政务云

云密码应用项目

整体建设方案

佰倬信息科技有限责任公司

2021 年 12 月 04 日

目录

第 1 章 项目概述

随着信息技术的发展，一个国家拥有的数据规模，以及对数据的运用能力已成为衡量综合国力的重要组成部分，对数据的占有权和控制权将成为“海、陆、空”之外的国家战略资源。我国高度重视“互联网+政务”建设，近几年各地方政府积极推进党政机关数据资源整合和开放共享，掀起了以云计算、大数据技术为主的“政务云”建设高潮。目前中央层面，国家电子政务外网政务云平台已经为中央政务部门 30 余项业务系统部署提供了统一、安全、按需使用的基础设施环境及技术支撑服务。地方层面，有 30 个省级行政区已经建有或正在建设政务云，占比超九成；在我国 334 个地级行政区中，有 235 个地级行政区已经建有或正在建设政务云，占比超七成。特别是进入 2020 年，“政务云”建设已成为“中国新基建”的重要组成部分，将为国家发展数字经济注入新动能。而随着全国政务云的迅速发展，云计算安全已成为制约云计算发展的重要一环，大量存储或运行在云端的数据缺乏必要的数据隔离措施和安全的应用程序接口控制，面临数据丢失、泄露及非法访问等风险。

密码技术作为网络与信息安全保障的核心技术和基础支撑，在维护国家安全、促进经济社会发展、保护人民群众利益中发挥着不可替代的重要作用。

第 2 章 系统现状分析

电子政务云平台通过构建全市统一的电子政务外网，采用丰富的云基础设施、云存储、云安全和各类服务构件共同组建成云计算中心，

为市委、市人大、市政府、市政协、机关和市直部门的非涉密业务提供服务。

政务云架构主要由 DMZ 区和非 DMZ 构成，分别上联至市民中心电子政务外网的 DMZ 区和非 DMZ 区。两个区域内部都由云平台区域、网络核心区域、网络出口区域、云安全区域构成，采用分区规划，分层设计，双节点冗余部署。云平台区域主要用于给租户分配计算资源、存储资源、网络资源，并承载了租户的东西向流量访问；网络核心区主要用于云平台数据层面、控制层面、租户南北向流量访问的数据交互，核心区域部署的安全设备保证了云平台的安全性；网络出口层主要用于和政务外网的互联互访，提供了云内和政务网的互联互通；云安全区域主要用于给租户发放安全组件，保证了租户业务系统的安全性。

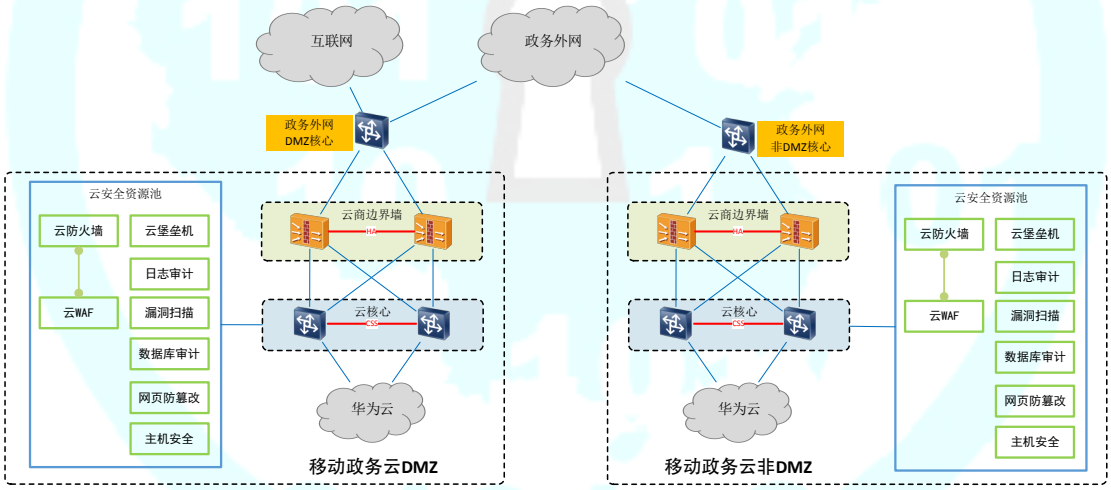


图 2-1 电子政务云平台架构

现针对整体网络架构特点，结合其网络安全实际需求，分析其目前存在的网络安全风险，并提出针对性的商用密码解决方案。

第 3 章 需求分析与响应

3.1 国家政策分析

近年来，为推进国家信息化战略的深入开展，国家主管部门先后出台了一系列网络安全法律法规和政策文件。密码技术作为网络与信息安全保障的核心技术和基础支撑，在解决网络身份的真实性、数据机密性、数据完整性保护和行为抗抵赖等方面发挥着不可替代的作用，也是构建无锡市电子政务外网网络安全保障体系的关键支撑。

2019 年 12 月 30 日，国务院办公厅发布《国家政务信息化项目建设管理办法》国办发[2019]57 号文，指出“项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。”安全可靠的密码技术已成为政务云安全的最后一道防线，各级党政机关网络与信息系统迫切需要加强国产密码应用。

2021 年 4 月 27 日 江苏省办公厅关于印发江苏省省级政务信息化项目建设管理办法的通知（苏政办发【2021】24 号）中在项目立项阶段、验收阶段有如下要求：

第十八条 项目建设单位应当落实国家和省密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。重要领域网络与信息系统规划阶段，项目单位应当依据有关规定，**制定密码应用建设方案**，组织专家或委托测评机构评估。对于涉及国家秘密的政务信息化项目，项目建设单位应当落实国家涉密信息系统分级保护制度和标准要求。安全保密防护措施和保密设施设备应当与涉密政务信息化项目同步规划、同步建设、同步运行。

第二十六条 省级政务信息化项目建成后半年内，项目建设单位应当按照国家有关规定申请省发展改革委组织竣工验收，提交验收申请报告时应当一并附上项目建设总结、财务报告、审计报告、安全风险评估报告(包括涉密信息系统安全保密测评报告或者非涉密信息系统网络安全等级保护测评报告等)、**密码应用安全性评估报告**等材料。省有关部门可以依据职责组织专项技术验收。

3.1.1 网络安全等级保护标准分析

网络安全等级保护制度是国家网络安全工作的基本制度,是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。《中华人民共和国网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求履行安全保护义务。网络安全等级保护制度在 2.0 时代着重于全方位的主动防御、动态防御、精准防护和整体防控的安全防护体系，将云计算、物联网、移动互联、工业控制信息系统和大数据等新应用、新技术纳入等级保护扩展要求。

本项目建设需要遵循的等级保护标准如下：

- 《GBT22239-2019 信息安全技术网络安全等级保护基本要求》
- 《GBT25070-2019 信息安全技术网络安全等级保护设计技术要求》
- 《GBT28448-2019 信息安全技术网络安全等级保护测评要求》

3.1.2 密码测评相关要求

《中华人民共和国密码法》第二十七条明确要求关键信息基础设施必须依法使用商用密码进行保护,并开展商用密码应用安全性评估；要求关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当依法通过国家网信办会同国家密码管理局等有关部门组织的国家安全审查。

本项目信息安全部分的建设除了符合等级保护 2.0 标准相关安全要求之外，还要遵守相关法律，符合相关标准：

- 《中华人民共和国密码法》
- 《GBT 39786-2021 信息安全技术 信息系统密码应用基本要求》

3.2 业务安全需求响应

3.3.1 设备和计算安全需求响应

3.3.1.1 用户身份鉴别需求响应

基于密码硬件设备，部署数字认证服务子系统，为所有访问应用系统的用户，包括 PC 客户端及移动客户端签发具有法律效力的数字证书，数字证书作为用户登录应用系统的身份凭证，保证数字证书的唯一性，工作人员访问各个应用系统时，需输入用户名及口令，并通过证书认证系统对用户的数字证书的有效性进行验证，只有验证成功后，才可被信息系统授权访问。

同时也作为应用系统内部的管理员、审计员等系统内部管理人员登录应用系统的身份凭证，保证数字证书的唯一性，并通过证书认证系统对用户的数字证书的有效性进行验证，只有验证成功后，才可被信息系统授权访问。

以上所有用户的数字证书存储载体应采用智能密码钥匙，当登录应用系统失败后，应用系统应在操作日志上进行记录，并进行告警。进而为用户建立网络安全信任体系，解决应用系统中因身份被假冒和欺诈造成的信息泄露。数字证书的应用，实现了在访问控制、数据操作等方面的可追溯机制，进而让信息泄露的行为无法否认及抵赖。

对于终端设备，数字证书服务子系统也可签发设备证书，用于对

链接到内部网络的终端设备进行安全认证，确保访问终端接入安全，防止非法设备入侵造成的网络攻击及数据泄露。

3.3.1.2 流程安全审批安全响应

对于需要通过单位或个人的盖章或签名来实现责任认定的认证需求，该项目除了部署数字证书服务子系统之外，还部署了电子签章服务子系统、时间戳服务器。针对像电子证照系统需要加盖电子印章的业务需要，电子签章服务子系统可以为电子证照系统提供合法可信的电子签章服务，时间戳服务器提供可信时间服务，以上服务基于国产密码算法技术、图像防伪技术以及组件技术，将电子印章与数字签名技术、时间戳技术相结合，最终形成文件内容可验证、身份真实性可验证、时间有效性可验的合法电子印章，进而确保了电子文件的真实性、有效性和合法性。

3.3.2 网络和通信安全需求响应

3.3.2.1 网络通信安全响应

传输安全需求响应方面，对于两个数据中心之间搭建的运维专线，需要在两端分别部署通过国家密码管理部门核准的 IPSec VPN 综合安全网关，构建国密 IPSec 加密通信专用通道，对网络中的安全设备或安全组件进行集中管理。两边的通信数据采用 SM1 或 SM4 国密算法进行加密，同时采用 SM3 算法进行完整性保护，确保通信过程中数据的机密性和完整性。

3.3.2.2 数据传输安全响应

目前各应用系统在数据传输的时候均是以 HTTP 协议明文传输

数据，信息赤裸裸的暴露在网络中，毫无安全性可言。为了防止明文数据在传输过程中的泄露风险，由中控平台集成的中间件通过调用云密码资源池子系统的密码服务，封装基于国密SSL协议的加密套件，各应用系统通过中间件使用HTTPS协议进行密文传输数据，确保数据传输的机密性和完整性。

3.3.3 应用和数据安全需求响应

3.3.3.1 数据库存储安全响应

应用系统在产生的数据需要定时备份归档，数据库集群设备中存储了大量的重要数据、个人敏感信息、云服务用户管理员账户数据，以上数据都是以明文形式进行存储，数据库很容易遭到黑客及内部高权限工作人员的拷贝，造成数据泄露。因此数据库可以调用云密码资源池子系统对数据库敏感信息进行加密存储和完整性校验，确保存储数据的机密性和完整性。

3.3.3.2 日志审计安全响应

（1）采用数字签名技术对日志数据进行签名，确保日志数据完整性，防止日志数被恶意篡改。

（2）当日志数据被修改或被篡改，应用系统能够发现，将相关操作记录在日志中，并进行告警。

（3）采用数字签名技术对审计数据进行签名，确保审计数据真实性，防止审计数被恶意篡改。

（4）当审计数据被非授权人员修改或被篡改，应用系统能够发现，将相关操作记录在日志中，并进行告警。

3.3.3. 密钥存储安全响应

应用系统的私钥和对称密钥以密文的方式安全存储在密码基础设施中的密码硬件设备中，私钥不得以明文方式导出密码硬件设备。

第 4 章 项目总体设计

4.1 设计依据及原则

4.1.1 建设原则

一是坚持政府主导、市场参与。创新电子政务云安全管理模式，建立健全配套工作机制，加强部门责任分工，高效搭建电子政务云密码应用平台，为全省提供统一云密码服务。

二是坚持集约高效、开放融合。加强统筹规划，实现信息化基础设施、平台和应用的共建共享，降低建设运维成本，提高政府资金使用效益。有效整合横向和纵向软硬件资源，消除信息孤岛，形成逻辑一体、开放共享的良好格局，推动电子政务创新发展。

三是坚持安全合规、自主可控。遵循《GBT 39786-2021 信息安全技术 信息系统密码应用基本要求》中等级保护第三级信息系统的密码应用要求，执行电子政务网络安全相关标准规范，落实网络等级保护要求。

4.1.2 建设依据

围绕无锡市信息化建设和发展对信息安全的实际要求，以需求为导向，建设佰倬信息电子政务云密码应用整体建设方案的工作，应参照以下重要文件、方案和规范：

- 《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》国办发【2019】57 号
- 《国务院办公厅转发密码局等部门关于-金融领域密码应用指导意见的通知》
- 《基于云计算的电子政务电子认证服务应用指南（征求意见稿）》
- 《关于进一步做好信息安全等级保护工作的意见》
- 《国务院关于印发促进大数据发展行动纲要的通知》
- 《政务服务中心网上服务规范》
- 《中华人民共和国电子签名法》
- 《电子认证服务密码管理办法》
- 《电子认证服务管理办法》
- 《信息安全等级保护商用密码技术要求》
- 《网络安全等级保护条例（征求意见稿）》
- 《网络安全等级保护基本要求》

4.1.3 建设目标

本项目严格按照《中华人民共和国密码法（草案）》及商用密码有关规范，以落实网络安全等级保护、GB/T-39786-2021 密码测评等相关标准为原则，搭建市级电子政务云密码应用平台。项目从安全计算环境、安全区域边界、安全通信网络和集中安全管理等方面，通过国产商用云密码产品和技术，实现多种类密码服务资源上云、云密钥隔离、密码资源弹性扩展、密文计算、数据溯源等功能，解决传统

云密码服务性能低、密钥安全风险高、数据隐私泄露等安全问题，实现密码资源的高效利用，为政务云提供统一的密码管理服务。

该项目建设后可为政务云应用系统提供身份识别、安全隔离、信息加密、完整性保护、抗抵赖性等方面的密码防护，为信息系统的安全可靠运行提供全面高效的密码支撑，保证达到国家密码管理局合规性、完整性和安全性要求。项目的实施对于提升全社会信息化水平，提升政府公共服务水平，实现政务云的可控、可信、可管、可监督和可追溯，发挥政府信息资源在推动经济社会全面发展中的重要作用，推动政府职能转变，提升政府公共服务水平，促进信息服务产业发展。

4.2 项目总体设计

4.2.1 总体架构设计

按照“整体规划、安全合规、集约高效、按需服务”的原则，规划建设面向政务云、政务大数据中心的云密码应用项目。项目依托“无锡市政务云平台”进行统筹规划。

项目总体架构图如图 4-1 所示。

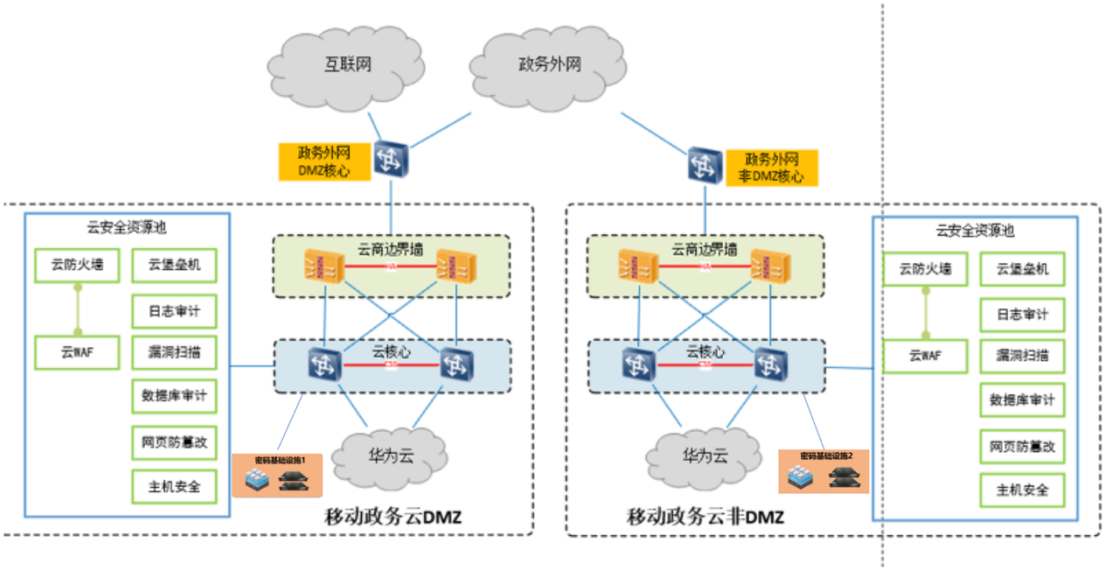


图 4-1 政务云总体网络架构图

各数据中心按照区域划分为统一互联网出口区、互联网数据中心、电子政务外网数据中心、安全管理区、网管中心区等，其中密码基础设施分别部署在政务云 DMZ、政务云非 DMZ。

密码基础设施由云密码服务平台、佰倬密码服务模块、数字证书认证系统、密钥管理系统、电子签章系统、时间戳服务器、SSL VPN 安全网关等密码软硬件设备组成，见图 4-2。各密码基础设施均为双机冗余结构设计，可避免因一台设备或单个系统异常而导致业务中断，也可为业务流量负载分担。

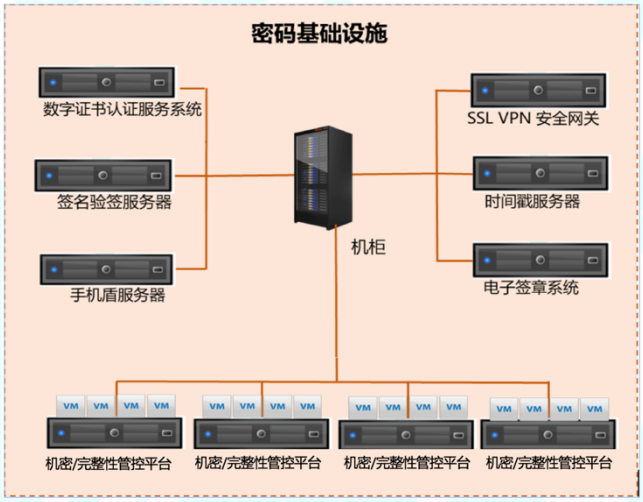


图 4-2 密码基础设施组成

其中云密码服务平台是政务云密码应用平台的核心，负责密码资源的申请、创建流程。其余密码设备如数字证书认证系统、密钥管理系统、SSL VPN 安全网关等与上述原理类似，结合虚拟化弹性扩展、自动迁移、镜像安全等技术实现密码资源应用层上的高效利用，为云上应用系统提供虚拟化的身份认证、密钥管理、授权管理、权限控制、策略安全等密码服务。

4.2.2 商密应用逻辑架构

本项目通过在大数据中心机房的政务云 DMZ、政务云非 DMZ 区分别建设密码基础设施，以平台服务的形式对外提供政务业务密码服务。密码应用逻辑架构包括应用层、相关接口、云密码管理服务层、密码基础服务层、基层设施层组成，见图 4-3。

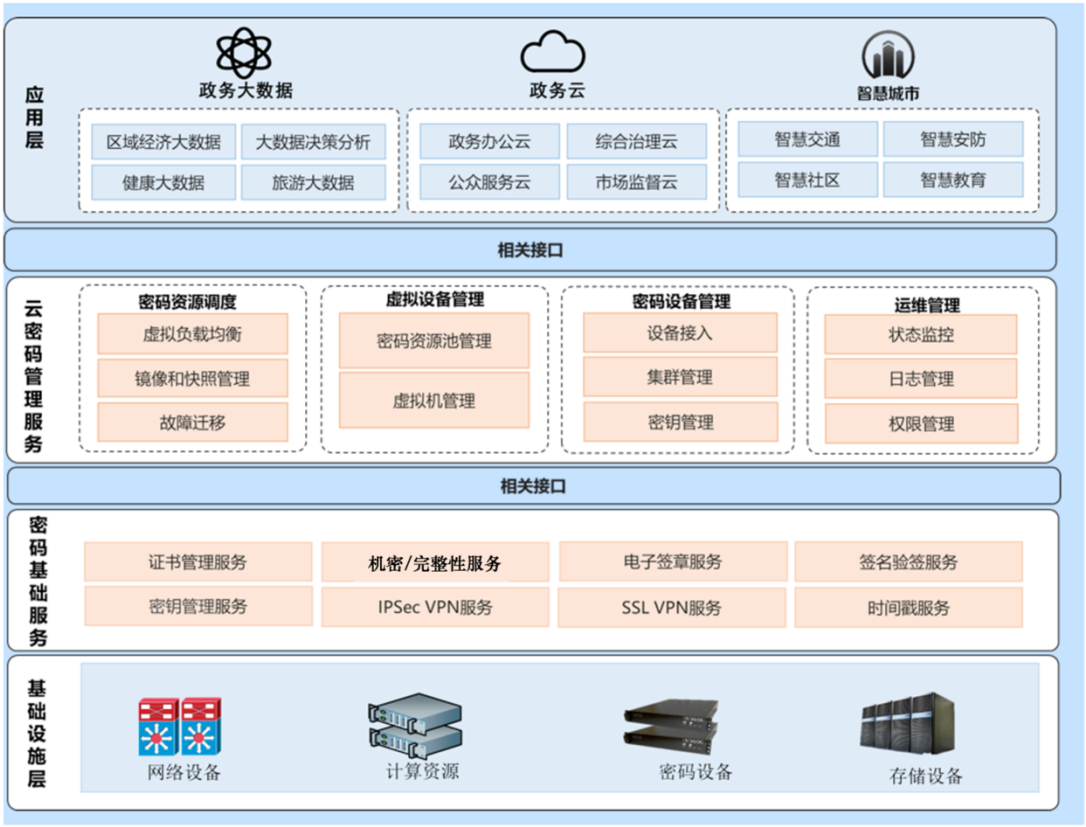


图 4-3 政务云密码应用逻辑架构图

各层功能如下：

应用层：包含智慧城市、政务云、政务大数据中心等相关应用。

相关接口：以接口形式为上层应用提供密码服务。

云密码管理服务层：提供密码资源虚拟化功能，可实现在应用层的资源调度、动态迁移、权限控制、弹性扩容、资源容灾、密钥同步等。

密码基础服务层：为整个上层应用提供包括密码算法服务、证书管理服务、密钥管理服务、电子签章服务、时间戳服务、随机数服务等。通过采用虚拟化技术在硬件平台上同时运行多个虚拟化密码机，达到保证功能服务不变、降低总体成本、提高服务资源利用率的目的。

各密码设备提供的服务如下：

1）云密码服务平台。提供虚拟机资源的管理、业务绑定、高可用等配置功能，同时为租户调用提供界面友好管理客户端，帮助用户实现便捷的虚拟密码机设备管理、人员管理、密钥管理、权限管理和备份/恢复等操作。对于用户/租户而言，可以根据自身需求直接选择 VHSM 提供各种典型密码服务。

2）佰倬密码服务模块。可以实现以 SM3 和 GB/T 15852.2 MAC 密码算法为基础的消息鉴别服务，实现对数据和控制访问信息进行完整性保护；以 SM4 密码算法为基础的数据加密解密服务，实现重要数据在传输和存储过程中的机密性保护，确保重要数据的机密性和完整性。

3）数字证书认证系统。包括 CA 证书认证系统、RA 证书注册系统、OCSP 证书状态在线查询系统、LDAP 目录服务器等部分。云数字证书认证系统具备部署快速、灵活，可以动态配置，易于水平扩展的特点，具有大并发、弹性部署的优势，能够满足云上大量用户证书的管理需求。通过云数字证书服务，满足电子政务外网对身份认证和行为认证的要求，形成覆盖政务云的安全、规范、可靠、易用的密码应用基础服务体系；

4）密钥管理系统。密码安全的核心是密钥的安全，密钥的产生、

存储、分发、恢复等对保障信息系统的安全至关重要。政务云中有大量密钥需要统一管理，由于云上业务系统数量多、网络实体类型多，云上存储大量重要的数据需要加密保护，不同用户的数据、不同类型的数据需要不同的密钥，包括证书公钥、加密密钥等对称密钥和非对称密钥等；大量用户和网络实体的身份密钥、海量的数据加密密钥使得云中的密钥管理必须使用专门的云密钥管理服务。通过部署佰倬信息云密钥管理系统，可规范政务云上密钥管理，实现各级部门自上而下密码应用的互信互任；

5）电子印章系统。可实现电子印章从制作、发布、到应用完整的公共服务支撑体系，确保单位使用电子印章对电子文件加盖过程、结果符合国家法律法规要求，实现电子文件安全、合法、有效应用。

6）IPSec/SSL VPN 综合安全网关。佰倬信息通过 IPSec/SSL VPN 综合安全网关可构建基于国产密码技术的加密隧道，为需要远程接入的业务系统建立一个安全的接入网络，实现对远程接入的内部用户进行统一身份认证、统一系统账号管理、统一访问权限及单点登录，满足内部用户在任何时间、任何地点、使用任何主流终端，安全、快速地接入平台相关业务系统，实现业务移动化，提高办事效力，提升服务质量，同时保证用户身份安全、接入终端和数据安全、传输安全、应用权限安全和审计安全。

7）签名验签系统。签名验签服务主要应用于电子签名、电子政务等业务类型系统，可以为电子签章服务提供基础支撑能力。通过签名验证服务，对安可云平台中各应用单位关键业务数据和政务安可云平台管理中审计数据进行签名与验签，实现不同单位和人员责任认定

的不可否认性。

8）时间戳服务器。时间戳服务器是提供国家授时中心权威时间源和第三方权威认证机构的时间戳服务的软硬一体设备。该产品对网上交互中各方交互数据产生的时间点提供第三方时间戳认证,为数据产生时间点提供公正可信的认证支持,有效解决信息的时效性和操作行为的时效性。

9）手机盾系统。手机盾系统主要为移动端业务系统提供移动端证书的申请、签名、对称加解密、非对称加解密、用户信息变更等功能。

4.2.3 商密应用网络部署

本项目密码应用网络部署如下：

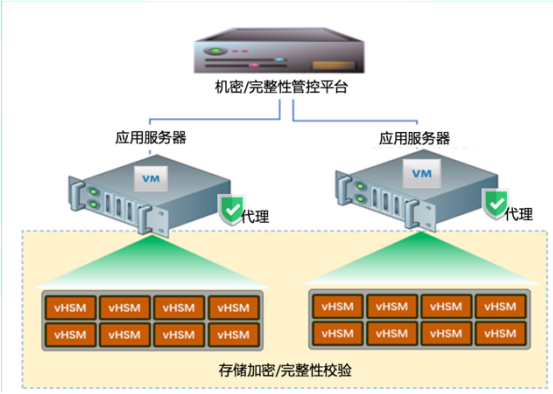


图 4-4 密码应用网络部署图

云密码服务的用户可能通过物理设备访问服务，也可能通过云中虚拟主机访问服务，因此云密码服务的访问主体最终会落实到物理设备，或云中的虚拟主机、微服务实例、或应用程序等实体。在这些实体的设备或者虚拟操作系统中部署数安密码模块,为这些实体提供数据存储机密性和完整性服务，无需这些实体做任何应用层代码改造，

监控信息通过加密通道返回给佰倬岗哨平台。见图 4-5。

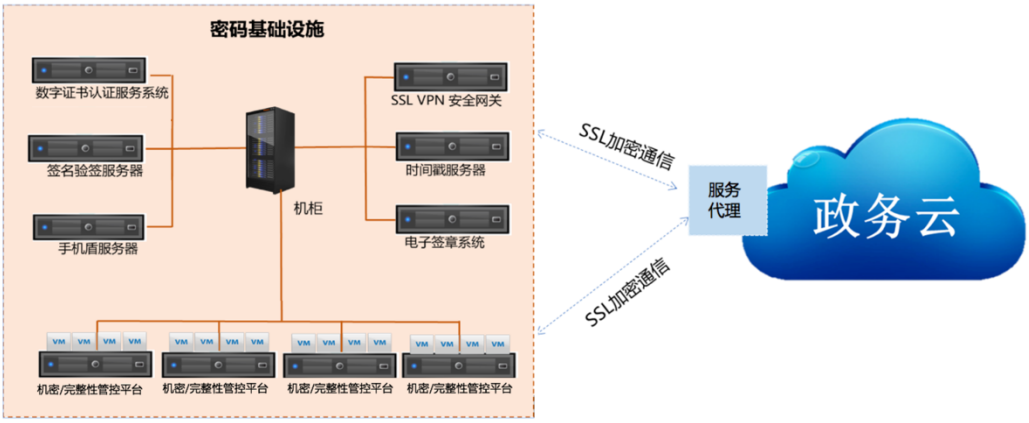


图 4-5 存储机密性保障服务调用原理

云应用/用户通过调用密码接口实现密码资源池内相应虚拟密码机的密码运算和密钥管理操作，无需关心这些功能是在哪些基础设施上完成，密码基础设施的建设、部署和维护，均委托给云服务提供方，用户只需要关注密钥管理、安全策略配置及安全审计等方面的运维管理。密码服务开通后，可有服务提供商设置初始管理员后，将身份认证凭证（装载数字证书的智能密码钥匙）交给用户，用户即可远程登录到云密码服务管理界面。

4.2.4 商密应用双活设计

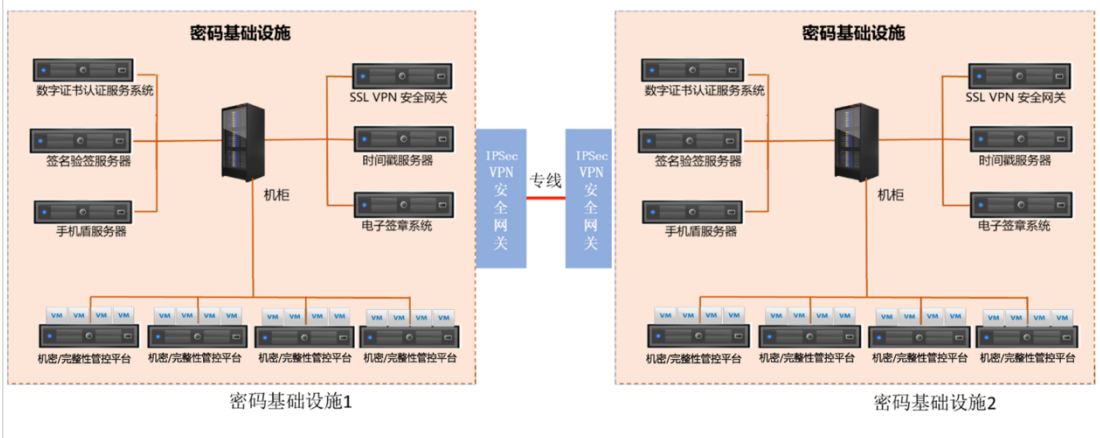


图 4-6 云密码应用双活设计拓扑图

为了满足两个数据中心的双活要求，密码基础设施也完成了双活模式的部署，该项目中关键核心技术就是密钥等重要数据的安全同步。

（1）设备认证

密码基础设施采用设备认证机制，设备完成双向认证后，才可以安全通讯。

（2）安全传输

密钥等重要的数据通过国密 SSL 协议安全传输，并对传输数据进行签名及完整性校验，确保数据安全同步。

（3）瞬间迁移

密码基础设施如遇一侧发生故障，在客户无感知的情况下进行的瞬间迁移，确保云密码应用的高可用性。

第 5 章 商密改造详细设计方案

5.1 设备和计算安全密码改造

5.2.1 PC 端基于证书的单点登录改造

单点登录（Single Sign On）指用户只需要登录一次就可以访问所有相互信任的应用系统。政务云上有大量业务系统，用户登录多个业务系统需要多次手动输入用户名和口令，从而增加了管理成本，并降低访问效率。

根据等保 2.0 及 GBT/39786 相关规范要求，需要应用密码技术对用户进行身份鉴别。针对电子政务云上业务系统进行国密改造，其中涉及内容包括：

- 云平台统一身份认证系统改造为“SM2 密码算法数字证书+智

能密码钥匙”双因子认证模式；

● 云平台业务系统改造为“SM2 密码算法数字证书+智能密码钥匙”双因子认证模式；

工作流程如下：

（1）用户插入 Ukey，刷新单点登录系统登录页面。

（2） 调用客户端控件登录服务接口，客户端向服务器发出访问请求，并产生一个随机数 A 发给服务器；

（3）服务器用私钥对随机数 A 进行签名得到服务器签名 A’，并产生一个随机数 B，连同证书相关信息发回客户端；

（4）客户端利用服务器提供的证书信息查询 LDAP 目录服务器，获取服务器证书后，利用证书中的公钥对签名 A’进行签名验证，从而确认服务器身份。

（5）客户端用私钥对服务器发来的随机数 B 进行签名得到客户端签名 B’，连同客户端证书的相关信息发给服务器。

（6）服务器利用客户端提供的证书相关信息查询 LDAP 目录服务器，获取客户端证书后，利用证书中的公钥对客户端签名 B’进行签名验证，从而确认客户端身份。

（7）单点登录系统查询用户单点登录映射表，找到该用户证书相应的应用系统上绑定的账号，生成用户令牌，重定向到应用系统。

（8）应用系统接收统一格式的用户令牌，取得用户在本系统上的登录账号，将用户在本系统上状态置为登录，返回用户请求访问的页面，完成用户对该应用系统的访问。

5.2.2 移动端基于数字证书的身份认证改造

随着移动互联网、云计算的发展，移动政务的应用越来越多，而传统的身份认证手段在移动互联网环境下的安全问题面临着巨大挑战。对用户本身的身份认证采用用户名、口令方式不安全，容易被嗅探、破解甚至拖库；短信动态口令容易被劫持；动态口令令牌存在钓鱼风险；安全级别最高的 UKEY，采购成本高，分发管理困难，用户使用不方便，最重要的是也不适合手机终端的使用。

为解决移动政务业务的安全，需要应用基于密码技术的身份鉴别、电子签名、数据加密等服务，对移动端业务系统进行安全加固。针对电子政务云上移动政务业务系统进行国密改造，其中涉及内容包括：

在移动终端（IOS、Android）系统中部署 SDK/APP，政务云服务端部署手机盾系统，实现终端用户移动终端的身份认证、签名验签、数据加密功能。

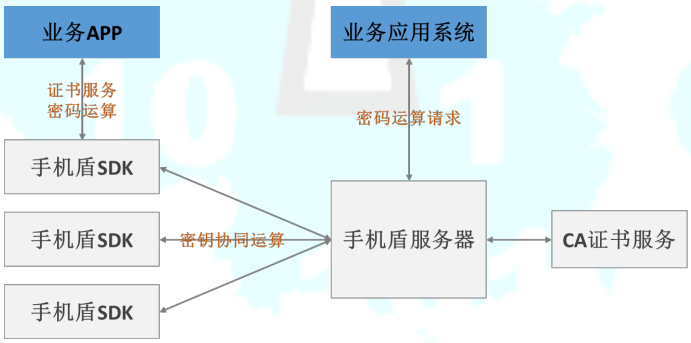


图 5-1 手机盾工作原理

手机盾系统应用的特点：

（1） 手机端安装手机盾 SDK，采用数字证书技术满足合法性、等级保护相关要求；

（2） 采用密钥分割和协同计算，密钥分别由手机端和云端手机盾服务器生成，“云+端”协同计算，密钥永远不会以明文形式出现；

（3） 手机盾 SDK 盾和手机盾服务器之间采用 SSL 协议保证安全通信。

5.2 网络和通信安全密码改造

Http 超文本传输协议协议被用于在 Web 浏览器和网站服务器之间传递信息，http 协议属于明文传输协议，交互过程以及数据传输都没有进行加密，通信双方也没有进行任何认证，通信过程非常容易遭遇劫持、监听、篡改，严重情况下，会造成恶意的流量劫持等问题，甚至造成云租户隐私数据泄露等严重的安全问题。

为了数据传输的安全，https 在 http 的基础上加入了 SSL 协议，SSL 依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。可信安全 SSL 站点证书用于标识网站真实身份，它能够实现网站身份验证，确保用户访问网站的真实性，确保用户所浏览的信息是真实的网站信息，能有效防范假冒网站和钓鱼网站。同时，SSL 站点证书也可让用户在网上输入的各种个人机密信息都能自动地加密传输，确保不会被非法窃取和非法篡改，让用户可以放心地使用各类网上服务。

图 5-2 Http 和 Https 协议对比

通过浏览器可以查看到经权威浏览器厂商信任的证书颁发机构，当在访问使用该类证书的网站时，浏览器就会自动下载该网站的 SSL 证书，并且对证书的安全性进行检查。站点数字证书通过对网站安全

的认证，能有效地提升政府的形像，有效地防止假冒网站的盛行和用户身份信息的窃取，保障广大客户的利益。

https 可以理解为 http over ssl，既把 http 明文流量通过 ssl 协议进行加密传送，从而保证数据的安全性。Https 加密技术是保护数据传输安全的技术保障技术，结合 SSL 证书的认证机制，实现数据加密、数据完整性和服务器身份鉴别等安全功能，见图 5-1-1。

目前部分政务业务系统仍然使用 Http 协议传输数据，无法适应政务云的安全建设需求。同时，有的政务业务系统即便采用 Https，也是采用 RSA 算法实现，不符合密码算法合规性要求。因此在数据传输环节，应采用基于国产 SM2 密码算法技术的加密技术保护传输数据，保障数据保密性和完整性。

目前主流的 Https 国密改造有两种模式：

1、 国密 SSL VPN 安全网关

2、 国产浏览器 Https 国密改造

5.3.1 国密 SSL VPN 安全网关

采用 SSL 服务器证书可解决网站信任及数据加密传输问题，但若直接部署至服务器时，SSL 协议及加解密运算会消耗大量的服务器资源，服务器启用 SSL 加密技术之后,有部分计算性能都消耗在了 SSL 的加密运算方面。另外，由于 web 服务器基本采用国外的中间件应用服务器（如 webLogic 等），在服务器上直接部署 SSL 时，存在不可预知的高危漏洞。

因此，针对 SSL 加解密事务处理的高性能需求，可通过部署专

用的 SSL 加速产品——国密 SSL VPN 安全网关，将 SSL 加密和解密工作交由专用设备完成，对网站 SSL 进行卸载，有效减少服务器性能开销，解决安全问题和性能问题，见图 5-3。

图 5-3 SSL VPN 安全网关部署示意图

配备 SSL 卸载功能的国密 SSL VPN 安全网关设备，可以充当起 SSL 代理服务器的角色，将专用的 SSL 应用程序置于网络服务器的前端，不影响后台服务器主机的 CPU 资源，从而全面卸除 SSL 数据处理的负荷。

当客户端发起的 HTTPS 连接，经过安全网关设备处理后，变成明文的 HTTP 数据，即可被 WEB 服务程序(例如 IIS、APACHE)直接读取，无需特殊的驱动程序来传送和接受网络数据。

5.3.2 国产浏览器 https 国密改造

Https 国密改造优势如下：

- 高安全性

采用的服务器安全站点证书，支持证书显示域名、域名持有单位名称等信息，保证站点真实可靠，实现 128 位安全通道加密、支持多域名扩展。

- 高可靠性

考虑到之前发生的棱镜门等国外监听计划，政府网站不仅要全站

HTTPS ,还应选择自主可控的国产 SSL 证书 ,防止加密流量被监听，防止国家重要民生数据被泄露。本方案采用国内第三方 CA 机构签发出的可信国产 SSL 证书，同时支持微软等主流浏览器无缝嵌入，直接信任。

针对电子政务云上业务系统进行国密改造，其中涉及内容包括：

- 云平台 web 管理系统 Http 改造为符合国密的 Https；
- 国产浏览器、国产中间件采用符合国密算法的产品和模块；
- 云平台、堡垒机或云访问安全代理 CASB 采用符合国密算法的产品和模块。

工作流程如下：

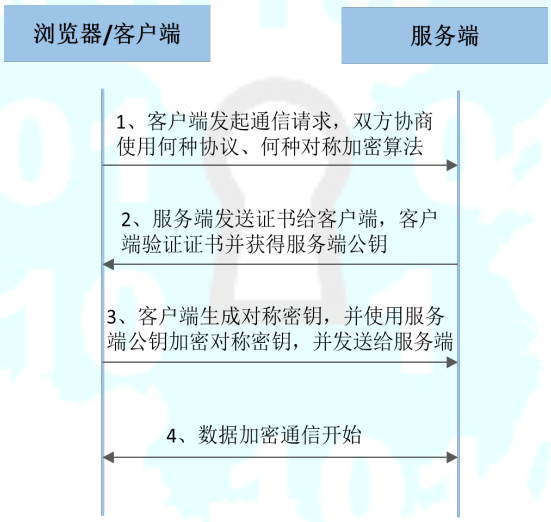


图 5-4 https 改造流程图

客户端在使用 HTTPS 方式与 Web 服务器通信时有以下几个步骤，如图所示。

（1）客户使用 https 的 URL 访问 Web 服务器，要求与 Web 服务器建立 SSL 连接。

（2）Web 服务器收到客户端请求后，会将网站的符合国密要求

的证书信息（证书中包含公钥）传送一份给客户端。

（3）客户端的浏览器与 Web 服务器开始协商 SSL 连接的安全等级，也就是信息加密的等级。

（4）客户端的浏览器根据双方同意的安全等级，建立会话密钥，然后利用网站的公钥将会话密钥加密，并传送给网站。

（5）Web 服务器利用自己的私钥解密出会话密钥。

（6）Web 服务器利用会话密钥加密与客户端之间的通信。

5.3 应用和数据安全密码改造

5.3.1 设计原理

应用和数据安全部分，涉及身份鉴别、数据传输的机密性和完整性保护、数据存储的机密性和完整性保护、访问控制信息的完整性保护。

5.3.1.1 身份鉴别

身份鉴别采用 SM2 数字证书+用户名+口令的方式实现，由 VPN 综合安全网关提供统一认证并提供单点登录服务。

部署签名验签服务器,对接入的用户进行身份验证,由自建的 CA 中心统一发放的数字证书进行检验,通过 USBkey+口令方式,确认用户的真实身份,增加系统的抗抵赖性.

5.3.1.2 访问控制信息完整性

业务系统对用户访问控制权限列表导出其 SM3 文件数据，并对相应的 SM 3 文件数据进行 GB/T 15852.2 MAC 计算， 从而实现访

问控制信息的完整性保护，保护访问控制权限列表不被篡改。

5.3.1.3 传输安全

通过国密 SSL 协议保证数据传输安全。国密 SSL 协议由 VPN 综合安全网关实现，支持 L4 层和 L7 层的安全传输保护。对于支持安全浏览器的 PC 客户端，可通过国密 https 协议，保证数据传输的完整性和机密性。国密 https 协议通过部署 VPN 综合安全网关的 SSL 卸载功能实现。对于不支持安全浏览器的 PC 客户端，通过客户端代理方式，实现 L4 层安全传输保护。

5.3.1.4 存储机密性安全

通过对应用系统的合法应用/进程进行授权，该服务运行在操作系统内核级，从计算执行环境中加密划分出安全隔离的活动空间来进行数据活动，保证在应用系统在读写磁盘时透明实现数据存储的加密与解密操作，存储加密采用国密 SM4 算法，对于每个存储的数据文件采用一文一密的方式，保证最大限度的存储机密性。

密码算法

- 对称算法：SM4
- 非对称算法：SM2
- 杂凑算法：SM3
- 国标 GB/T 15852.2 MAC

5.3.2 密码产品与服务

应用和数据安全层面采用的密码产品包括：服务器密码机。各产

品主要功能如下：

5.3.2.1 时间戳服务器

产品资质	商用密码产品认证证书
产品标准	符合GM/T 0033-2014《时间戳接口规范》
密码算法	支持SM2、SM3、SM4算法。
用途	部署在应用服务器,使用数字签名技术，在时间方面，防止网上操作行为抵赖、电子数据有效性抵赖以及重要流程中环节执行时间或完成时间的顺序控制。

5.3.2.2 CA数字证书认证系统

取得商用密码产品认证证书，符合 GMT 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》，数字证书格式符合 GM/T 0015-2012《基于 SM2 密码算法的数字证书格式规范》。CA 数字证书认证系统包含 CA、RA、LDAP、OCSP 等证书服务模块，支持 SM2 双证书签发。支持数字证书申请、签发、认证、更新、注销等全生命周期的管理。

5.3.2.3 智能密码钥匙

取得商用密码产品认证证书，符合 GM/T 0027-2014《智能密码钥匙技术规范》、GM/T 0048-2016《智能密码钥匙密码检测规范》。支持 SM1、SM2、SM3、SM4 算法。采用物理噪声源生成真随机数。支持 128K 用户存储空间，可安全存储密钥、证书等敏感数据。支持 PKCS#11、CSP 标准安全中间件接口

5.3.2.4 数安密码模块

密码模块已取得商用密码产品认证证书,可以实现受集中管控的分布式的内核级数据透明加解密功能和数据完整性检查。采用标准的密码算法接口，使用国家标准加密算法 SM2 验签算法，SM3、SM4 和国标 GB/T 15852.2 MAC 算法，遵循国密算法标准实现 SM4 对称加密算法 GM/T 0002-2012。内核级密码模块直接对可执行程序，存储的各类数据文件譬如访问控制信息日志记录等进行完整性保护。对于结构化敏感数据以及嵌入式系统中的敏感数据,则由数安岗哨平台进一步通过读取各个相关的设备的访问控制信息/数据库关键敏感信息譬如身份认证信息/关键访问登录信息等等，计算并记录 MAC（GB/T 15852.2 MAC)值,然后依托岗哨平台或密码模块进行 MAC 检验,确保此类结构性信息或嵌入式系统敏感信息的完整性监测和保护。

5.3.3 工作流程

5.3.3.1 数据加解密流程

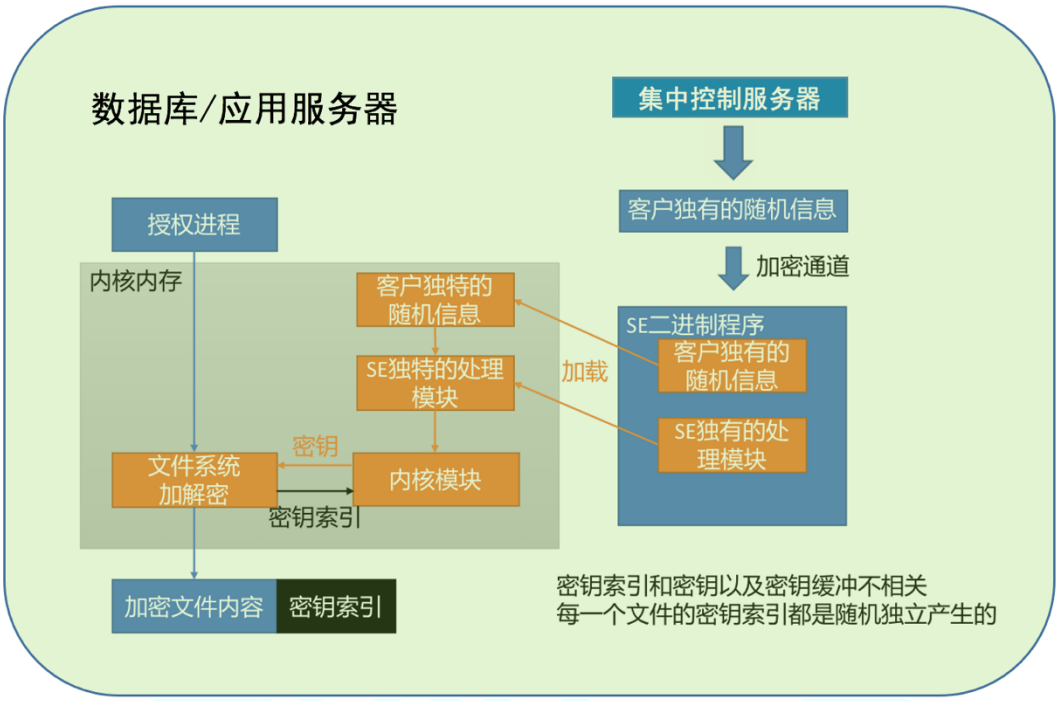


图 5-5 数据加密流程

具体业务流程如下：

数据存储加密：

首先从硬件的根密钥生成器获取随机信息，通过建立安全传输通道从集中控制服务器接收的保密材料，这些信息与模块就会被加载到操作系统的内核之中，独有的密钥处理模块使用客户独有的随机信息生成密钥种子放在内核模块之中。当选定需要被加密保护的数据文件之后，加密保护软件会为被选中的每一个文件生成一个互不相同、且无规律的、随机的密钥索引，密钥索引不包含任何与密钥相关的信息—即两者“互信息”为零。此密钥索引被传递到内核模块中加上之前的密钥种子进行处理并生成对任何一个单一文件的密钥，密钥传递给文件加解密模块并对相对应的文件进行加密处理，同时密钥索引也会与相对应的加密文件一起存储。

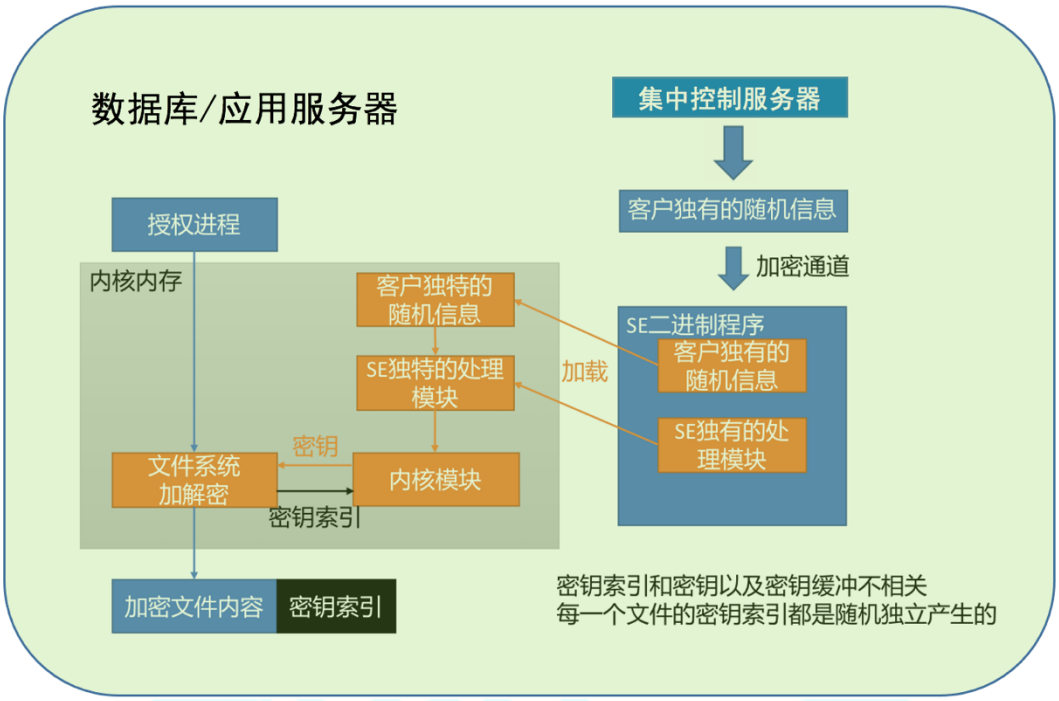
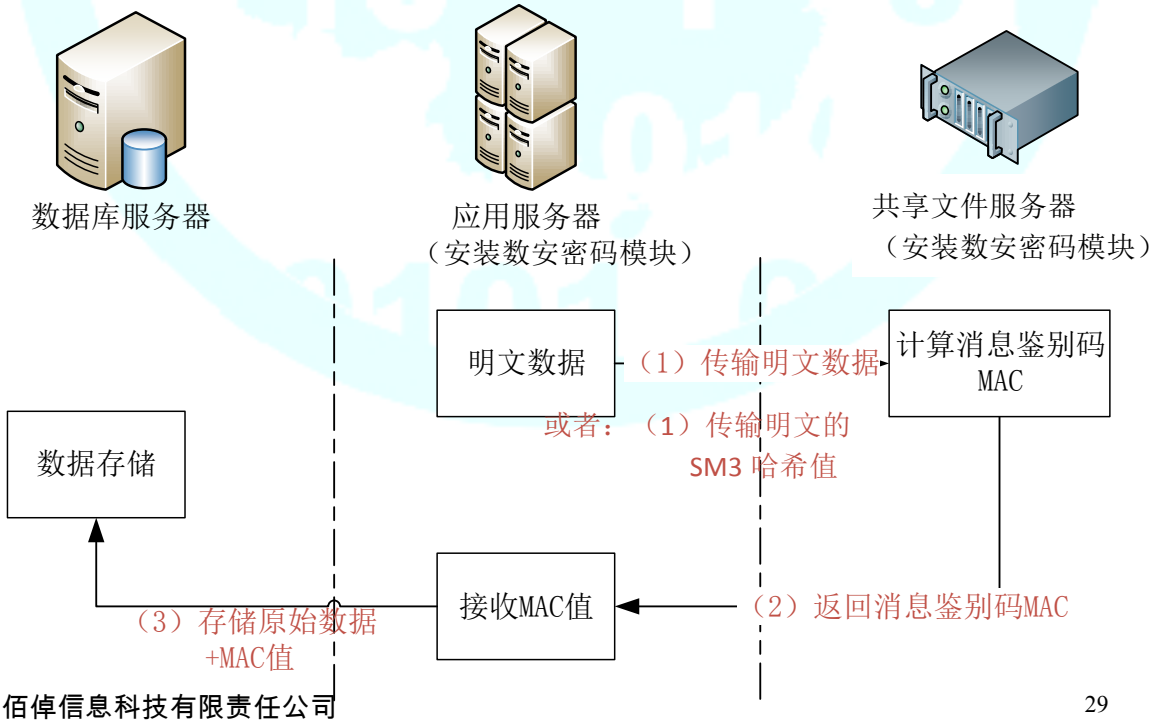


图 5-6　数据解密流程

数据解密流程：

后续被授权程序要访问被加密的数据文件时，密钥索引会被读到内核模块使用同样的逻辑（数据加密时）再次生成密钥，然后使用此密钥对文件进行透明解密。

5.3.3.2 数据完整性保护流程



或者：（3）原始数据的 SM3 哈希+MAC 值

图 5-7 MAC 计算流程

具体业务流程如下：

(1)应用系统将收到的明文数据上传到装有数安密码模块的文件服务器。

(2)文件服务器上的数安密码模块对关键的数据进行完整性保护：计算其 MAC 值，并且在任何读取操作前进行文件完整性验证，确保文件的使用完整性。

5.3.3.3 数据完整性验证流程

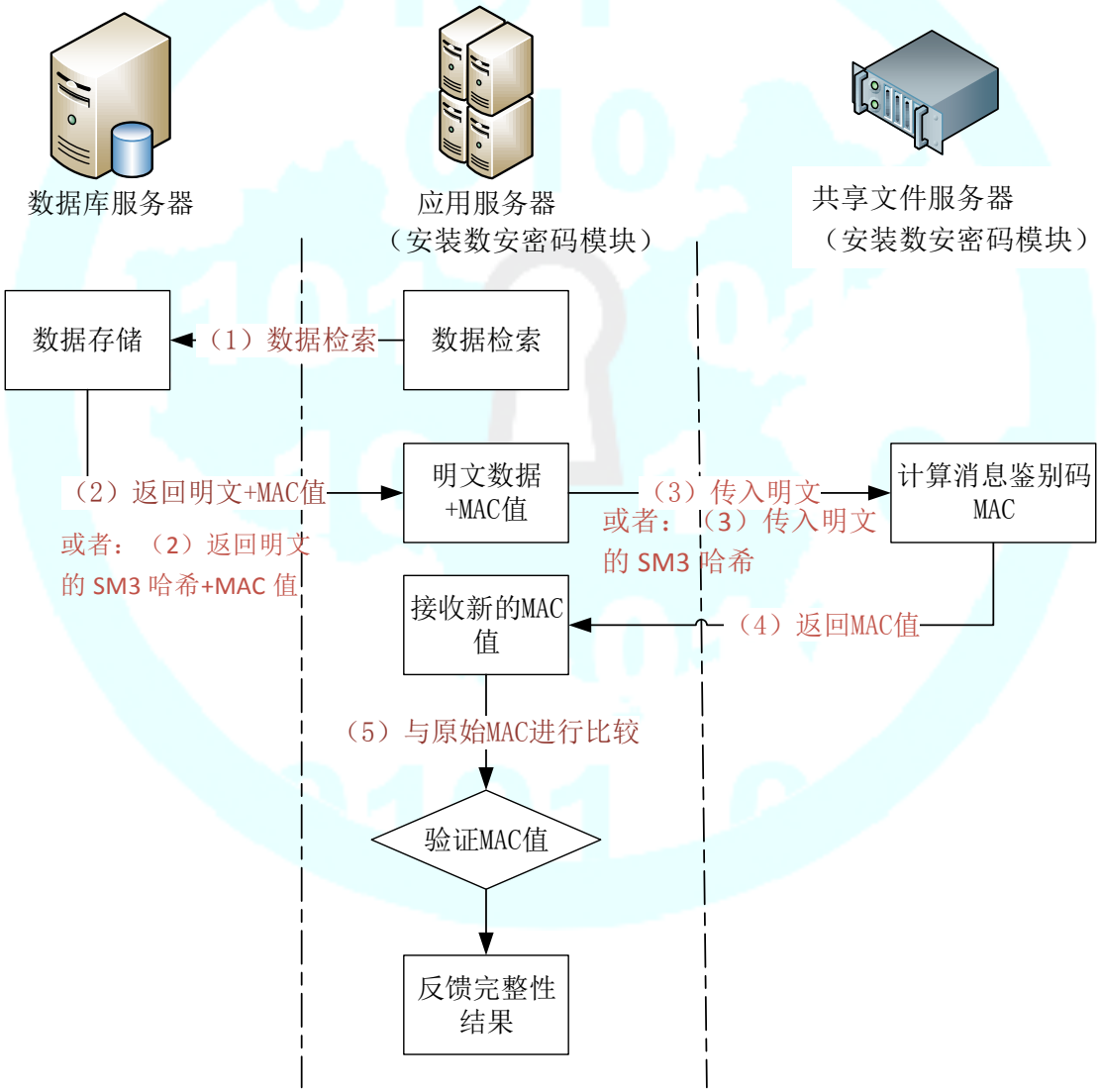


图 5-8 MAC 验证流程

具体业务流程如下：

(1)应用系统检索数据库中所需数据，得到原始明文和 MAC 值。

(2)应用系统将明文和 MAC 传递至装有数安密码模块的文件服务器。

(3)密码模块对原始明文进行 MAC 计算并且和相应的 MAC 值进行对比。

(4)比对一致，则原始数据未被篡改；比对不一致，则原始数据被篡改。

5.3.4 业务系统改造

5.3.4.1 敏感数据加密改造

本项目中，敏感数据主要为结构化数据，通过数据表的方式，存储在数据库服务器中。敏感数据主要包括 :各业务系统用户登录口令、用户访问控制权限以及其他重要数据等。

敏感数据加密由操作系统级透明的数安密码模块完成。敏感数据加密遵循不影响正常业务使用的前提下，进行敏感数据加密保护，实现存储在数据库敏感信息的数据文件的加密。敏感数据加解密服务流程见 5.3.3。

第 6 章 标准配置清单

序号	产品名称	品牌型号	数量	备注
1	数字证书认证系统		2	
2	密钥管理系统		2	
3	佰倬密码服务模块		4	

4	时间戳服务器		4	
5	签名验签服务器		4	
6	电子签章系统		4	
7	SSL VPN安全网关		4	
8	IPSec VPN安全网关		10	
9	手机盾系统		2套	
10	智能密码钥匙		若干	

第 7 章 方案优势

- 软硬结合 部署灵活，应用改造较少。
- 覆盖所有高风险项
- 满足不同的得分要求
- 产品符合国密要求并拥有《商用密码产品认证证书》
- 符合未来《数据安全法》落地细则--《网络数据安全管理条例》关于加密、访问控制的要求
- 同时满足等保 2.0 中通用要求--安全计算环境、可信验证的相关要求