**5 密码应用技术方案**

本方案根据北京市医疗系统密码应用改造要求和相关建设的整体规划，以及密码应用的合规性、正确性和有效性，保证密码应用改造的正确实施部署，来采用此套密码应用技术方案。

**5.1 密码应用技术框架（陈凯）**

基于国产密码标准体系和密码管理体系，结合北京市医疗系统平台的实际情况，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

北京市医疗系统密码应用架构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：PC端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，移动端采用手机盾实现用户在登陆系统的身份鉴别，保证了身份的真实性。

(2) 网络和通信安全密码应用，部署SSL VPN和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) 应用和数据安全密码应用，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。

(4) 设备和计算安全密码应用，主要对系统内各设备进行管理，对运维人员以及登录设备的用户进行身份鉴别，保证远程管理通道安全，提供访问控制信息完整性保护、日志记录完整性保护和重要程序完整性保护等。

2、 密码服务层

密码服务层为密码应用层提供数据加密服务、时间戳服务、签名验签服务、完整性验证服务、数据库安全服务和身份认证服务等密码应用所需基础服务。

3、 密码设施层

[这里从数据库填入场景描述]

**5.2 方案整体设计（陈凯）**

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。

**5.2.1 密码基础服务层**

密码基础服务层整合服务器密码机、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。

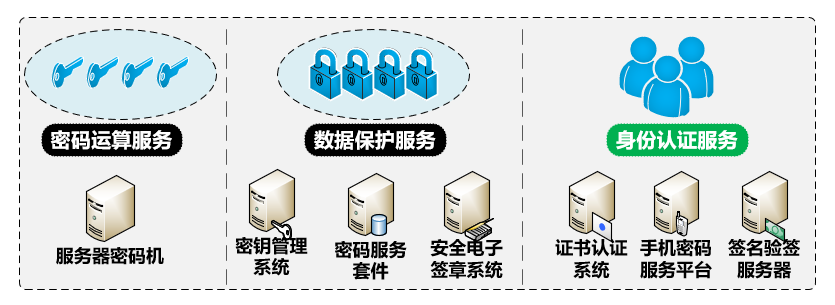


图 5.2 密码基础服务

密码基础服务层包括如下：

* 1. **服务器密码机：**密码运算：支持数据加密/解密、数字签名/验签、消息鉴别码的产生/验证、数字信封、密钥协商等类型的密码运算，并且支持多任务并发访问；密钥管理：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；密钥安全存储：支持100对SM2非对称密钥、100对RSA非对称密钥、200个对称密钥，并使用管理密钥加密存储；随机数产生：采用双路国家密码管理局批准的物理噪声源随机数芯片；访问控制：支持管理员、操作员角色，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。
  2. **密钥管理系统：**密钥管理：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、更新、查询、删除、分发、恢复与备份、销毁等密钥全生命周期管理；支持物理噪声源随机数：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； 密钥的安全存储：设备内可存储至少10000个对称密钥以及10000对非对称密钥，并且支持加密存储或微电保护存储；身份鉴别：对管理人员、操作人员、维护人员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；系统审计：对各密钥管理操作及其内容进行审计，确保审计信息不可被修改和删除。
  3. **国密安全密码应用中间件**：统一密码服务接口：提供数据加解密、签名验签、数字信封、摘要计算、随机数等接口服务能力；密码设备管理：支持对接不同厂商的各类异构密码设备（包括服务器密码机、签名验签服务器、时间戳服务器、云密码机等），并将密码设备进行会话级别（Session）的细粒度管理与调度；证书与密钥管理：内置基础证书与密钥管理能力，可对接具有商密产品认证资质的CA、密钥管理系统，以提供证书与密钥的全生命周期管理能力；密码设备模拟器：内置密码机软件模拟器，可方便开发人员进行应用无密码设备开发集成与调试，可与硬件密码设备无缝切换；应用管理：可以支持多应用系统接入，并通过数字证书对应用系统进行访问控制。
  4. **安全电子签章系统：**提供电子印章管理、电子签章/验章等功能的密码应用系统；签章可视化：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；不可否认性保护：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书。
  5. **证书认证系统：**用户注册管理：负责用户的证书申请、身份审核和证书下载；证书状态查询：提供CRL查询和在线证书状态查询，支持OCSP协议，查询速度高；负责生成、签发数字证书和证书撤销列表，支持用户证书注销列表（CRL）和CA证书撤销列表（ARL），支持增量或全量CRL注销列表；证书管理：支持证书全生命周期的管理，包括证书管理证书的申请、审核、生成、签发、存储、发布、注销、归档等；安全管理：提供事件级审计功能、访问控制、入侵检测、漏洞扫描等网络安全功能；支持CA多根：支持设置多个根CA，例如SM2根、RSA根，根据需求可以根据行业设置根CA；支持多级CA：根据业务需要可以设置多级CA，灵活配置；多算法支持：支持签发SM2证书、RSA1024证书、RSA2048证书，可扩展支持RSA3072证书、RSA4096证书； 系统备份及恢复：支持系统信息的备份和恢复功能，保证了安全应用系统的安全性和可靠性。
  6. **协同签名系统：**SM2密钥对生成：SM2私钥使用密钥分割技术生成，从生成到运算整个过程中不出现完整的SM2私钥，保障了私钥的安全；证书、设备管理：对终端移动终端进行管理，包括设备的查看、挂起、停用；支持对接第三方CA系统：导入CA获取的证书和私钥数据，并解析传入的证书相关信息；密码运算：支持数据签名/验签，数字信封封装/解析等类型的密码运算；支持管理员、审计员、操作员角色：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法。
  7. **签名验签服务器：**对证书管理和验证功能：支持与CA连接，提供证书管理功能，支持CA、CRL、OCSP等多种方式证书有效性验证；数字签名验签：支持基于SM2、RSA算法数字证书的数字签名、验证签名等服务，以保证业务信息的真实性、完整性和不可否认，提供对PKCS#1、PKCS#7 Attach、PKCS#7 Detach、XML等电子数据的数字签名/验签功能，提供对消息、文件等多种格式的运算方式；数字信封功能：支持基于SM2、RSA密码算法的数字信封功能，支持PKCS#7标准各种格式的数字信封封装和解封；由签名验签服务器产生应用实体的签名密钥对和证书请求，支持通过管理界面导入应用实体的签名证书、加密证书和加密密钥对；密钥的安全存储：设备内可存储至少200个对称密钥以及100对非对称密钥，并且支持加密存储或微电保护存储；访问控制功能：具备完善的身份鉴别机制，通过智能密码钥匙与口令相结合的方式实现管理员身份的鉴别；支持连接白名单：通过连接白名单的支持，实现了签名验签服务器对应用服务器的授权认证点。

**5.2.2 密码协议**

本方案中所有密码子系统中涉及的密码设备和密码协议，均遵循国家密码管理局发布的密码行业标准和规范，如下所示：

* GM/T 0002-2012《SM4 分组密码算法》
* GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》
* GM/T 0004-2012《SM3 密码杂凑算法》
* GM/T 0006-2012《密码应用标识规范》
* GM/T 0009-2012《SM2 密码算法使用规范》
* GM/T 0015-2012《基于SM2 密码算法的数字证书格式规范》
* GM/T 0017-2012《智能密码钥匙密码应用接口规范》
* GM/T 0018-2012《密码设备应用接口规范》
* GM/T 0019-2012《通用密码服务接口规范》
* 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》
* GM/T 0029-2014《签名验签服务器技术规范》
* GM/T 0031-2014《安全电子签章密码技术规范》
* GM/T 0030-2014《服务器密码机技术规范》
* 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》
* GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

**5.2.3 密钥管理**

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 5.1所示。

表 5.1 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 |
| 物理密码机主密钥 | 由密钥管理员基于双人控制明文输入 | 物理密码机内部存储 | 不涉及 | 通过专用介质导入导出，用于备份和恢复 | 物理密码机内部使用 | 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 | 物理密码机内部完成销毁 |
| 物理密码机关键数据加解密密钥 | 物理密码机内部生成 | 物理密码机主密钥加密存储 | 不涉及 | 不涉及 | 物理密码机内部使用 | 物理密码机内部完成备份和恢复 | 物理密码机内部完成归档 | 物理密码机内部完成销毁 |
| 物理密码机镜像密钥 | 物理密码机内部生成 | 物理密码机主密钥加密存储 | 不涉及 | 不涉及 | 物理密码机内部使用 | 物理密码机内部完成备份和恢复 | 物理密码机内部完成归档 | 物理密码机内部完成销毁 |
| 物理密码机日志密钥 | 物理密码机内部生成 | 物理密码机主密钥加密存储 | 不涉及 | 不涉及 | 物理密码机内部使用 | 物理密码机内部完成备份和恢复 | 物理密码机内部完成归档 | 物理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 5.2所示。

表 5.2 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 |
| 物理密码机非对称私钥 | 密码机内部生成 | 物理密码机内部存储 | 不涉及 | 不涉及 | 物理密码机内部使用 | 不涉及 | 不涉及 | 物理密码机内部完成销毁 |
| 物理密码机非对称公钥 | 物理密码机内部生成 | 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 |
| 系统管理员非对称私钥 | 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 |
| 系统管理员非对称公钥 | 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 |
| 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 |

**5.3 方案详细设计**

北京市医疗系统密码应用建设是从物理和环境安全、网络和通信安全、设备和计算安全和应用和数据安全五个方面进行建设。

**5.3.1 物理和环境安全（董涵宁）**

1. [身份鉴别]
2. [视频完整性]

**5.3.2 网络和通信安全（贾红豆、陈凯、曹冉筝）**

网络与接入安全密码应用，在应用系统接入边界部署安全网关，配合远程终端在应用系统，对访问应用业务系统的用户进行身份鉴别和权限控制，对传输的数据进行机密性和完整性保护。

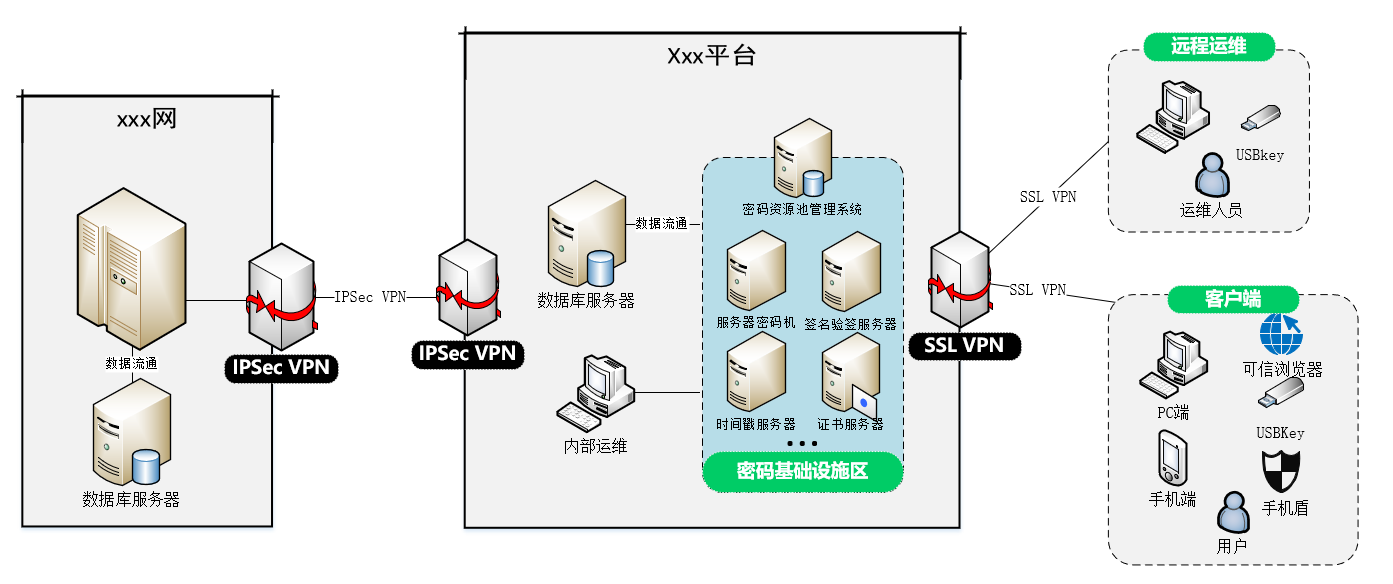


图 5.5 网络和通信安全架构图

[这里填入通道1]

1. 身份鉴别
2. 网络完整性

[这里填入通道2]

1. 身份鉴别
2. 网络完整性

**5.3.3 设备和计算安全（卢焱、王晨、曹冉筝）**

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]
2. [设备完整性]

**5.3.4 应用和数据安全（冯天浩、张海政、刘双平）**



图 5.7 应用和数据安全架构图

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。

1. [身份鉴别]
2. [数据完整性]

**5.4 密码应用部署（贾红豆）**

密码应用部署拓扑图如所示：

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、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。

**5.5 密码软硬件产品清单（刘双平）**

通过上述分析，北京市医疗系统的实现所需的密码产品所包括硬件、软件以及相关的服务如表 5.11所示。

表 5.11 系统拟部署的密码产品清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 功能说明 | 形态 | 数量  (台/套) | 备注 |
| 1 | 服务器密码机 | 功能 | 硬件 | 2 | 备注 |
| 2 | 时间戳服务器 | 功能 | 硬件 | 2 | 备注 |
| 3 | 签名验签服务器 | 功能 | 硬件 | 2 | 备注 |

**5.6 安全与合规性分析**

北京市医疗系统的安全与合规性分析如表 5.12所示。

表 5.12 安全与合规性分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | 采用安全门禁系统实现进入人员身份鉴别 | 符合 | 无 |
| 电子门禁记录数据完整性 | 部署服务器密码机，使用HMAC对电子门禁记录数据和视频记录数据进行完整性保护 |
| 视频监控记录数据完整性 |
| 密码服务 | 密码应用技术服务 |
| 密码产品 | 服务器密码机 |
| 网络和通信安全 | 身份鉴别 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现通信实体身份鉴别，保证通信实体身份的真实性 | 符合 | 无 |
| 通信数据完整性 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现通信数据的机密性和完整性保护 | 符合 | 无 |
| 通信过程中重要数据的机密性 |
| 网络边界访问控制信息的完整性 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现网络边界访问控制信息的完整性保护 | 符合 | 无 |
| 安全接入认证 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现安全接入 | 符合 | 无 |
| 密码服务 | 数字证书认证服务 | 符合 | 无 |
| 密码产品 | SSL VPN、IPSec VPN、智能密码钥匙 | 符合 | 无 |
| 设备和计算安全 | 身份鉴别 | 在本系统运维人员PC端，配发USBKey，在密码基础设施区部署签名验签服务器，用户登录应用时验证人员数字签名，实现对登录应用用户的安全身份鉴别，防止非授权人员登录 | 符合 | 无 |
| 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安全网关搭建安全的远程管理通道 | 符合 | 无 |
| 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 | 符合 | 无 |
| 重要信息资源安全标记完整性 | - | 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 | 符合 | 无 |
| 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 | 符合 | 无 |
| 密码服务 | 数字证书认证服务、密钥管理服务 | 符合 | 无 |
| 密码产品 | SSL VPN安全网关、USBKey、服务器密码机、签名验签服务器 | 符合 | 无 |
| 应用和数据安全 | 身份鉴别 | 在本系统应用用户人员PC 端采用USBKey登录，在基础设施区部署签名验签服务器，用户登录应用时验证人员数字签名，实现对登录应用用户的安全身份鉴别，防止非授权人员登录 | 符合 | 无 |
| 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 | 符合 | 无 |
| 重要信息资源安全标记完整性 | - | 不适用 | 本系统不涉及重要信息资源的敏感  标记 |
| 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 | 符合 | 无 |
| 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 | 符合 | 无 |
| 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 | 符合 | 无 |
| 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 | 符合 | 无 |
| 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 | 符合 | 无 |
| 密码服务 | 密码应用技术服务 | 符合 | 无 |
| 密码产品 | 服务器密码机、国密安全密码应用中间件、签名验签服务器、时间戳服务器、可信浏览器、USBKey | 符合 | 无 |