# 5 密码应用技术方案

根据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，结合信息系统的实际情况，项目预算及拟采购的密码产品，设计密码应用技术方案，保障密码应用的合规性、正确性和有效性。

其中，5.1节介绍密码应用技术框架和整体架构，5.2-5.5节分别从物理和环境、网络和通信、设备和计算、应用和数据四个方面介绍典型的密码应用技术方案，以及结合本系统实际情况、采用的密码产品、设计的密码应用解决方案，5.6节介绍密钥管理方案，5.7节介绍密码应用部署，5.8节介绍本项目拟采购的密码软硬件产品，5.9节从物理和环境、网络和通信、设备和计算、应用和数据四个方面，做商用密码应用的技术部分安全与合规性分析。

## 5.1 密码应用技术框架

基于国产密码标准体系和密码管理体系，结合目标信息系统的实际情况，基于GB/T 39786-2021《信息系统密码应用基本要求》，建设以保护业务系统的身份认证及数据资产为中心的、自主可控的密码服务体系，通过核心的密码技术、密码模块、密码产品、密码基础设施等产品服务，为网络基础资源、信息设施、计算分析、应用服务、网络通道、接入终端、设备控制等提供身份鉴别、访问控制、数据机密性、完整性、及抗抵赖的密码服务。

密码应用技术总体架构如图 5.1所示。



图 5.1 密码应用技术架构

密码应用技术框架分为密码基础服务层和密码应用层，密码应用层包括终端安全密码应用、网络接入安全密码应用、业务安全密码、平台管理安全密码应用四部分。

1. 密码基础服务层

密码基础服务层由服务器密码机、签名验签服务器、时间戳服务器、数字证书认证系统、安全电子签章系统、密钥管理系统等设备组成，通过统一密码服务中间件，为业务应用提供数据加密服务、时间戳服务、签名验签服务、完整性验证服务等密码应用所需基础服务。

1. 密码应用层

密码应用层通过调用密码服务平台的一系列服务来保证密码应用安全：

* 1. 终端安全密码应用：采用智能密码钥匙解决用户在登录系统和业务操作的身份鉴别，保证了身份的真实性。
  2. 网络接入安全密码应用，部署可信浏览器、IPSec VPN，实现终端身份鉴别和数据传输加密保护；在PC端部署VPN客户端，建立数据安全传输通道。
  3. 系统业务安全密码应用，主要为业务应用提供身份验证服务、数据加密服务、完整性验证服务、数据安全存储服务。

密码基础服务平台

基于各密码产品构建的密码基础服务平台的主要功能是为上层应用提供密码基础服务支撑，实现上层应用的密码安全增强。该平台使用符合国家密码法规和标准规定的商用密码算法，使用经过国家密码管理局核准的密码产品，遵循“GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》”以及相关“密评”规范。

密码基础服务平台整合服务器密码机、证书认证系统、签名验签服务系统、通用统一密码等产品能力，打造服务化、场景化，易于行业快速对接集成的密码服务能力，实现密码基础服务平台统一、集约化建设，密码服务按需获取，弹性扩展。

密码基础服务如图 5.2所示。

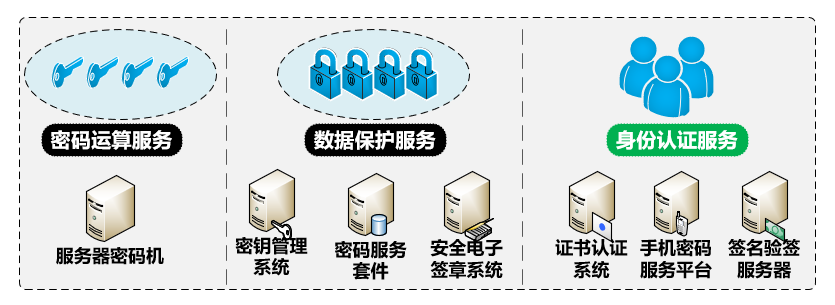


图 5.2 密码基础服务

## 5.2 物理和环境

### 5.2.1 密码应用技术方案

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》：采用基于密码技术的电子门禁系统和视频监控系统，对设备机房出入人员的身份进行鉴别，并对电子门禁系统进出记录数据和视频监控音像记录数据进行完整性保护。

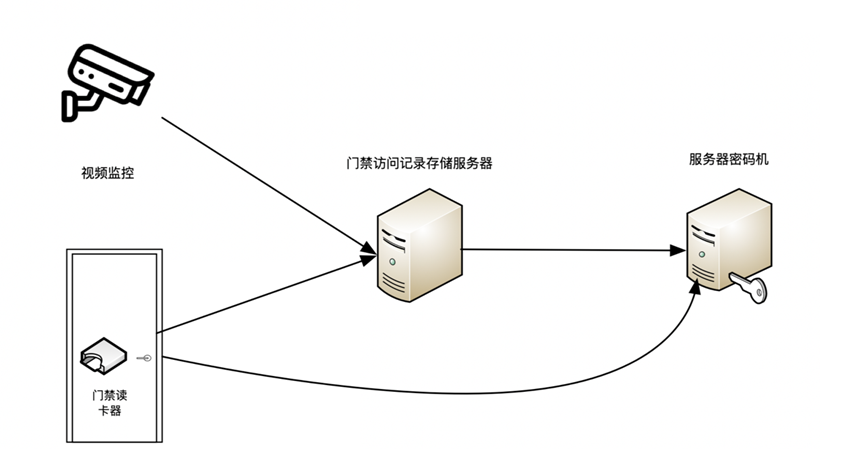


图 5.4 物理环境图

1. 身份鉴别：采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，保护物理访问控制身份鉴别信息。符合该标准的电子门禁系统使用SM4等算法进行密钥分散，实现门禁卡的一卡一密，并基于SM4等算法鉴别人员身份。
2. 电子门禁记录数据完整性：采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，电子门禁系统进出记录应严格进行完整性保护，完整的进出记录是实现安全管理、事后追责的重要基础。符合该标准的电子门禁系统使用采用MAC或数字签名等技术对记录进行完整性保护，保证进出数据记录的存储完整性。
3. 视频监控音像记录数据完整性：采用基于密码技术的的视频监控系统，视频监控系统的音像记录应严格进行完整性保护，完整的音像记录是实现安全管理、事后追责的重要基础。使用采用MAC或数字签名等技术对记录进行完整性保护，保证视频监控音像记录数据的存储完整性。

### 5.2.2 本系统密码应用技术方案-物理和环境

本项目对应方案如表5.1所示。

表 5.1 密码应用技术方案表-物理与环境

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品{{table51}} | 方案描述 | 结论 |
| [cpdx] | [zb] | [mmcp] | [fams] | [jl] |

## 5.3 网络和通信

### 5.3.1 密码应用技术方案

系统应部署符合密码相关国家、行业标准要求的密码设备或产品，保证通信实体身份的真实性；保证通信过程中数据的完整性和机密性；保证网络边界访问控制信息的完整性；保证接入的设备身份真实性。



图 5.5 网络和通信安全架构图

1. 身份鉴别：客户端对服务端响应报文中数字证书进行解析，如未发现异常则保证通信实体的真实性。
2. 通信数据完整性和通信过程中重要数据的机密性：部署已通过商用密码机构认证的密码产品或者使用合规的国密算法实现对通信数据完整性保护和通信过程中重要数据的机密性保护。
3. 网络边界访问控制信息的完整性：部署已通过商用密码机构认证的

密码产品或者调用服务器密码机实现对网络边界访问控制信息的完整性保护。

1. 安全接入认证：通过网络安全设备控制外部设备接入，只有已授权的外部设备可以接入到内部网络，保证接入设备的身份真实性。

### 5.3.2 本系统密码应用技术方案-网络和通信

表5.2 密码应用技术方案表-网络和通信

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品{{table52}} | 方案描述 | 结论 |
| [cpdx] | [zb] | [mmcp] | [fams] | [jl] |

## 5.4 设备和计算

### 5.4.1 密码应用技术方案

在设备和计算安全中主要是指管理员在对业务系统进行运维时，需要对运维管理员身份鉴别，保障网络环境中主机系统以及存储资源以及其上所承载的应用程序等重要数据的机密性和完整性。架构图如图 5.6所示：



图 5.6 设备和计算安全架构图

1. **身份鉴别：**本系统由经批准的数字证书认证系统提供数字证书，在密码基础设施区部署堡垒机和签名验签服务器。运维人员配发USBKey（USBKey中存有数字证书），运维人员在PC端使用用户名+口令+USBKey的方式保证身份的真实性；登录堡垒机时验证运维人员的签名证书，通过后选择对应的应用服务器、数据库服务器等设备，通过SSH2协议对系统中的各业务应用服务器、各数据库服务器进行运维管理。以此实现对运维人员的安全身份鉴别，防止非授权人员登录。
2. **远程管理通道安全：**采用遵循密码相关国家标准和行业标准的VPN技术，使用密码产品SSL VPN安全网关登录堡垒机，再由堡垒机使用SSH2协议登录到各设备，以搭建安全的远程管理通道。
3. **系统资源访问控制信息完整性：**在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。
4. **重要信息资源安全标记完整性：**本系统不涉及重要信息的敏感标记。
5. **日志记录完整性：**在密码基础设施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记录进行完整性保护。
6. **重要可执行程序完整性、重要可执行程序来源真实性：**在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性。

### 5.4.2 本系统密码应用技术方案-设备和计算

表5.3 密码应用技术方案表-设备与计算

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品{{table53}} | 方案描述 | 结论 |
| [cpdx] | [zb] | [mmcp] | [fams] | [jl] |

## 5.5 应用和数据

### 5.5.1 密码应用技术方案

针对在应用和数据安全层面的密码应用需求，本节提出对应的功能设计，主要包括身份鉴别、访问控制信息完整性、重要数据传输完整性、重要数据传输机密性、重要数据存储机密性、重要数据存储完整性、不可否认性，应用和数据安全架构图如图 5.7所示。



图 5.7 应用和数据安全架构图

1. **身份鉴别：**在密码基础设施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、USBKey，实现对登录用户的安全身份鉴别，保证应用系统用户身份的真实性，防止非授权人员登录。
2. **访问控制信息完整性：**在密码基础设施区部署服务器密码机，使用HMAC对系统应用的访问控制信息进行完整性保护，防止访问控制信息被篡改。
3. **重要信息资源安全标记完整性：**无（根据系统定义的安全标记进行有针对性的防护）
4. **重要数据传输机密性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2及SM3算法进行会话密钥交互，采用SM4算法对传输的数据信息进行机密性保护，防止其被非授权窃取。
5. **重要数据存储机密性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用SM4算法对数据信息存储进行机密性保护，防止其被非授权窃取。
6. **重要数据传输完整性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2算法进行会话密钥交互，采用HMAC算法对传输的数据信息进行完整性保护，防止其被非授权篡改。
7. **重要数据存储完整性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用HMAC对数据信息存储进行完整性保护，防止其被非授权篡改。
8. **不可否认性：**在基础设施区部署时间戳服务器，在系统中重要数据进行数字签名，并加盖时间戳，实现操作行为的不可否认性。

### 5.5.2 本系统密码应用技术方案-应用和数据

本项目对应方案如表5.4所示。

表5.4 密码应用技术方案表-应用和数据

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品{{table54}} | 方案描述 | 结论 |
| [cpdx] | [zb] | [mmcp] | [fams] | [jl] |

## 5.6 密钥管理

### 5.6.1 密码应用技术方案

密码服务中，对称密钥全生命周期包括密钥的生成、存储、分发等，具体如表5.5所示。

### 5.6.2 本系统密码应用技术方案-密钥管理

表5.5 对称密钥全生命周期表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 密钥 | 生成 | 存储 | 分发 | 导入  导出 | 使用 | 备份  恢复 | 归档 | 销毁 |
| 服务器密码机主密钥 | 由密钥管理员基于双人控制明文输入 | 服务器密码机内部存储 | 不涉及 | 通过专用介质导入导出，用于备份和恢复 | 服务器密码机内部使用 | 专用密钥存储介质存储分量 | 两个密钥分量单独由负责人保存 | 服务器密码机内部完成销毁 |
| 服务器密码机关键数据加解密密钥 | 服务器密码机内部生成 | 服务器密码机主密钥加密存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 服务器密码机内部完成备份和恢复 | 服务器密码机内部完成归档 | 服务器密码机内部完成销毁 |
| 服务器密码机镜像密钥 | 服务器密码机内部生成 | 服务器密码机主密钥加密存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 服务器密码机内部完成备份和恢复 | 服务器密码机内部完成归档 | 服务器密码机内部完成销毁 |
| 服务器密码机日志密钥 | 服务器密码机内部生成 | 服务器密码机主密钥加密存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 服务器密码机内部完成备份和恢复 | 服务器密码机内部完成归档 | 服务器密码机内部完成销毁 |
| 应用主密钥 | 虚拟密码机内部生成 | 虚拟密码机内部存储 | 通过租户证书、设备证书，租户和设备建立安全信道实现分发 | 通过安全信道加密导入导出 | 虚拟密码  机内部使用 | 通过租户证书、设备证书，租户和设备建立安全信道实现备份和恢复 | 租户指定在一台虚拟密码机内部归档 | 虚拟密码机内部完成销毁 |

密码服务中，非对称密钥全生命周期包括密钥的生成、存储、分发等，具体如表5.6所示：

表5.6 非对称密钥全生命周期表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 密钥 | 生成 | 存储 | 分发 | 导入  导出 | 使用 | 备份  恢复 | 归档 | 销毁 |
| 服务器密码机非对称私钥 | 服务器密码机内部生成 | 服务器密码机内部存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 不涉及 | 不涉及 | 服务器密码机内部完成销毁 |
| 服务器密码机非对称公钥 | 服务器密码机内部生成 | 以公钥形式存储 | 以数字证书形式分发 | 以公钥证书形式导入导出 | 虚拟密码机迁移时使用 | 不涉及 | 不涉及 | CA证书平台进行撤销 |
| 用户非对称私钥 | 智能密钥钥匙生成 | 智能密钥钥匙内部存储 | 不涉及 | 不涉及 | 智能密钥钥匙内部使用 | 不涉及 | 不涉及 | 智能密钥钥匙内部完成销毁 |
| 用户非对称公钥 | 智能密钥钥匙生成 | 以公钥形式存储 | 以数字证书形式分发 | 以公钥证书形式导入导出 | 业务应用使用 | 不涉及 | 不涉及 | CA证书平台进行撤销 |

## 5.7 密码应用部署

密码应用部署拓扑图如图所示：

1. 客户端在PC端配发USBKey智能密码钥匙。授权用户通过PC端登录，采用SM2数字证书认证机制，使用USBKey，与安全通道中的SSL VPN综合安全网关之间，实现双向身份认证，确保授权用户身份的真实性。



图 5.8 密码应用部署拓扑图

1. 安全通道部署SSL VPN综合安全网关，系统运维人员配发智能密码钥匙，由CA机构签发SM2数字证书，实现客户端与SSL VPN综合安全网关之间的双向身份认证。运维人员通过安装SSL VPN客户端实现安全接入。
2. 服务端包括交换机以及密码基础设施区，密码基础设施包括服务器密码机、签名验签服务器、时间戳服务器、数字证书认证系统、国密安全密码应用中间件为上层提供各种密码服务：服务器密码机可以提供加解密服务和密钥管理服务；签名验签服务器可以提供签名验签服务，实现身份验证；时间戳服务器的时间戳签发服务可以为操作节点签发时间戳，实现操作行为可追溯；证书认证系统为用户的身份鉴别提供真实性服务；国密安全密码应用中间件可以提供重要数据存储的机密性与完整性保护。

## 5.8 密码软硬件产品

### 5.8.1 密码软硬件产品清单

通过上述分析，该目标系统的密码应用改造所需的密码产品所包括硬件、软件以及相关的服务，如表5.7所示。

表5.7 密码软硬件产品清单表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号{{table57}} | 产品名称 | 部署位置 | 主要用途 | 数量  (台/套) | 备注 |
| [id] | [name] | [location] | [function] | [num] | [remark] |

### 5.8.2 密码软硬件产品介绍

* 1. **服务器密码机：**服务器密码机为整个系统提供基本的密码运算服务以及基础密钥管理服务。遵循GM/T 0030《服务器密码机技术规范》及GM/T 0059《服务器密码机检测规范》；具有商用密码产品认证证书；支持SM2、SM3、SM4等国产密码算法；支持RSA、3DES、AES、SHA等常见国际算法；支持至少三层密钥结构，支持管理密钥、用户密钥、设备密钥、密钥加密密钥、会话密钥的管理；支持对称与非对称密钥的生成及管理。采用两路独立由国家密码管理局批准使用的物理噪声源产生器芯片生成的真随机数；设备内可存储至少100个对称密钥以及32对非对称密钥，并且支持加密存储或微电保护存储；支持数据加密/解密、签名/验签、杂凑算法等类型的密码运算；分别赋予不同的操作权限，并采用数字签名技术，实现对登录用户的强身份认证；支持SDF、JEC、P11接口。
  2. **密钥管理系统：**为用户或应用系统生产、分发和管理密钥的系统及设备，持对称密钥和非对称密钥的全生命周期管理，实现密钥的生成、存储、保护、恢复、分配、注册、注销和归档，以及密钥管理的审计和跟踪、密钥管理系统的访问控制等功能；支持SM2、SM4等国产密码算法，支持RSA、DES、3DES、AES常见国际算法。遵循GM/T 0034《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 0051《密码设备管理对称密钥管理技术规范》。
  3. **国密安全密码应用中间件**：国密安全密码应用中间件用于保证数据存储的安全。支持SM1、SM2、SM3、SM4等国产密码算法；以数据加密密钥管理服务端与数据加密套件（SDK）的形式向业务应用系统提供数据加解密服务，屏蔽不同型号服务器密码机的异构性，对服务器密码机资源进行基本的资源调度。

数据加密服务：

国密安全密码应用中间件由数据加密插件和服务器密码机组成，如图 5.3所示，明文可以通过数据插件套件进行数据加密并由服务器密码机进行存储保存。

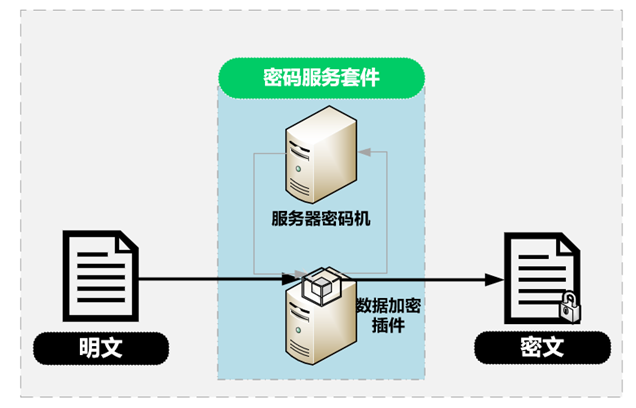


图 5.3 国密安全密码应用中间件设备图

① 数据加密插件

数据加密插件面向应用提供透明的加解密功能，插件与数据加密管理平台进行交互，获取加解密策略以及密钥，并提供数据库操作数据。通过数据加密插件，应用无需再进行任何额外的改造，即可向数据库传输密文，数据以密文的形式存储于数据库中。

数据加密支持结构化和非结构化的数据。

②签名验签服务功能

签名验签服务套件以软件形式部署于密钥管理服务平台中，签名验签服务，提供数字签名、签名验证服务，用来保障重要业务数据、权限管理数据、日志数据的完整性。签名验签服务：

签名验签服务套件对外的主要服务接口包括：

* 初始化接口：设置服务器连接、验证服务的访问权限；
* 数据签名接口：为应用系统提供数据签名接口；
* 签名验证接口：为应用系统提供签名数据的验证接口，并将签名数字证书信息解析返回给应用系统。

③完整性保护服务功能

完整性保护服务套件面向重要数据的完整性保护需求，结合数字证书、签名验签、服务器密码机提供完整性保护服务，提供基于消息鉴别码的完整性保护（HMAC-SM3）算法和基于数字签名的完整性保护（SM2-SM3）算法，支持数据完整性保护、文件完整性保护服务等。主要功能：

* 访问控制信息完整性
* 重要程序或文件完整性保护
* 日志记录完整性
  1. **安全电子签章系统：**电子签章将传统印章与电子签名技术进行结合，通过采用密码、图像处理等技术，使电子签名操作和纸质文件盖章操作具有相同的可视效果。提供电子印章管理、电子签章/验章等功能的密码应用系统。电子签章基于公钥密码技术标准体系，以电子形式对电子文档进行数字签名及签章，以确保文档来源的真实性以及文档的完整性，防止对文档未经授权的篡改，并确保签章行为的不可否认性。遵循GM/T 0031《安全电子签章密码技术规范》。支持SM2、SM3国产密码算法。具有商用密码产品认证证书
  2. **数字证书认证系统：**数字证书作用是为用户提供数字证书的申请、审核、签发、注销、更新、查询、下载等全生命周期的综合管理功能。符合国家标准GB/T 25056-2018《信息安全技术 证书认证系统密码及相关安全技术规范》；支持SM2、SM3、SM4等国产密码算法；且具有商用密码产品认证证书。
  3. **手机密码服务平台：**手机密码服务平台为移动互联网、移动设备提供密码运算支撑，用于身份认证、电子签名、数据保护等密码服务。支持基于数字证书的身份鉴别。提供用户个人敏感信息保护。提供移动端密钥生成、分发、使用、存储、销毁等全生命周期管理。提供数据签名服务接口，支持从业务系统发起签名请求，服务器与用户手机端共同完成协同签名操作流程。支持SM2、SM3、SM4商密算法以及RSA、DES、AES、SHA等国际密码算法。
  4. **签名验签服务器：**对各种类型的电子数据给出基于数字证书的数字签名服务,并向签名数据验证其签名的真实性与有效性的专用服务器。数字签名验证服务器可普遍应用在网上审批、银行、办公、支付与证券等电子政务、商务与企业信息化中向业务系统给出安全保护。

具有身份认证功能、数据签名功能、验证签名功能、系统备份功能、日志管理功能等特点。

## 5.9 安全与合规性分析

### 5.9.1 物理和环境

物理与环境安全与合规性分析结果如表5.8所示：

表5.8 安全与合规性分析表-物理和环境

|  |  |  |  |
| --- | --- | --- | --- |
| **指标点{{table58}}** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |

### 5.9.2 网络和通信

表5.9 安全与合规性分析表-网络和通信

|  |  |  |  |
| --- | --- | --- | --- |
| **指标点{{table59}}** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合，缓解/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |

### 5.9.3 设备和计算

表5.10 安全与合规性分析表-设备和计算

|  |  |  |  |
| --- | --- | --- | --- |
| **测评单元{{table510}}** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合，缓解/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |

### 5.9.4 应用和数据

表5.11 安全与合规性分析表-应用和数据

|  |  |  |  |
| --- | --- | --- | --- |
| **测评单元{{table511}}** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合，缓解/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |