应用，如表2.5所示：

表 2.4 业务应用调查表

|  |  |  |
| --- | --- | --- |
| **业务应用{{table27}}** | **功能描述** | **对外服务方式** |
| [ywyy] | [gnms] | [fwfs] |

### 2.3.2 重要数据

{{sysname}}系统的重要数据如表2.6所示：

表 2.6 重要数据调查表

|  |  |  |  |
| --- | --- | --- | --- |
| **业务应用{{table28}}** | **数据类型** | **数据内容** | **安全需求** |
| [ywyy] | [sjlx] | [sjnr] | [bhxq] |

## 2.4 系统软硬件构成

{{sysname}}系统的软硬件设备情况如表2.5所示：

表 2.5 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2.6所示：

表 2.6 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] |
|  | | | | | | | |

## 2.5 管理制度

{{26}}