**5 密码应用设计**

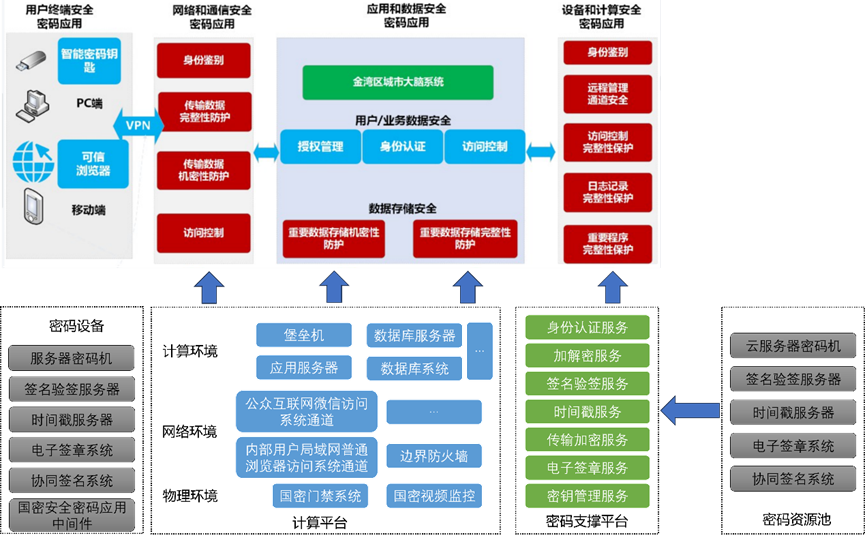
**5.1密码应用技术框架**

{{sysname}}密码应用技术框架如下图2所示。

下图二选一



**图2密码应用技术框架（非云）**

****

**图2密码应用技术框架（云）**

密码产品主要实现说明如下：

{{sysname}}的密码应用架构分为密码资源池、密码支撑平台、计算平台、密码应用层，密码应用层包括用户终端安全密码应用、网络接入网络和通信安全密码应用、业务安全密码应用和数据安全密码应用、平台管理安全密码应用设备和计算安全密码应用四部分。

**1、密码支撑平台**

密码支撑平台为云密码服务平台提供基础的密码运算资源。为业务应用提供身份认证、数据加密、操作不可否认、数字证书管理等密码应用所需基础服务。当单位用户通过PC端连接SSL VPN，浏览器访问系统时需通过智能密码钥匙USBKey进行身份验证，以避免其用户名/口令遭到截获、假冒或重用，导致业务应用系统被入侵，将造成用户身份信息泄露、业务系统其他信息泄露或伪造业务指令风险。数据在传输时需通过服务器密码机、国密安全密码应用中间件、进行加密传输，保证用户信息不被窃取偷听篡改等，以保障传输过程的机密性与完整性。

**2、密码资源池**

基于各密码产品构建的密码基础服务层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。

密码资源池整合服务器密码机、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，对外统一提供密码服务、集约化建设，密码服务可弹性扩展。

以下密码产品均满足GB/T 37092-2018《信息安全技术 密码模块安全要求》或GM/T 0028-2014《密码模块安全技术要求》密码模块二级及以上。

1)服务器密码机：遵循GM/T 0030-2014《服务器密码机技术规范》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GM/T 0028-2014《密码模块安全技术要求》和GM/T 0059-2018《服务器密码机检测规范》；支持SM1、SM2、SM3、SM4等国产密码算法；支持RSA、AES、3DES、MD5、SHA等国际算法；具有商用密码产品认证证书；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；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；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；采用双路国家密码管理局批准的物理噪声源随机数芯片；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；同时支持SDF、JCE、PKCS11接口，具有良好的通用性。

2)签名验签服务器：遵循GM/T 0028-2014《密码模块安全技术要求》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》、GM/T 0029-2014《签名验签服务器技术规范》和GM/T 0060-2018《签名验签服务器检测规范》；支持SM1、SM2、SM3、SM4等国产密码算法；支持RSA,3DES,AES,SHA等常见国际算法；具有商用密码产品认证证书；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；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；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；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；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；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。

3)国密安全密码应用中间件：信息系统与密码应用系统及密码设备之间的重要中间件；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；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；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；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；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；为应用开发提供支持包括C/C++、Java、Go、PHP、.Net、Shell等语言的密码服务接口调用。

4)国密数字证书：由受信任的数字证书颁发机构（CA），在验证身份信息（包括域名、主机名、服务器名、申请者身份、机构身份等）后颁发。支持SM2等国产密码算法。

5)智能密码钥匙：遵循GM/T 0027-2014《智能密码钥匙技术规范》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》、GM/T 0028-2014《密码模块安全技术要求》和GM/T 0048-2016《智能密码钥匙密码检测规范》；支持国产密码算法；实现密码运算、密钥管理功能的终端密码设备，提供USB接口；支持数据加解密、消息鉴别码等功能；至少支持三种密钥，包括设备认证密钥、用户密钥、会话密钥，具有对用户密钥和会话密钥的产生、存储、使用、导入、导出、协商等功能；能够至少保存2对RSA密钥对、2对SM2密钥对和2个对称密钥（设备认证密钥和会话密钥）；随机数由多路硬件噪声源产生；证书管理：支持数字证书的读写、枚举、删除，可作为数字证书的安全载体。

6)SSL VPN安全网关：遵循GM/T 0025-2014《SSL VPN 网关产品规范》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GM/T 0028-2014《密码模块安全技术要求》；支持SM2、SM3、SM4国产密码算法；具有商用密码产品认证证书；基于 SSL/TLS 协议，在通信网络中构建安全通道；随机数由多路硬件噪声源产生；提供密钥交换功能，通过协商产生工作密钥；提供符合国际和国密标准SSL的VPN通道防护，有安全报文传输功能，支持抗重放攻击，保证数据的安全传输；通过数字证书的方式对实体鉴别，保证鉴别信息的完整性和有效性；具有细粒度的访问控制功能，基于用户或用户组对资源进行有效控制，并能根据访问时间进行控制；根据时间周期或报文流量进行工作密钥更新；能够对用户对系统的访问进行详细记录，记录信息包括：时间、用户IP、用户证书信息、访问资源、上传流量、下载流量、访问结果、错误原因；用户访问HTTP应用时，系统在完成相应的身份鉴别后，把验证结果、用户基本信息插入到HTTP请求中传送给后台的应用系统，应用系统通过标准的HTTP操作即可获取信息，并基于该信息作相应的访问控制以及进行相应的业务审计；客户端在连接服务端时，根据服务端下发的客户端安全策略检查用户操作系统的安全性。

7)可信浏览器：支持SM2、SM3、SM4国密算法；具有商用密码产品认证证书；支持国密SSL双向协议；支持最新TLCP标准；支持沙箱机制、浏览器内核隔离域、跨域安全隔离、站点安全隔离防护、可信证书校验等功能；支持本地用户数据加密，防止用户保存的密码被明文导出；支持国密网站、国密应用自动识别及国密标识展现，针对国密网站优先通过国密协议访问，单向SSL连接性能不低于200次/秒；可信浏览器管控中心支持证书的统一导入和下发，证书下发支持RSA国际证书和国内商密证书。

8)协同签名系统：支持SM2、SM3、SM4等国产密码算法；具有商用密码产品认证证书； 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；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；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。

**5.2计算平台密码应用方案**

**5.2.1物理和环境安全**

（云平台机房已密改通过密评描述）XXX{云平台名称}已通过密码应用安全性评估第三级评估且安全等级不低于云上应用，其密评报告中对XXX{云平台名称}的支撑能力进行了评估，XX机房作为被完全评估的支撑能力，能同时支撑云平台和云应用在物理和环境安全层面的密码应用安全，采用云平台密评对物理和环境安全的结论。

{{?solution}}

{{?wlhhjFAList}}

{{index}}、{{name}}

{{\*description}}

{{/wlhhjFAList}}

{{/solution}}

**5.2.2网络和环境安全**

1. **员工用户PC浏览器与业务系统之间的通信信道**

1)身份鉴别：部署已通过商用密码机构认证的SSL VPN安全网关，PC端部署VPN客户端，SSL VPN安全网关中配置由合规CA颁发的国密数字证书，基于SM2数字证书实现对服务端的证书进行身份鉴别，保证通信过程中通信实体身份鉴别的真实性。

2)通信数据完整性：部署符合已通过商用密码机构认证的SSL VPN安全网关，已通过商用密码机构认证，基于HMAC-SM3算法可保证通信过程中数据的完整性。

3)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SSL VPN安全网关，基于SM4算法可保证通信过程中重要数据的机密性。

4)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SSL VPN安全网关，SSL VPN安全网关具有细粒度的访问控制功能，基于用户或用户组对资源进行有效控制，并能根据访问时间进行控制，基于HMAC-SM3算法保证通信过程中访问控制信息的完整性。防火墙和边界路由未使用密码技术保护网络边界访问控制信息的完整性。

5)安全接入认证：该指标要求属性为“可”，不纳入本次测评范围。

**2、系统业务服务区和数据灾备区之间的专线通信信道**

1)身份鉴别：在系统在网络接入区和数据灾备区部署符合GB/T 36968-2018《信息安全技术 IPSec VPN技术规范》、GB/T 37092-2018 《信息安全技术密码模块安全要求》二级模块要求的IPSec VPN，使用IPsec VPN建立安全传输通信信道。建立IPsec协议安全传输通道时通过双向传递数字证书，在主模式下基于SM2算法实现通信实体的身份鉴别，数字证书由证书认证系统签发。

2)通信数据完整性：业务服务器IPsec VPN和数据灾备区IPsec VPN建立安全关联SA后，协商安全参数交换密钥，使用AH协议保证数据传输的完整性，AH协议使用SM3算法计算消息摘要，将摘要与数据一起加密。接收方使用相同的散列函数对收到的数据进行处理，并与收到的摘要进行比较，以验证数据的完整性。

3)通信过程中重要数据的机密性：业务服务器IPsec VPN和数据灾备区IPsec VPN建立安全关联SA后，协商安全参数交换密钥，使用ESP协议保证数据传输的完整性，协议使用SM4对称加密算法加密数据。接收方使用相同的密钥和加密算法对收到的数据进行解密，以恢复原始数据。

4)网络边界访问控制信息完整性：该条信道的网络边界访问控制信息主要为IPsec VPN的访问控制列表信息，VPN已符合GB/T 37092-2018 《信息安全技术密码模块安全要求》二级模块要求，可通过自身较高的安全防护能力，基于SM2算法数字签名技术实现访问控制列表的完整性校验。

5)安全接入认证：该指标要求属性为“可”，不纳入本次测评范围。

**3、公众用户移动端APP与业务系统之间的通信信道**

1)身份鉴别：在服务端部署非国密站点证书（不包含高风险算法）实现通信实体身份鉴别，数字证书由具备资质的机构签发。

2)通信数据完整性：通过移动端APP和服务端构建非国密HTTPS通道，基于无高风险密码算法的HMAC技术实现通信数据完整性保护。

3)通信过程中重要数据的机密性：通过移动端APP和服务端构建非国密HTTPS通道，使用基于无高风险的密码算法对通信数据进行加密，实现通信过程中重要数据的机密性的保护。

4)网络边界访问控制信息的完整性：防火墙和边界路由未使用密码技术保护网络边界访问控制信息的完整性。

5)安全接入认证：本系统不涉及。

4、系统与系统、机房与机房之间的通信信道：通过纯物理裸光纤进行数据传输，作为不适用项处理。

**5.2.3设备和计算安全**

1、堡垒机

1)身份鉴别：在密码基础设施区部署堡垒机，给运维人员配发已通过商用密码产品检测认证的USBKey（内存有合规的国密数字证书），首先通过SSL VPN安全网关接入网络，再登录堡垒机进行设备的运维管理，SSL VPN安全网关的身份鉴别措施可有效缓解运维人员登录堡垒机的身份鉴别风险，因此不对堡垒机进行改造。（不改造堡垒机）

{使用支持国密算法的堡垒机，堡垒机通过密码产品认证。设备登录人员使用ukey登录堡垒机，ukey内置SM2数字证书，采用基于SM2算法的数字签名机制保证堡垒机登录人员身份的真实性。（国密堡垒机）}

{管理区部署堡垒机，运维人员PC端配发USBKey（内有国密数字证书），配合签名验签服务器的签名验签服务对运维人员进行身份鉴别。（改造堡垒机）}

2)远程管理通道安全：在政务外网出口区部署已通过商用密码产品认证的SSL VPN安全网关登录堡垒机，先通过国密HTTPS协议建立运维人员到内网的安全传输通道，再使用堡垒机自签的证书，通过非国密HTTPS协议建立运维人员到堡垒机的安全传输通道。（不改造堡垒机）

{堡垒机的远程管理通道，基于不包含高风险密码算法的非国密HTTPS协议保证远程管理通道安全。}

3)系统资源访问控制信息完整性：由于堡垒机不支持系统资源访问控制信息调出，本次项目暂不考虑对堡垒机系统资源访问控制信息完整性进行密码应用建设。

4)重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。

5)日志记录完整性：由于堡垒机不支持日志记录调出，本次项目暂不考虑对堡垒机的日志记录完整性进行密码应用建设。

6)重要可执行程序完整性、重要可执行程序来源真实性：于堡垒机技术上无法实现，本次项目暂不考虑对堡垒机重要可执行程序完整性和重要可执行程序来源真实性进行密码应用建设。

2、通用设备

1. 身份鉴别：使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机利用用户名+口令对通用设备进行运维过程中的身份鉴别。（不改造堡垒机）

{本项目将不考虑对通用设备进行改造，相关设备虽使用账号口令登录，但均使用堡垒机进行统一管理，能够降低相关设备身份鉴别所面临的安全风险。（改造堡垒机/国密堡垒机）}

1. 远程管理通道安全：使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机，由堡垒机使用无高风险的SSH2协议对通用设备进行运维的过程中远程管理通道安全的保护。（不改造堡垒机）

{堡垒机到通用服务器、数据库管理系统的链路，使用非高风险密码算法，基于SSH2.0或者RDP协议（Linux系统：SSH2.0；Windows系统：RDP），采用公私钥体系的RSA2048算法的数字证书、采用SHA256和AES算法保证远程管理通道安全。}

1. 系统资源访问控制信息完整性：因全球信息化历史原因，各通用设备系统内核技术上无法实现基于密码技术的访问控制，本次项目暂不考虑对此类通用设备系统资源访问控制信息完整性进行密码应用建设。
2. 重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。
3. 日志记录完整性：部署已通过商用密码产品检测认证的服务器密码机，使用HMAC-SM3技术实现对通用设备的日志记录信息进行完整性保护。

{由于各类服务器之间协调难度大，密码改造成本高，同时设备部署在机房，机房具有完善的管理机制；且设备只由专人管理，未授权人员无权使用，通过严格的安全措施，保障了设备的安全运行。因此本项目暂不采用密码技术对上述设备的日志记录进行完整性保护。（不改造）}

1. 重要可执行程序完整性、重要可执行程序来源真实性：通用设备暂无机制保护其重要可执行程序。

**3、密码设备**

1)身份鉴别：运维人员通过堡垒机使用USBKey（内有数字证书认证系统签发的国密SM2证书）登录到各密码设备，配合已通过商用密码产品检测认证的签名验签服务器，在登录时验证运维人员USBKey中的国密数字证书实现运维人员登录密码设备的身份鉴别。

2)远程管理通道安全：由堡垒机使用无高风险的HTTPS协议对各密码设备进行运维管理，从而搭建安全的远程管理通道，实现运维人员登录堡垒机，从而对密码设备进行运维的过程中的远程管理通道安全的保护。

{密码设备均是本地运维，不涉及远程管理通道，该指标作为不适用项处理。}

{密码设备的远程管理通道，采用公私钥体系的RSA2048算法的数字证书、采用SHA256和AES算法保证远程管理通道安全，且通过堡垒机进行统一运维管理。}

3)系统资源访问控制信息完整性：密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备访问控制信息的保护。

4)重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。

5)日志记录完整性：密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备日志记录的保护。

6)重要可执行程序完整性、重要可执行程序来源真实性：密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对重要可执行程序完整性、真实性的保护。

**5.3密码支撑平台方案**

（密码应用中间件系统方式）

密码支撑平台为承载在计算平台上的各类业务应用提供密码功能服务，选择采用经认证合格的密码应用中间件系统，系统底层部署云服务器密码机、服务器密码机、签名验签服务器、时间戳服务器密码设备。

**5.3.1 密码服务机构的确定、接入方式和服务策略**

采用{{jg}}机构颁发的数字证书。

网络层的国际或国密算法的站点证书，采用外部生成证书索引，后导入网关内生成站点证书的方式。

应用层的个人数字证书采用智能密码钥匙进行承载，线下签发制作的方式。

设备层的设备数字证书采用SSL VPN/时间戳服务器进行承载，线下签发制作的方式。

**5.3.2 支持的密码体制和密码算法**

（密码应用中间件系统方式）

密码应用中间件系统覆盖的密码算法包括但不限于：

1. **对称算法：SM4、AES等**

密码应用中间件系统支持对称算法，包括SM4、AES等。其中，SM4为国密算法。

1. **非对称算法：RSA、SM2等**

密码应用中间件系统支持非对称算法，包括RSA、SM2等，其中，SM2为国密算法。

1. **摘要算法：SM3、SHA256**

消息摘要算法主要应用在“数字签名”领域，消息摘要算法包含MD（消息摘要算法）、SHA（安全散列算法）和MAC（消息认证码算法）共3大系列，常用于验证数据的完整性，是数字签名算法的核心算法。

密码应用中间件系统支持算法清单如下表所示：

|  |  |  |
| --- | --- | --- |
| 算法类型 | 算法名称 | 工作模式 |
| 对称算法 | SM4 | ECB、CBC、GCM |
| AES128/AES256 | GCM |
| 非对称算法 | RSA2048/RSA4096 | 加密、解密、签名、验证 |
| SM2 | 加密、解密、签名、验证 |
| 摘要算法 | SM3、SHA256、HAMC-SM3 | / |

**5.3.3 接口和功能遵循的标准**

（密码应用中间件系统方式）

密码应用中间件系统提供接口和功能遵循的标准包括但不限于：

|  |  |  |
| --- | --- | --- |
| 接口功能 | 功能描述 | 遵循的标准 |
| 密钥管理服务 | 提供对称密钥和非对称密钥基于多层密钥保护体系的安全存储。提供密钥生成、存储、分发、使用、更新、备份恢复、销毁全生命周期管理。 | GM/T 0028《密码模块安全技术要求》 |
| 签名验签服务 | 提供PKCS1格式的数字签名和数字签名验证功能 | GB/T 38629 信息安全技术 签名验签服务器技术规范；  GB/T 35276 信息安全技术SM2密码算法使用规范；  GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范；  GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范； |
| 加解密服务 | 支持对称加解密、非对称加解密、数字信封等密码技术。 | GB/T 17964 信息安全技术 分组密码算法的工作模式；  GB/T 33560 信息安全技术 密码应用标识规范； |
| 时间戳服务 | 基于国家标准时间源，支持时间戳生成、解析、验证等功能。 | GM/T 0033 时间戳接口规范； |
| 完整性保护服务 | 支持国密SM3杂凑算法采用HMAC方式进行数据存储完整性保护，支持符合PKI标准的PKCS1签名进行数据传输完整性保护。 | GB/T 15852(所有部分)信息技术 安全技术 消息鉴别码； |

**5.3.4 提供的密码支撑方式**

采购符合规定的密码设备/租用密码设备/租用密码服务/建设密码资源

**5.3.5 提供的密码功能及接口**

密码功能及接口如下：

|  |  |
| --- | --- |
| 序号 | 提供的密码功能及接口 |
| 1 | 密钥管理 |
| 2 | 加密解密 |
| 3 | 消息鉴别码产生和验证 |
| 4 | 随机数产生 |
| 5 | 数据签名/验证 |
| 6 | 计算MAC/验证MAC |
| 7 | 签名验签 |
| 8 | 时间戳生成/验证/解析 |

**5.3.6 部署的位置和方式**

（密码应用中间件系统方式）

密码服务管理平台部署在XXX云平台的XX区内，以软件形式集中统一部署在虚拟机上，使用和管理由XX局负责，XX局以租户的形式租用密码服务。

**5.3.7 接入计算平台的方式**

非独立部署，使用XXX云平台/XX网的计算资源和网络资源。

**5.3.8 密钥管理方式，按责任主体的规划要求确定**

（密码应用中间件方式）

密钥由密码设备生成和管理，由密码服务管理平台进行统一管控（由使用密码应用中间件系统的租户进行管理），XXX局委托管理密钥（由租户自行管理密钥）

**5.3.9 支撑平台的自身安全性，包括密钥安全、访问安全、管理安全和租户间的隔离安全等**

（密码应用中间件方式）

密码应用中间件系统自身的安全性体现在：

系统只允许使用智能密码钥匙登录，不允许使用账号口令的方式，平台内的访问控制信息使用安全策略和使用完整性机制进行保护。平台内部密钥由底层密码设备硬件生成，以三层密钥管理机制加密存储在数据库中。系统自身具备三权分立和多级管理员方式，各个管理员只允许访问自身权限内的功能和数据。租户间的密钥相互独立，租户只允许访问自身密钥，基于数字证书鉴别进行访问管控，实现租户间的隔离安全。

**5.4业务应用密码应用方案**

1. 身份鉴别：业务系统对接中间件做集成改造，系统管理员和内部用户PC端使用Ukey登录，Ukey内置SM2数字证书，登录时，服务器产生随机数，客户端使用数字证书对服务器端产生的随机数进行签名，服务器端通过密码应用服务系统的接口服务调用签名验签服务器进行验签，基于SM2数字签名技术保证登录用户身份的真实性。

采用USBKey登录的流程图如下图所示：

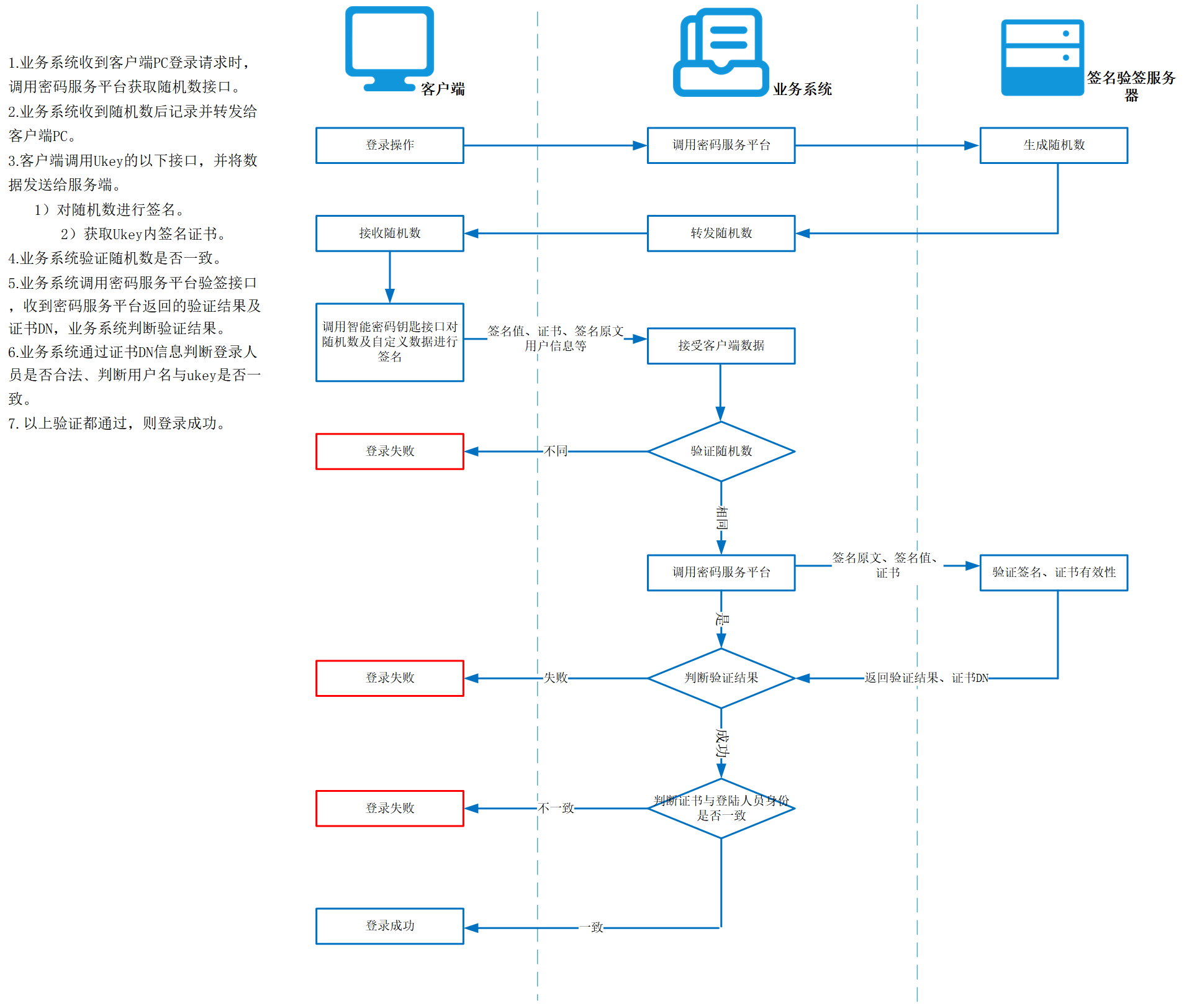


图 2 身份鉴别流程

1.业务系统收到客户端PC登录请求时，调用密码服务平台获取随机数接口。

2.业务系统收到随机数后记录并转发给客户端PC。

3.客户端调用Ukey的以下接口，并将数据发送给服务端。

1）对随机数进行签名。  2）获取Ukey内签名证书。

4.业务系统验证随机数是否一致。

5.业务系统调用密码服务平台验签接口，收到密码服务平台返回的验证结果及证书DN，业务系统判断验证结果。

6.业务系统通过证书DN信息判断登录人员是否合法、判断用户名与ukey是否一致。

7.以上验证都通过，则登录成功。

{XX{用户类型，如普通用户}{通过XX系统（第三方系统名称，如省统一身份认证平台）登录，使用{账号口令+手机短信验证码/扫码/刷脸}方式登录业务系统，降低了应用和数据安全层面用户身份鉴别的风险。（缓解措施）}

1. 访问控制信息完整性：部署具有商密资质的服务器密码机，业务系统通过中间件调用服务器密码机，使用HMAC-SM3算法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。
2. 重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。
3. 重要数据存储机密性：在密码基础设施区部署具有商密资质的服务器密码机和国密安全密码应用中间件，国密安全密码应用中间件采用插件模式，业务系统通过国密安全密码应用中间件调用服务器密码机，使用SM4算法对业务系统中的重要数据的存储进行机密性保护，防止其被非授权窃取。

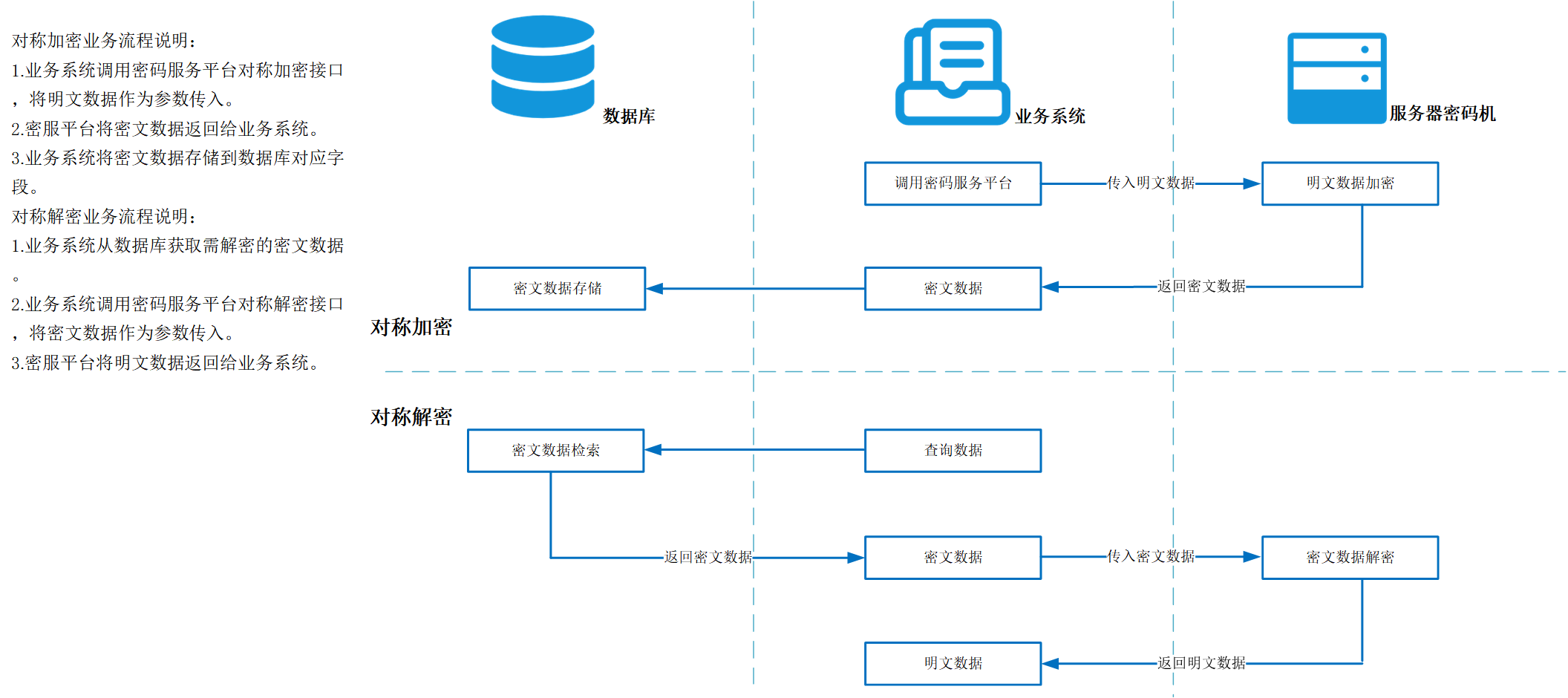


图 3 加密存储流程

对称加密业务流程说明：

1.业务系统调用密码服务平台对称加密接口，将明文数据作为参数传入。

2.密服平台将密文数据返回给业务系统。

3.业务系统将密文数据存储到数据库对应字段。

对称解密业务流程说明：

1.业务系统从数据库获取需解密的密文数据。

2.业务系统调用密码服务平台对称解密接口，将密文数据作为参数传入。

3.密服平台将明文数据返回给业务系统。

1. 重要数据存储完整性：在密码基础设施区部署具有商密资质的服务器密码机和国密安全密码应用中间件，国密安全密码应用中间件采用插件模式，业务系统通过国密安全密码应用中间件调用服务器密码机，使用HMAC-SM3对业务系统中的重要数据进行存储完整性保护，定期校验数据存储完整性，防止其被非授权篡改。

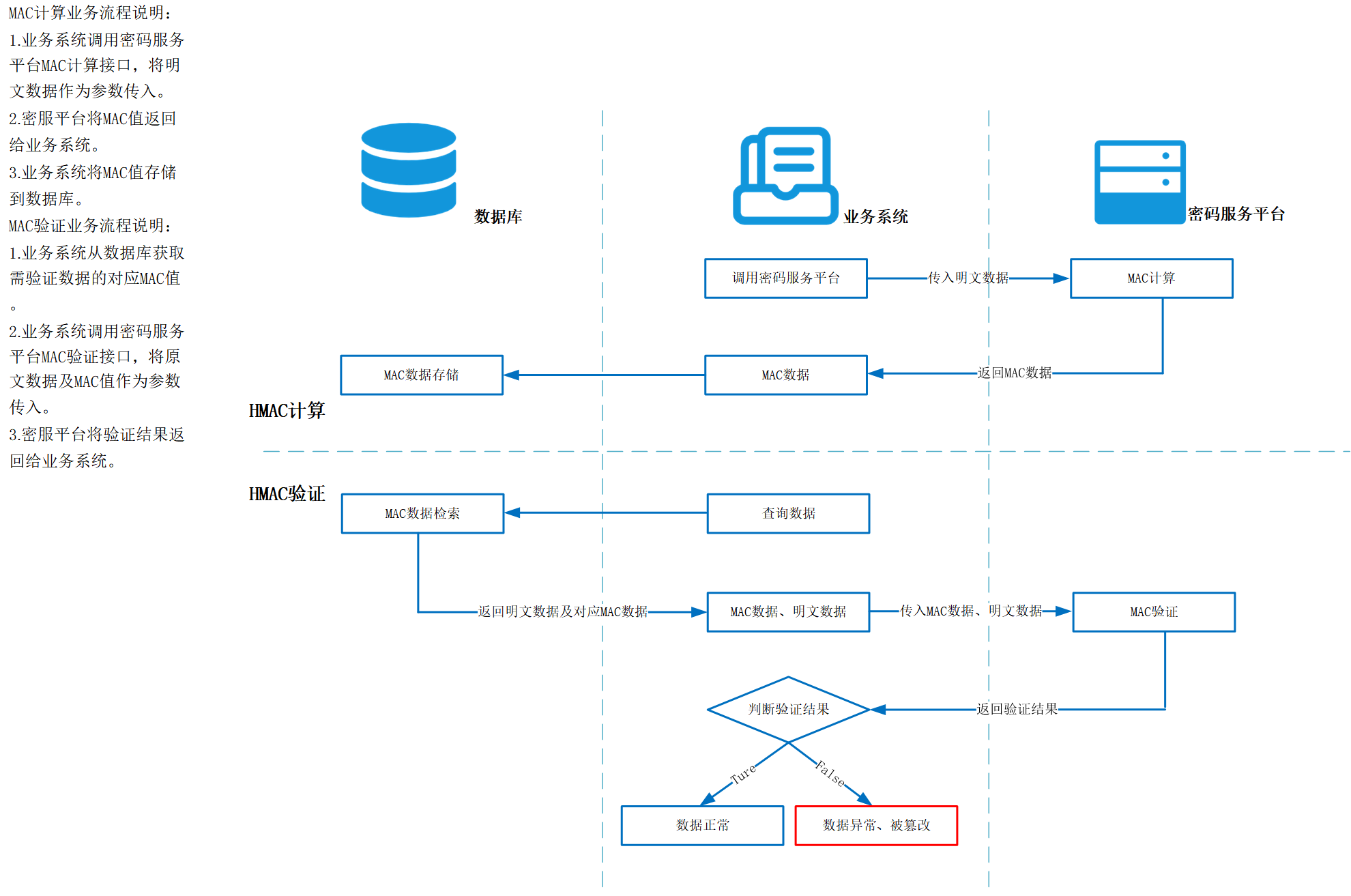


图 4 重要数据存储完整性保护

MAC计算业务流程说明：

1.业务系统调用密码服务平台MAC计算接口，将明文数据作为参数传入。

2.密服平台将MAC值返回给业务系统。

3.业务系统将MAC值存储到数据库。

MAC验证业务流程说明：

1.业务系统从数据库获取需验证数据的对应MAC值。

2.业务系统调用密码服务平台MAC验证接口，将原文数据及MAC值作为参数传入。

3.密服平台将验证结果返回给业务系统。

1. 重要数据传输机密性：部署已通过商用密码机构认证的SSL VPN安全网关，复用网络和通信层面搭建的国密SSL安全通信链路对重要数据传输进行机密性保护。
2. 重要数据传输完整性：部署已通过商用密码机构认证的SSL VPN安全网关，复用网络和通信层面搭建的国密SSL安全通信链路对重要数据传输进行完整性保护。
3. 不可否认性：本系统不涉及法律责任认定的应用场景，在本次密码应用改造及测评时，作不适用项处理。

{1.对于关键的操作行为，{操作者/应用系统}使用电子印章对关键操作行为和内容进行SM2算法/RSA算法的数字签名，签名内容为原数据的哈希值，签名主体为系统关键操作人员，签名位置为文件/网页，并由服务器端调用时间戳服务器加盖时间戳，把签名值、时间戳存到数据库。

在验证操作行为时，调用XX{密码设备名称，如签名验签服务器}对签名值进行验证，调用时间戳服务器校验时间戳，以此来实现关键操作的不可否认性。所使用的密码产品（UKey、时间戳服务器以及XX{密码设备名称，如签名验签服务器}）经商用密码认证机构认证合格，且满足密码模块第二级安全要求。

【病例、处方单、凭证等文件和文书，通过电子签章实现不可否认性】3.应用系统输出的{病例、处方单、凭证等文件和文书}），使用签发单位/签发人的电子印章，通过电子签章系统，对{病例、处方单、凭证等文件和文书}进行电子签章，签名算法为SM3+SM2，签名主体为公众用户，签名位置为文件或文书指定签名位置。

验证相关文件或文书时，通过调用安全电子签章系统进行验证，使用公钥验证电子签名值，实现关键操作的不可否认性。所使用的Ukey、安全电子签章系统经商用密码认证机构认证合格，其组件满足密码模块第二级安全要求，证书由合规的密码服务机构签发。}

**（添加流程）**

**密钥管理策略：**

1)密钥管理

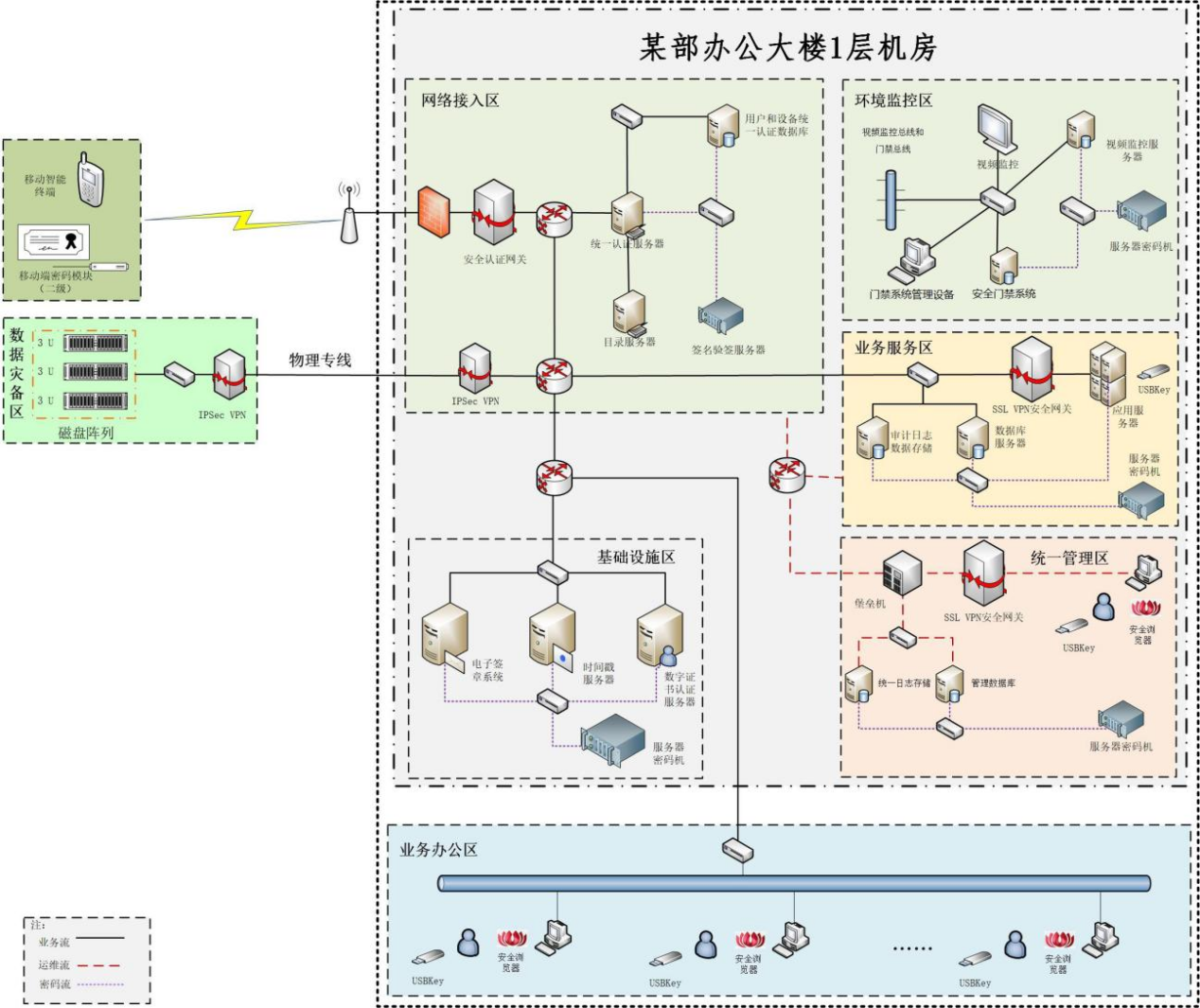
| **序号** | **密钥名称** | **算法** | **用途** | **存储位置** |
| --- | --- | --- | --- | --- |
| 1 | 重要数据传输机密性保护密钥 | SM4 | 用于保护SSL通道中重要业务数据的传输机密性 | 临时协商，用完销毁 |
| 2 | 重要数据传输链路身份鉴别私钥 | SM2 | 用于建立链路时SSL客户端和服务端的身份鉴别 | 服务端在密码卡、客户端在UKEY |
| 3 | 重要数据传输链路身份鉴别公钥 | SM2 | 以证书形式使用，用于建立链路时SSL客户端和服务端的身份鉴别 | 服务端在密码卡、客户端在UKEY |
| 4 | 重要数据传输链路密钥协商私钥 | SM2 | 用于SSL客户端和服务端的密钥协商 | 服务端在密码卡、客户端在UKEY |
| 5 | 重要数据传输链路密钥协商公钥 | SM2 | 以证书形式使用，用于SSL客户端和服务端的密钥协商 | 服务端在密码卡、客户端在UKEY |
| 6 | 用户签名私钥 | SM2 | 系统管理员登录应用系统 | Ukey |
| 7 | 用户签名公钥 | SM2 | 以证书形式使用，用于系统管理员登录应用系统 | Ukey |
| 6 | 应用系统主密钥 | SM4 | 用于通过密钥分散技术，派生重要数据存储完整性保护密钥和重要数据存储机密性保护密钥 | 密码应用中间件数据库 |
| 7 | 应用系统主密钥保护密钥 | SM4 | 用于保护应用系统主密钥 | 服务器密码机 |
| 8 | 重要数据存储完整性保护密钥 | HMAC | 用于保护身份鉴别信息、重要业务数据、日志数据的存储完整性 | 临时分散，用完销毁 |
| 9 | 重要数据存储机密性保护密钥 | SM4 | 用于保护身份鉴别信息、重要业务数据的存储机密性 | 临时分散，用完销毁 |

2) 密钥生命周期

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **密钥名称** | **生产** | **存储** | **分发** | **导入和导出** | **使用** | **备份和恢复** | **归档** | **销毁** |
| 1 | 重要数据传输机密性保护密钥 | SSL VPN客户端和服务端通过重要数据传密钥协商公私钥协商产生 | 临时协商、用完销毁 | 不涉及 | 不涉及 | VPN内部使用 | 不涉及 | 不涉及 | 临时协商、用完销毁 |
| 2 | 重要数据传输链路身份鉴别私钥 | VPN密码卡内部产生 | VPN密码卡内部存储 | 不涉及 | 不涉及 | VPN内部使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 3 | 重要数据传输链路身份鉴别公钥 | VPN密码卡内部产生 | VPN密码卡内部存储 | 不涉及 | 以公钥证书形式导入导出 | 以公钥证书形式使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 4 | 重要数据传输链路密钥协商私钥 | 由CA生产 | VPN密码卡内部存储 | 不涉及 | 不涉及 | VPN内部使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 5 | 重要数据传输链路密钥协商公钥 | 由CA生产 | VPN密码卡内部存储 | 不涉及 | 以公钥证书形式导入导出 | 以公钥证书形式使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 6 | 用户签名私钥 | 由ukey产生 | Ukey内部存储 | 不涉及 | 不涉及 | Ukey内部使用 | 不涉及 | 不涉及 | Ukey内部销毁 |
| 7 | 用户签名公钥 | 由ukey产生，由CA签发为公钥证书形式 | 以公钥证书形式存储 | 以公钥证书形式分发 | 以公钥证书导入导出 | 以公钥证书形式使用 | 不涉及、由CA备份和恢复 | 不涉及、 由CA归档 | 不涉及、 由CA销毁 |
| 8 | 应用系统主密钥 | 由密钥管理系统产生 | 密钥管理系统内部存储；  密码应用中间数据库密文存储； | 密钥管理系统使用密码应用中间平台根证书加密后分发至密码应用中间件；  密码应用中间将密文形式的应用系统主密钥分发至服务器密码机； | 不涉及 | 服务器密码机内部使用 | 密钥管理系统内部备份恢复 | 密钥管理系统内部归档 | 密钥管理系统内部销毁；密码应用中间件内部销毁 |
| 9 | 应用系统主密钥保护密钥 | 由服务器密码机内部产生 | 由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 | 服务器密码机内部备份恢复 | 不涉及 | 服务器密码机内部销毁 |
| 10 | 重要数据存储完整性保护密钥 | 由服务器密码机通过应用系统主密钥进行密钥分散内部产生 | 临时分散，用完销毁 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 临时分散，用完销毁 | 临时分散，用完销毁 | 临时分散，用完销毁 |
| 11 | 重要数据存储机密性保护密钥 | 由服务器密码机通过应用系统主密钥进行密钥分散内部产生 | 临时分散，用完销毁 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 临时分散，用完销毁 | 临时分散，用完销毁 | 临时分散，用完销毁 |

**5.5密码应用部署**

本系统部署和使用了【服务器密码机、签名验签服务器、SSL VPN安全网关、国密安全密码应用中间件、USBKey、IPSec VPN、电子签章系统、时间戳服务器】等密码产品，均具有商用密码产品认证证书，满足GB/T 37092-2018 《信息安全技术密码模块安全要求》标准二级模块要求。密码应用部署示意图如下：



**图3密码部署示意图**

1. 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，实现单向身份认证，确保授权用户身份的真实性。
2. 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安全网关之间的单向身份认证。运维人员通过安装SSL VPN客户端实现安全接入。
3. 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、密钥管理系统、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；密钥管理系统通过标准接口和不同密码设备对接，对外提供统一的密钥管理服务；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。

**密码软硬件产品：**

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，如下表所示。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 部署位置 | 主要用途 | 数量  (台/套) | 备注 |
| 1 | 服务器密码机 | 密码资源池 | 提供身份鉴别，保证关键业务信息的真实性、完整性和不可否认性 |  |  |
| 2 | 签名验签服务器 | 密码资源池 | 提供身份鉴别，保证关键业务信息的真实性、完整性和不可否认性 |  |  |
| 3 | 国密安全密码应用中间件 | 密码资源池 | 向下对接不同厂商的各类异构密码设备，向上提供统一的密码服务接口 |  |  |
| 4 | 密钥管理系统 | 密码资源池 | 通过标准接口和不同密码设备对接，对外提供统一的密钥管理服务 |  |  |
| 5 | 国密数字证书 | 智能密码钥匙 | 为系统提供基于密码技术的服务区分、标识、鉴别参与方身份/身份认证、电子签名/数据加密 |  |  |
| 6 | 智能密码钥匙 | 用户及运维人员PC端 | 用于PC端登录，实现登录人员的安全身份鉴别，防止非授权人员登录 |  |  |
| 7 | SSL VPN安全网关 | 网络接入区 | 基于国密SSL协议保证移动端、PC端与站点之间构建安全通道的设备 |  |  |
| 8 | IPSec VPN安全网关 | 网络接入区 | 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 |  |  |