北京商用密码行业协会
Beijing Commercial Cryptography Industry Association

北京商用密码应用方案集锦

北京商用密码行业协会

2019 年 9 月

前言

没有网络安全就没有国家安全。密码是网络安全的核心支撑，是构建网络信任体系的重要基石，是保护国家安全的战略性资源。党中央高度重视密码工作。近年来，中央办公厅、国务院办公厅多次印发通知，就金融及重要领域的密码应用作出部署。

为积极响应建设网络强国的号召，落实国家密码管理局相关指示精神，促进密码应用在国家关键信息基础设施和重要系统的落地，为《密码法》的实施做好准备，北京商用密码行业协会特组织了 2019 年商用密码应用典型方案征集与评选活动。

此次活动得到了北京市国密局领导的大力支持，方案征集得到了协会各成员单位的积极响应，经过筛选、修改和专家评审，最终形成了本方案集锦。本方案集锦涵盖了金融领域、能源领域、水利/自然资源领域、国防和工业领域、公共通信领域、交通领域、公共服务领域、电子政务领域等多个领域的密码应用解决方案。每个方案的内容主要包括概述、需求分析、方案架构、方案特色、适用领域、企业分工和应用案例等部分。

北京商用密码行业协会以宣传和普及商用密码，推动首都商用密码产业发展，实现资源共享，加强行业自律，提升我国信息安全水平和促进首都经济社会发展为宗旨。协会同时也是商用密码供需双方沟通的平台和桥梁，希望本方案集锦能够为推进优秀密码应用解决方案的落地实施，保障各行业网络信息安全尽到绵薄之力。如此，便不负初心！

感谢

北京市密码管理局领导的支持与帮助！

杨恒亮、于佳、何德彪、张大伟、孔凡玉等专家的方案审查与指导！

目 录

政府行业

电子政务密码应用解决方案

1. 概述

国家密码管理局在《关于做好公钥密码算法升级工作的函》中要去 2011 年 7 月 1 日以后建立并使用公钥密码的信息系统，应当使用 SM2 算法；以建设完成的系统，应尽快进行系统升级，使用 SM2 算法。对于数字证书的使用应符合《深圳市电子公共服务数字证书使用技术指南》要求。

中办、国办联合印发的关于《金融和重要领域密码应用与创新发展工作规划（2018-2022）》（厅字[2018]36 号）中，在重点行业进行商用密码和产品使用做出规划性指导意见。

2. 需求分析

目前，CA 中心只支持 RSA 国密通用密码算法，在此基础上建立的数字证书身份认证、加密传输等密码保护措施存在安全风险。需建立一套自主、可控并且安全的密钥基础支撑平台，以此展开对电子政务数据加密传输、无纸化办公、数据安全存储、电子回执、电子审批等各个密码应用环节，达到整体的机密性、完整性、可用性、可控性、不可否认性以及责任回溯。

3. 方案架构

3.1 技术架构

可采用自建 CA 方式，为整个体系应用提供国密数字证书来源，并部署密码安全产品为上层应用系统应用支撑，完成电子回执、电子审批，互联网申报和无纸化办公的全电子化方式的密码应用。

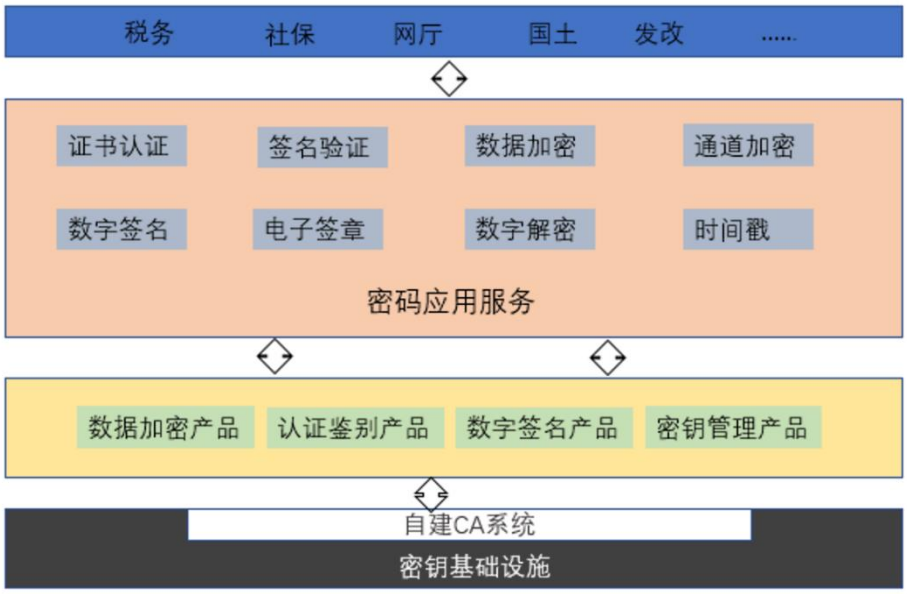


图 3-1 方案架构图

3.2 产品部署图

分为互联网区、DMZ 区和核心业务区三个部分，其中 CA 中心部署在核心业务区中的安全区。互联网区客户端安装支持国密算法的浏览器，部分企业用户还需采用 U-KEY 方式经过互联网通道完成双向身份认证。DMZ 区部署 SSL 应用安全网关和用户建立端到端的安全隧道。核心业务区部署 CA 中心，签名验签服务器和电子印章服务器并和业务系统完成业务接口对接。推荐密码产品采用双机部署方式保障业务的高可用和冗余，减少单点故障风险。

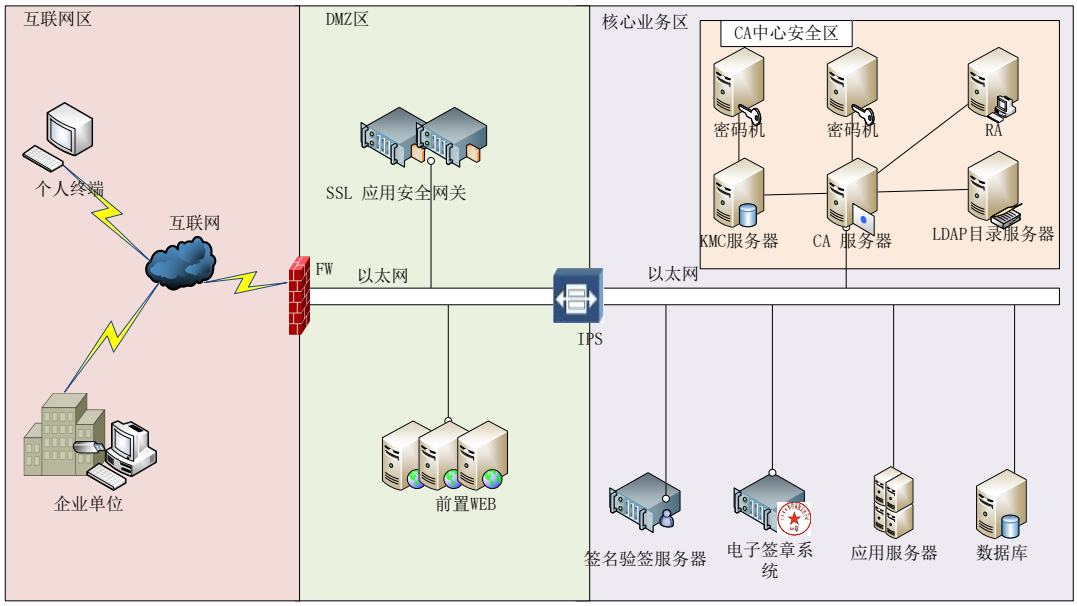


图 3-2 产品部署图

3.3 主要功能

数据安全传输。适配国密算法的浏览器，实现双向身份认证和基于国密算法建立 SSL/TLS 安全通道，保障数据交互的机密性和完整性。

可信国密数字证书应用。签名验签服务器验证数字证书的有效性和合法性，结合电子签章系统管理可视电子印章的使用，对敏感数据和电子单证存档，保障整体业务数据的公信力、不可否认性和鉴别。

3.4 主要技术指标

本方案主要达到以下技术指标：

建设基于 SM2 系列的数字证书应用支撑平台，全方位提升数据的加密传输、安全存储、可回溯以及业务单证的采信。

4. 方案特色

安全传输、服务高可靠。SSL 应用安全网关具备硬件加速模块和负载均衡功能附以 HTTP 压缩 WEB 高速缓存功能，提供高性能的应用支撑。方案采用双机 HA 部署方式，保障业务的冗余，避免单点故障，全面提升客户体验。

数据安全。在身份认证、数字签名、签名验证和电子签章的可视表现，解决了电子业务单证的完整性、公信力、不可否认性，并可对重要数据、电子业务单证进行加密存储，便于责任回溯。

自主、可控。本方案推荐采用自建 CA 基础密钥设施方式，可以根据自身业务需要合理进行调整。

经济、可行。一次性建设，再无其他证书方式逐年续费；本方案产品和方案设计参考国家相关规范文档，合规、可靠、易部署。

5. 适用领域

本方案主要适用工商局、人社厅（局）的互联网申报、电子回执、电子审批、

办公系统单点登录以及办事窗口场景，同时适用于税务、网厅、国土、发改委等类似的电子政务场景。

6. 企业分工

产商名称	职责	产品	国密型号	适用场景
北京信安世纪科技股份有限公司	提供国密改造方案、实施、安全产品	电子签章系统	SFT1901 电子签章系统	审批、电子回执、无纸化窗口
		密钥管理系统	SYT1902 密钥管理系统	自建 CA 中心
		数字证书系统	SZT1901 数字证书认证系统	
		SSL 安全网关	SJJ1515 SSL VPN 安全网关	申报、查询、HTTPS 的 B/S 架构等
		签/验签服务器	SRJ1904 签名验签服务器	
北京海泰方圆科技股份有限公司	提供国密专用浏览器、USBKEY	安全浏览器	SHM1602-G 安全浏览器密码模块	
		多算法只能密码钥匙	SJK1110-G 智能密码钥匙	
应用系统开发商	浏览器兼容方案	各相关应用系统	不涉及	

7. 应用案例

湖北省测绘地理信息局

湖南省工商局

北京信安世纪科技股份有限公司

联系人：邵素芬　　康茹

电　话：010-68025518-8118　010-68025518-8531

电子政务智能应用安全接入解决方案

1. 概述

1.1 建设背景

电子政务服务平台作为政府机构对外交流，以及政府内部办公的信息化服务平台，既可以帮助公众快速、稳定办理需求业务，还可以帮助机关用户提高工作效率。可能的业务系统包含电子政务门户系统、办公内网系统、远程报件系统、公文传输系统等多种系统。所有业务系统相对独立，但是随着业务的不断发展，信息化平台的不断完善，现有业务系统的业务安全性、系统稳定性及对外服务的无间断性，成为了需要考虑的问题。

随着移动设备产品的飞速发展，智能手机、平板电脑在移动办公业务上的应用已经成为一种发展趋势。如何对移动设备、移动应用、移动文档进行集中管理和控制，移动数据的安全如何得到保障，目前，已成为安全管理的首要问题。

为个人消费者设计的智能手机和平板电脑正在不断被用于承载关键业务及核心应用，使用移动设备访问内部信息，虽然提高了办公效率，但是也会给内网带来很多安全隐患，因此，如何保护敏感信息并确保连接安全变得日趋重要，这就要求能够应用 IT 策略及规范管理这些设备，并且提供安全的接入通道及统一认证门户。

1.2 安全目标

本案的建设目标是在国家相关法规和标准的指导下，结合项目需求分析，完成从人员管理，PC、智能终端管理，应用管理与授权，到数据加密管理，通信加密管理，单点登录等，主要解决用户的智能应用在新的计算环境下的问题及安全隐患，通过多种安全手段的智能互动，实现云（管理端）、管（安全通道）、端（智能终端）的业务安全。

1.3 设计依据

本案参照的信息安全标准规范包括：

- 中华人民共和国密码行业标准《GM/T 0022-2014 IPSec VPN 技术规范》
- 中华人民共和国密码行业标准 《GM/T 0024-2014 SSL VPN 技术规范》
- 安全断言标记语言：SAML
- 权限策略交换标准:OASIS（结构化信息标准促进组织）标准
- 权限管理标准：RBAC
- 基于角色的访问控制:ANSI/INCITS 359-2004 标准
- 目录访问协议：LDAP v2/v3
- 轻型目录访问协议：RFC 1777 V2 版和 RFC 2251 标准
- 安全套接字层：RFC2246 标准
- 公钥密码标准：X.509

本案借鉴的其他信息安全标准包括：

- GB/T 22080-2008（idt ISO/IEC 27001:2005）《信息技术 安全技术 信息安全管理体系要求》
- GB/T 22081-2008（idt ISO/IEC 27002:2005）《信息技术 安全技术 信息安全管理实用准则》
- ISO/IEC 13335《信息技术 安全技术 信息技术安全管理指南》
- IATF《信息保障技术框架》
- 《信息安全等级保护管理办法》
- 《企业内部控制基本规范》
- 《中华人民共和国电子签名法》
- 《GW0202-2014 国家电子政务外网安全接入平台技术规范》

2. 现状及需求分析

2.1 现状分析

（1）安全互联需求

政务系统在通过互联网向公众开放时，往往有对外开放服务端口，这为互联

网上的不法分子提供了扫描和攻击的入口，导致业务存在被攻击的风险，需要提供安全可靠的通讯链路。

从技术上需要实现移动安全、通讯安全、认证安全，从国家的政策法规的角度，需要采用国家密码管理局（以下简称国密局）的指定密码算法来实现。

（2） 统一管理需求

随着信息化的不断深入和普及，使日常办公更加方便、简单，最直接的目标提高了工作效率。特别是针对一些窗口性行业，极大地提升了服务品牌。但是，对于业务的信息化管理，提出了严峻的挑战，比如信息系统的复杂和多样性、共享性、安全性等一系列的问题，使管理者每天花费大量的时间进行系统管理和维护，并且不断的投入人力和资源来保障，结果还是存在管理漏洞和安全风险。如何能有效地降低安全风险，提高管理能力是对管理者最大的考验。

（3）移动管理需求

业务系统对外开放本身导致大量移动设备进入信息化系统，移动设备操作系统和硬件类型繁多，无法完成系统化的管理，设备的维护和查询十分不便。设备的移动化特性给网络的安全管理带来了严峻的考验，设备丢失或人员离职给内网的数据安全带来的及大安全隐患。设备的使用者大多工作地点不固定，管理员难以对监控移动设备的使用状态，难以保证移动设备被正常使用。应用分发渠道和来源让移动设备处在一个保护极其脆弱的环境；安全漏洞的隐患，给不法分子带来了可乘之机。

（4）强身份认证需求

在进行业务访问时面临着多种安全问题，这些问题包括信息的保密性、完整性、抗抵赖、身份鉴别和授权等等。目前解决电子政务安全问题的最佳手段是多因子认证，并根据等保 2.0 的要求采用国产密码技术进行安全保障。

国产密码技术是指能够实现商用密码算法的加密、解密和认证等功能的技术，即国密局指定的商用密码技术。目前该技术的应用领域十分广泛，主要用于对不涉及国家秘密内容但又具有敏感性的内部信息、行政事务信息、经济信息等进行加密保护。

2.2 需求分析

综合上述分析，用户需求为以下几点：

- 能够保证可信局域网和移动用户安全快捷地与业务局域网互访。
- 数据在 Internet 上传输时应保证足够的安全。
- 实现业务资源整合
- 提供统一身份管理
- 实现安全策略集中管理
- 实现移动设备管理
- 实现移动应用管理
- 实现移动内容管理
- 实现移动安全管理

基于上述需求，天融信充分考虑终端安全、接入安全、用户安全、边界安全、统一接入、应用安全等技术，提供基于国密协议和国密算法的智能应用安全接入解决方案。

2.3 整体架构

图 2-1 架构图

3. 方案综述

3.1 部署说明

整体方案拓扑如下图：

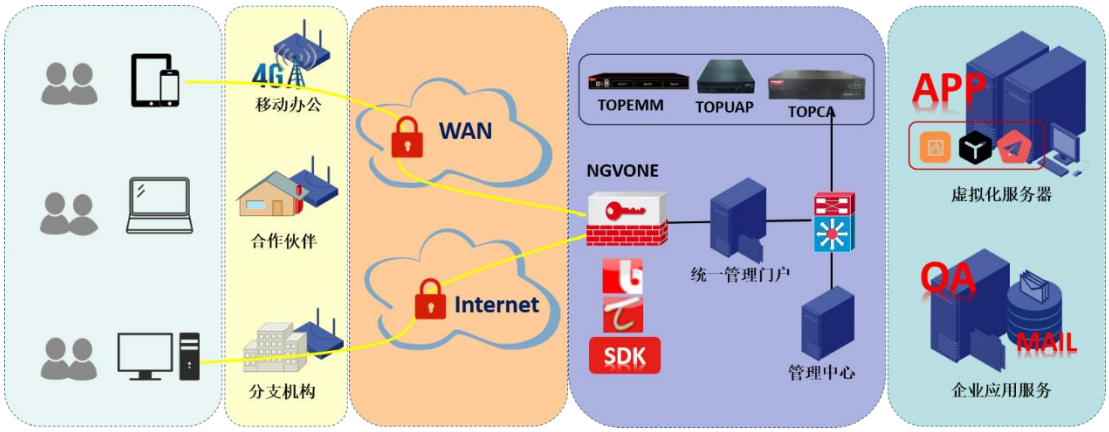


图 3-1 方案部署图

（1）本案政务服务中心集中了各类业务应用服务器，是应用的核心所在，对外提供各类政务服务；

（2）政务服务中心部署 VPN 网关，提供远程接入服务，在远程数据传输上实现安全保密需求，解决用户数据在互联网上传输安全问题。VPN 是安全接入的首选技术，既能降低用户接入成本，又能达到类似专网的效果；VPN 网关上采用国密局认可的对称密码算法（SM1/SM4）对传输过程进行加密，并采用 SM2 证书进行身份认证，并启用 SM3 算法校验传输过程中的数据，完整的国密算法套件可对用户的业务数据进行量化；

（3）对于用户应用系统在智能终端的使用情况，部署 EMM 安全网关进行有效管控，对设备（时间、地点、状态）、应用（推送、更新、使用）、内容、安全进行统一管理，达到安全使用智能终端的目的；EMM 在终端采用沙箱技术，对应用环境进行隔离，并可选择采用国密算法（SM1/SM4）对本地数据进行加密保护；

（4）用户内网部署 CA 数字证书系统，为终端接入、应用身份认证提供强身份认证服务；电子证书系统采用国密 SM2 证书；

（5）用户业务应用系统账号、VPN 账号、EMM 账号等均采用天融信统一接入平台进行身份认证，实现一次登录，处处识别，方便用户在智能终端上的使

用，无论是智能终端上的 UAP 还是电脑端的应用程序，只需输入一次主账号认证凭证（主账号为 VPN 账号，从账号为 EMM 网关账号及各种业务系统账号），在后台的业务系统上均能智能识别用户身份，自动分配相应的权限；统一接入平台可使用国密证书作为主认证凭证，强化认证环节的安全性，整体安全认证性符合等保 2.0 中 8.1.4.1 所要求的身份鉴别等级；

（6）智能终端安装 EMM 客户端实现移动设备管理，配合 EMM 安全容器套件（已集成 VPN 客户端），在使用 APP 时自动创建安全通道，保护用户数据链路，并将本地数据进行加密保存（可选择国际标准算法或者国密标准算法），创建安全通道、保存安全数据的过程对用户完全透明，减少用户在智能终端上的操作，简化用户认证流程。

3.2 技术指标

本案主要性能指标如下：

10000 点安全接入性能；

10000 个用户管理能力；

10000 点移动终端管理；

10000 个安全智能钥匙（含 10000 个数字证书）。

主要产品清单如下：

序号	产品名称	产品说明
1	VPN 系统	实现基于国密 SM1/SM2/SM3/SM4 算法的安全通讯传输，细粒度的权限控制，可以和多种身份认证机制配合
2	安全认证网关	提供如下功能模块：1. 统一用户管理；2. 统一认证管理；3. 统一授权管理；4. 单点登录系统；5. 审计管理
3	移动安全管理	提供如下功能模块：1. 移动终端管理；2. 移动应用管理；3. 移动内容管理；4. 移动安全管理；5. 移动大数据展示平台
4	数字证书系统	实现证书注册、颁发、更新、注销、冻结等功能的证书全生命周期管理
5	智能密码钥匙	可提供 USB 形式和蓝牙形式

3.3 方案特色

本案主要拥有三大特色：智能化、安全性、开放性。

（1）智能化

各类设备、终端以及组件均能智能连接至方案体系中；客户的各种应用均能轻松授权传递，快捷展现在各类终端，实现应用一体化；同时还可以智能管理人员、认证策略、网关、智能终端、应用、体验优化、运营策略等。

（2）安全性

可以保障接入终端及接入链路的安全；安全桌面及安全门户保证客户各类应用隔离，实现应用保护；数据在传输过程会进行加密、同时本地数据存储也会加密。本案安全性主要由国产密码体系来进行保障，通过确认使用者（使用 SM2 证书）身份、将业务数据通过安全通道传输（使用国密协议、国密算法加密传输）、进行统一安全授权（将使用者身份通过令牌方式验证）、数据安全存储（采用国密算法保护）等方面的技术手段，将国产密码覆盖到本案使用场景的所有层面。

（3）开放性

拥有通过各类标准的接口，可以无缝对接各类设备与应用；各类应用可随意扩展接入在统一的架构中；可对接各种认证系统、应用系统、管理系统，智能终端等各类平台等。

3.4 方案收益

（1）移动安全

业务员轻松完成 APP 的安装和更新，随时随地 APP 做业务办理，提升工作效率的同时带给了客户全新的体验。

因为使用 EMM 使工作变得简单、便捷，节省了大量的人力和时间成本。

移动设备管理变得更规范，资产清点一目了然，设备使用和 APP 应用可视化、可分析。

（2）数据安全

使用灵活多变的认证手段满足不同用户需求，实现同一体系下不同的安全需求.

通过隧道技术、加解密技术、密钥管理技术、身份认证技术建立透明的 VPN 通道，传输安全得到保障。

VPN 通过标准化接口无缝对接应用系统，让用户在无感知的情况下使用多种终端（包括智能终端）实现安全通讯。

（3） 管理安全

从复杂的认证关系中总结出共同的认证凭证，简化了复杂的用户管理，为用户提供良好的用户体验。

将异构的信息系统构建可协同的信息通道，优化了信息系统的架构，实现多信息系统的和谐体验。

规范化业务认证流程，制定业务统一接入标准，优化业务认证通道。

4. 应用案例

单位	国家信息中心（国家电子政务外网管理中心）是国家发展和改革委员会直属事业单位。1986 年，为迎接世界信息技术革命挑战、适应我国改革发展形势需要，国务院批准建设国家经济信息系统并组建国家经济信息中心。1987 年 1 月 24 日，国家经济信息中心正式成立。1988 年 1 月 22 日，邓小平同志亲笔题名“国家信息中心”。作为以经济分析预测、信息化建设和大数据应用为特色的国家级决策咨询机构和国家电子政务公共服务平台，国家信息中心始终坚持以先进信息技术为手段，以信息资源开发为核心，以服务科学决策为使命，在围绕党中央、国务院和国家发展改革委以及各级政府部门提供宏观决策支持，推进国民经济和社会信息化发展方面发挥了重要的思想库和主力军作用。
难点	接入规模大，实施难度高，协调工作困难，并发量巨大。
天融信方案	天融信为国家信息中心量身定做解决方案，分区域分中心的制定上线时间表，并按照整体安全防护规划，对上线的业务系统与多种安全防护系统进行深度结合。
本案亮点	实现了多应用系统的国密安全防护策略，实现接入接入、认证安全、移动安全等安全需求。

影响	为电子政务工程在各省市推进落地起到示范作用，成为各地电子政务工程的标杆。

北京天融信网络安全技术有限公司

联系人：刘治平

电　话：13910294344

电子政务电子证照商用密码应用解决方案

1. 概述

2016 年 9 月，国务院关于加快推进“互联网+政务服务”工作的指导意见国发（〔2016〕55 号）的文件明确提出：“积极推动电子证照、电子公文、电子签章等在政务服务中的应用，开展网上验证核对，避免重复提交材料和循环证明”。

在开放的互联网环境中，电子扫描、图片技术的普及大大降低伪造电子证照、纸质证照的成本，进而存在假证假照泛滥现象。这种现象究其原因是证照的使用管理中防伪、真伪鉴别等存在问题，造成证照的可信度低。为此，亟需解决证照的可信问题，既提高政府办公效率，又为百姓提供了便捷的服务。

2. 需求分析

在无纸化、互联网的大环境下，电子证照的数据电文真实性、合法性存在若干风险：

- 电子证照数据电文的内容真实性无法认定

电子证照在表现形式上与纸质证照相同，相比传统纸质载体易于固化和展示，数据电文的无形性、多样性和易破坏性，无法保证其自身真实性。

- 电子凭据的效力认定

电子形式的凭据如何能承载原来纸质凭据的书证和物证效力，其证据效力如何等同于纸质单据，如何确保电子证照的合法性。

为解决电子证照的可信与真实性，在电子证照的基础上采取可靠电子签名技术实现对电子证照的签名，保障电子证照的真实性、可信性。电子证照没有数字签名就不具备法律效力，而电子证照的电子签名必须满足《电子签名法》的可靠电子签名要求，才能具备法津效力。

根据《电子签名法》第十四条规定：可靠的电子签名与手写签名或者盖章具有同等的法律效力。因此，在电子证照中使用基于可靠电子签名的可信签名技术，

实现对电子证照的电子签名，确保了可信电子证照的合法性。

3. 方案架构

3.1 技术架构

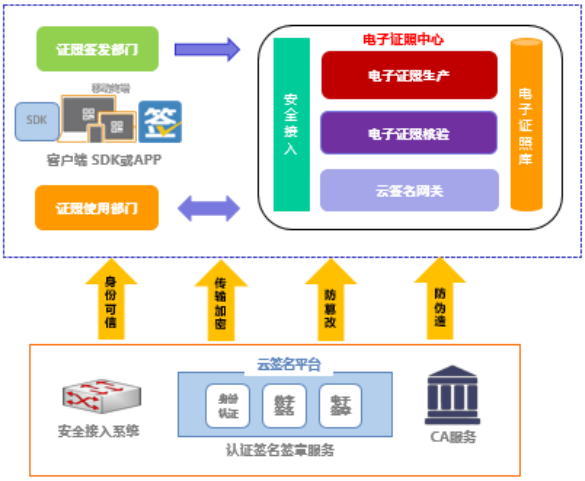


图 3-1 电子证照技术架构图

电子证照系统密码应用体系包含安全接入系统、云签名平台、CA 中心。其中云签名网关负责转发身份认证和签名请求，包含身份认证、数字签名、电子签章功能服务模块。身份认证功能服务模块采用密码云技术，为证照签发部门、证照使用部门、电子证照中心发放数字证书，解决电子证照参与各方的身份可信；数字签名服务模块将各部门发送的数据进行数字签名，解决数据来源不可靠等问题；电子签章服务模块采用电子印章技术，依据证照签发部门提供的证照数据，生成电子证照模板，并加盖电子印章。安全接入系统解决各接入部门与电子证照中心之间传输信息的机密性和完整性，防止非法窃取和篡改。

3.2 产品部署图

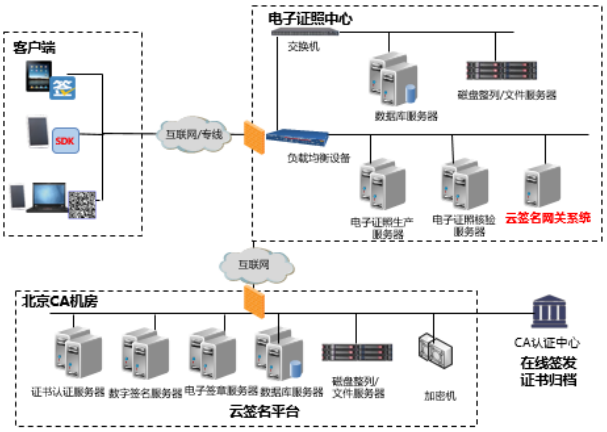


图 3-2 电子证照产品部署图

在电子证照中心部署云签名网关系统，客户端集成 SDK 安全组件包。客户端通过 SDK 安全组件包发起请求，通过云签名网关系统调用云签名平台（数字认证已建），调用云签名服务和云签章服务，实现电子证照生成时对数据进行电子签名，核验时数据签名验签。

3.3 主要功能

数字证书：提供基于移动端的手机证书生命周期服务。

身份认证：提供自然人、企业法人实名用户的身份认证功能。

数据签名：实现对电子证照数据的可靠电子签名。

电子签章：提供电子证照格式的电子签章功能。

可信二维码：提供电子证照附有可信二维码，实现证照可信。

3.4 主要技术指标

登录认证：500tps/秒；数据签名：500tps/秒。

证照电子签章盖章：100tps/秒；验章：500tps/秒。

4. 方案特色

电子证照建设中，采用密码云技术，应用建设无需购置密码设备，通过云签名网关系统使用云签名平台，提供专业的密码云签名和云签章服务。如在电子证

照版式文件上加盖电子印章，完成证照制作。

方案涉及的密码服务与产品，已获得国家密码局认可，并取得商用密码产品型号证书；电子签章采用国密 SM2、SM3 算法，电子证照支持专用阅读器、在线 WEB 方式验证电子证照数字签名,保障电子证照信息的真伪。

5. 适用领域

将电子签名技术与电子类证照文件相结合，实现电子类可信文件，在企业电子营业执照、残疾人电子证照、电子社保卡等各种证照类的应用领域适用。

6. 企业分工

本方案主要由数字认证提供方案设计、产品部署等工作。方案提供的产品清单如下：

序号	名称	提供单位	描述
1	电子证照系统	数字认证	实现各部门进驻、目录管理、发证管理、用证管理等功能。
2	电子证照库	数字认证	建设电子证照索引库、电子证照库，支撑电子证照的存储及调用。
3	云签名网关系统	数字认证	基于密码云的签名认证服务系统前置网关系统，提供电子证照签章、数字签名、身份认证功能。
4	云签名服务	数字认证	提供用户身份认证、数据签名、密钥管理等服务。
5	云签章服务	数字认证	提供电子证照签章、电子证照印章管理等服务。

7. 应用案例

- 北京政务服务中心电子证照项目

建设了北京市电子证照系统、电子证照信息库，实现了北京市网上政务服务大厅、行政审批管理等系统的电子证照数据信息共享。

- 中国残联电子证照项目

为中国残联建设了中国残联电子证照系统、密钥系统，为全国有 3000 多万残疾人颁发电子证照。

- 北京市残联

北京市残疾人在公园门票、证照扫描、公交乘车、辅助医疗等多种实际社会活动已便利地应用了残联人证，享受了残疾人应有的社会待遇。

北京数字认证股份有限公司

联系人：任家萍

电　话：17801108503

电子政务电子印章系统密码应用解决方案

1. 概述

电子印章是密码技术的重要应用之一，国发〔2018〕27 号《国务院关于加快推进全国一体化在线政务服务平台建设的指导意见》指出“应用基于商用密码的数字签名等技术，依托国家政务服务平台建设权威、规范、可信的国家统一电子印章系统。各地区和国务院有关部门使用国家统一电子印章制章系统制发电子印章”。国办函〔2018〕59 号《国务院办公厅关于切实做好各地区各部门政务服务平台与国家政务服务平台对接工作的通知》要求：“各省（自治区、直辖市）和国务院有关部门要按照全国一体化在线政务服务平台统一标准规范和相关工作的要求，加快建设完善本地区本部门的政务服务平台及与国家政务服务平台的深度对接融合”。要求按照一体化平台电子印章相关标准规范，完成与国家政务服务平台统一电子印章系统对接。2019 年 4 月 26 日中华人民共和国国务院令第 716 号第九条国家建立权威、规范、可信的统一电子印章系统。国务院有关部门、地方人民政府及其有关部门使用国家统一电子印章系统制发的电子印章。电子印章与实物印章具有同等法律效力，加盖电子印章的电子材料合法有效。第十一条除法律、行政法规另有规定外，电子证照和加盖电子印章的电子材料可以作为办理政务服务事项的依据。

2. 需求分析

首先对省级机构电子印章系统的现状进行分析，基本包括以下几种情况。

没有建设相关系统

省级机构没有建设电子印章平台，没有电子印章应用；

已经自建部分系统

省级机构、省级下属机构在部分业务系统中，以办公信息化、认证凭据等需求，自建了一些电子印章系统。

系统应用范围有限

已经自建的电子印章系统多数是以信息化系统建设和管理模式进行，由各自信息化部门直接为相关业务服务系统生成电子印章，电子印章使用范围也只限于各自的业务体系中，离开本体系无法被认可。

电子印章制发机制自行设置

已经自建的电子印章制作系统，多由各自信息化部门直接为其他部门制发电子印章。这与实物印章的制发、备案、管理的规定和流程有很大差异。

技术规范各自表述

已建系统中有部分采用商密标准，部分采用本行业定义的规范，有的按照自己业务需要定义了技术要求，相互间差异很大，很难实现互认互通。

针对上述问题为满足国家一体化在线服务的需要，建设省级一体化服务平台电子印章系统的应该实现一下要求：

需要设计与建设省级电子印章系统，为实现 27 号文中要求的全国互联网+电子政务的互联互通，对于没有建设相关系统的省级机构需要进行规划和建设，对于已建系统需要完善和改造。

需要与政务服务统一电子印章系统对接，通过向政务服务统一电子印章测试系统注册，并通过测试验证实现与国家平台的互认互验，打通各自壁垒，形成一体化架构。

需要统一技术规范，以实现国家政务服务平台与各省级平台的互通，包括电子印章格式、电子签章格式、数字证书内容、系统架构、系统对接接口及其协议。

3. 方案架构

3.1 技术架构

国家平台中的信任支撑系统、电子印章管理系统、国家电子印章发布系统担负着与各省级系统的对接服务功能。信任支撑系统为各省级系统提供治安密钥下发、制章备案、唯一赋码等对接服务；电子印章管理系统用于各省级系统选择的数字认证系统的根证书注册，为系统接入身份认证和电子印章制发的证书确认提供服务；国家电子印章发布系统汇聚了全国政务电子印章状态信息，验证签章时

刻该电子印章是否有效。

3.2 产品部署图

北京国脉信安科技有限公司的金玺电子签章系统是国家政务服务平台统一电子印章系统的中标和建设产品，这里以它为例介绍一下系统的部署情况。

（1）电子印章制作系统

制发符合国家政务服务平台规范的电子印章；

与国家统一电子系统系统对接，实现国家统一赋码、下发治安密钥，向公安系统报备制发的电子印章信息；

向状态发布系统发布制发的电子印章状态信息。

一个省级地区如果存在多个电子印章制作系统，为满足国家平台只对接省级一个平台的要求，其部署结构如下：

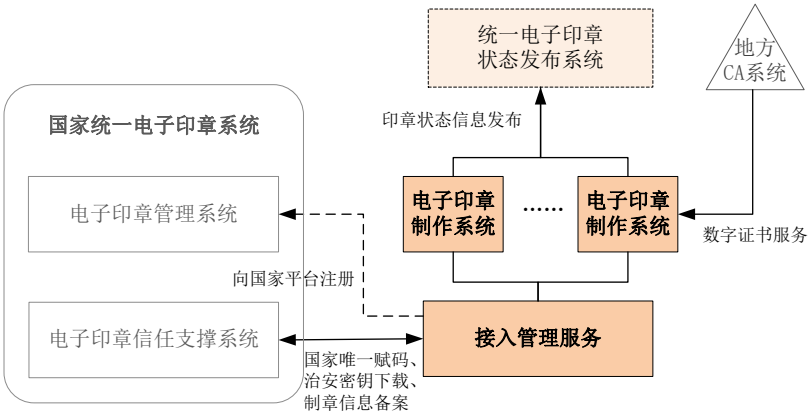


图 3-1 对接部署图

该部署结构与国家平台接入各省级系统的架构一致。通过接入管理服务实现多制章系统与国家平台的接入、认证、管理。

（2）统一电子印章发布系统

为省级范围公示已经制发的电子印章的各种状态信息；

为各业务系统提供电子印章状态信息的查询、下载服务；

对电子印章状态进行依法变更；

向国家平台统一电子印章系统的状态发布系统同步行业印章状态信息。

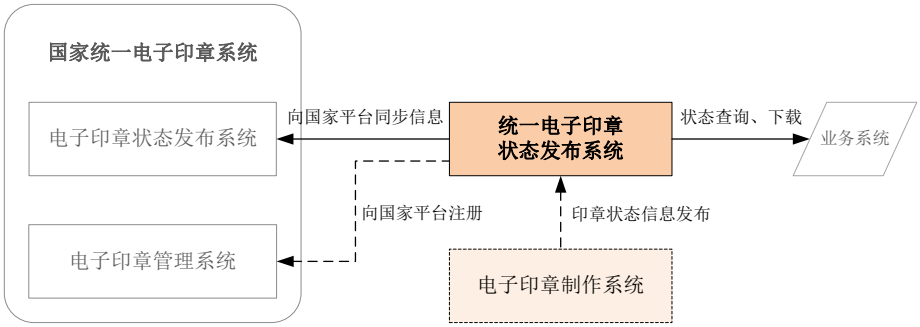


图 3-2 同步流程

（3）集中式用章系统

实现电子印章的集中管理，利用密码机、签名服务器等密码设备，通过建立在 PKI 体系下有着完整身份认证、访问控制、责任认定机制的用章系统，实现全流程安全管理；

面向不同业务系统，利用 API 接口方式提供标准的签章服务；

与用户管理向结合实现电子印章多种场景定制，以及对用章过程的监督认证；

基于 WEB 客户端技术支持分散模式下，统一印章使用。

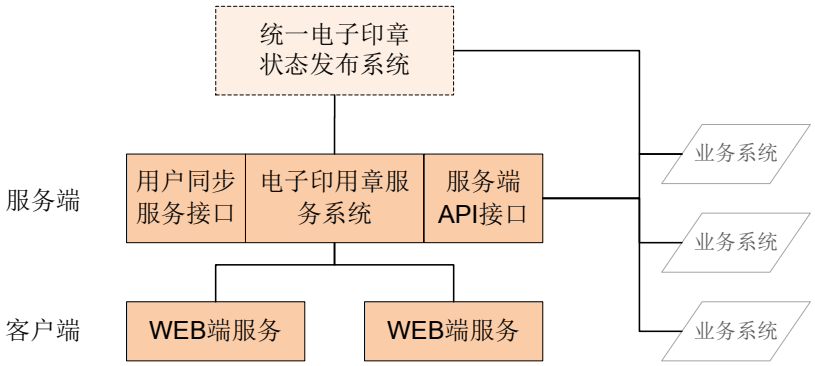


图 3-3 web 客户端分散模式图

（4）分散式用章系统

面向分散使用电子印章的场景，通过 UKey 方式直接在客户端为电子文件盖章；

通过独立用章工具实现离线或在线用章服务；

基于 WEB 客户端技术实现在线用章服务。

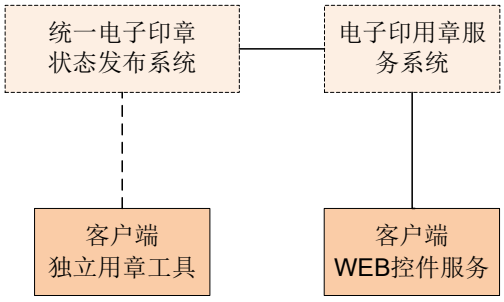


图 3-4 在线用章服务

3.3 主要功能

金玺电子印章制章系统的主要功能：

（1） 系统初始化管理：满足等保三级要求；

（2） 电子印章制作申请：通过页面按照公安治安管理要求，填报申请信息，提交制作所需数据内容；

（3） 电子印章下载、撤销、续期：将制发的电子印章写入 USBKey 或导入密码设备中，对制作有误的电子印章及时销毁，延长电子印章有效期；

（4） 证书申请：向 CA 系统申请并获取电子印章数字证书；

（5） 电子印章发布：向电子印章发布系统发布印章状态信息；

（6） 制作管理：日志查看、印章信息查询；

（7） 治安密钥下载：公安治安密钥的下载；

金玺电子印章发布系统的主要功能：

（1） 系统初始化管理：满足等保三级要求；

（2） 电子印章状态查询：根据盖章时间，在线获取电子印章当时是否有效的状态；

（3） 电子印章状态下载：下载电子印章状态列表，为本地查询使用；

（4） 电子印章状态变更：电子印章管理者在无需组织机构树前提下，能够准确对其管辖范围内的电子印章状态进行有效无效的状态变更，且有完整签名认证；

（5） 发布管理：日志查看、印章历史记录信息查询。

金玺电子印章用章系统的主要功能：

（1） 系统初始化管理：满足等保三级要求；

（2） 基于 PKI 技术操作员认证和授权管理；

（3） 用户与组织架构管理：提供自建与外部同步方式；

（4） 电子印章管理：电子印章的增删与分配；

（5） 用章授权管理：用章申请与审批；

（6） 批量签章、联合签章、骑缝章：服务端接口模式签章，同时签盖多个电子印章，仿效实物印章的骑缝章盖章；

（7） 模板管理：为不同业务提供盖章模板的定制和使用；

（8） 流程管理：为不同业务提供用章流程的设置；

（9） 指定位置、关键字盖章：基于坐标位、关键字位置盖章；

（10） 自由签章：支持 OFD、PDF 数据格式任意位置签章；

（11） 公安治安检查：支持公安机构对治安密钥的审查。

3.4 主要技术指标

（1） 标准支持能力：支持 C0119《国家政务服务平台 统一电子印章 签章技术要求》规范，C0120《国家政务服务平台 统一电子印章 印章技术要求》，C0121《国家政务服务平台 统一电子印章 接入测试方法》，C0122《国家政务服务平台 统一电子印章 系统接口要求》，同时支持 GM/T 0031-2014《电子签章密码应用技术规范》规范、GB/T 33481-2016《党政机关电子印章应用规范》。

（2） 多 CA 支持：电子印章制作系统同时支持 42 家 CA 根；

（3） 签章性能：230 次/秒；

（4） 互认性能：支持 32 个省/自治区/直辖市和所有部委接入国家平台的电子印章的互认互验。

（5） 电子印章管理：百万级；

（6） 电子文件支持：OFD 和 PDF 版式格式，以及 WORD、WPS 等流式文档；

（7） 环境支持：SFT1806 支持主流环境，SFT1806-G 支持安可环境。

4. 方案特色

（1）满足各省级单位统一电子印章建设

本方案能够支持全国各省级单位建设电子印章系统，并实现与国家平台对接，满足互联网+电子政务的需要，满足 27 号文要求。

（2）满足全国电子印章的互认互通

本方案能够支持全国统一的电子印章系统中，所有注册的数字证书互认互验，实现全国电子印章的互认互通，确保电子印章权威性

（3）满足电子政务和安可化建设需求

支持国内主要安可环境，支持政务服务中各种电子印章应用，可用于政府体系，也可用于社会体系。

（4）满足云平台建设部署需求

金玺电子签章系统的架构支持云架构，能够支持公有云和私有云。

5. 适用领域

（1）电子政务中的应用

电子证照

《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》（国办发〔2016〕108 号）要求：

“电子证照文件格式采用版式文件格式，文件内容包含与纸质证照相同比例的证照底图、电子证照的照面信息、电子证照元数据信息、签发单位的电子印章与对电子证照文件内容进行的数字签名”。

电子证照应用

电子公文

《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55 号）指出：

“积极推动电子证照、电子公文、电子签章等在政务服务中的应用”。

在电子公文的应用

（2）电子商务中的应用

电子合同

电子合同，又称电子商务合同，根据联合国国际贸易法委员会《电子商务示范法》以及世界各国颁布的电子交易法，同时结合我国《合同法》的有关规定，电子合同可以界定为：电子合同是双方或多方当事人之间通过电子信息网络以电子的形式达成的设立、变更、终止财产性民事权利义务关系的协议。电子印章可为电子印章的合法性提供支撑。

长沙大宗商品电子交易中心有限公司文件

长沙大宗司发[2010]第2号

关于CP100815和MP100815电子合同上市交易公告

各交易商，各指定交收仓库：

本交易中心决定于2010年1月15日（星期五）推出CP100815和MP100815中远期电子合同上市交易，现将有关具体事项通知如下：

合约代码	商品名称	首日上市参考价（元/吨）	首日涨跌幅	上市日期	最后交易日	最后交收日
CP100815	远月白100815	2150	10%	2010.01.15	2010.08.13	2010.08.16
MP100815	远月白100815	2650	10%	2010.01.15	2010.08.13	2010.08.16

特此公告。

长沙大宗商品电子交易中心有限公司

二〇一〇年一月十五日

电子发票

电子发票是信息时代的产物，同普通发票一样，采用税务局统一发放的形式给商家使用，发票号码采用全国统一编码，采用统一防伪技术，分配给商家，在电子发票上附有电子税局、商家的电子印章确保电子发票的合法和有效性。

6. 企业分工

金玺电子签章系统是个开放的架构，既能够独立形成整套产品并实施部署，也能够与其他企业的产品共同满足用户需求。

系统厂商：

金玺电子签章系统包括：电子印章制作系统 、电子印章发布系统、电子印章应用系统。这三个部分是相互独立部署的，能够与不同厂商的产品共同形成有机整体。

密码厂商：

金玺电子签章系统中采用的密码设备包括：密码机、UKey 等，可以选用符合国密标准的任何厂商的密码设备，包括密码机、签名服务器、UKey。

环境厂商：

金玺电子签章系统支持安可环境，国产 CUP、操作系统、数据库、中间件、版式、整机等厂商都是金玺的支撑单位。

注：在安可测试时，金玺通过了 3 组安可环境的测试。

7. 应用案例

金玺电子签章系统已经部署到了许多应用中，近期的案例有：

（1）国家政务服务平台（一期）建设项目

2018 年 3 月北京国脉信安科技有限公司中标国家政务服务平台建设项目中统一电子印章系统建设项目，承担国家统一电子印章系统建设和项目中相关标准规范的编写。

（2）四川省、广东省、广西自治区、云南省、吉林省、重庆市一体化政务服务平台；

（3）工信部一体化政务服务平台；

（4）发改委能源局公文系统；

……

北京国脉信安科技有限公司

联系人：张禹

电　话：18611520718

政务云密码应用安全解决方案

1. 概述

随着云计算、大数据等新技术迅猛发展，引领新一轮科技革命和产业变革，深刻影响人类生产生活方式。云计算、大数据环境中，数据集中、虚拟化和多租户使用问题，使得用户数据面临更大安全风险，催生更高等级密码安全防护需求。根据国家等级保护及密码相关政策，结合《金融和重要领域密码应用与创新发展工作规划（2018-2022 年）》（中办、国办〔2018〕36 号）、《关于加强重要领域密码应用的指导意见》（中办、国办〔2015〕4 号）等相关要求，兴唐通信科技有限公司积极推进政务云平台密码应用落地，基于自主研发的云服务器密码机，创新性构建云密码服务资源池，为国家电子政务的全面云化提供自主可控的云密码服务和成熟的政务云密码应用解决方案。该方案从政务云平台和政务云租户两个维度，针对物理与环境安全、网络与通信安全、设备与计算安全以及应用与数据安全四个方面，提出了基于国产密码体系化的安全解决方案，并已在云上贵州等政务云平台进行了试点落地应用，具有较高推广及实际应用价值。

2. 需求分析

政务云平台汇集和处理大量的政府公共敏感数据、个人隐私等重要数据，存在被泄露或被盗用的风险。数据从采集、预处理、传输、存储、分析、共享到销毁全生命周期的各个环节都存在着安全风险，应对重要数据进行机密性、完整性保护，防止被非法查看、恶意篡改等。依据国家密码相关标准规范和技术要求，新建网络和信息系统应当采用国产密码进行保护，已建网络和信息系统应当进行密码国产化改造，政务云属于国产密码应用重点。政务云密码应用应遵循《GMT0054-2018 信息系统密码应用基本要求》与《信息安全技术 网络安全等级保护基本要求》，从物理与环境、网络与通信、设备与计算、应用与数据等几个方面进行密码防护设计。密码防护设计应满足云计算环境下平台方与租户方之

间的责任分担需求。

表 1 政务云密码应用需求分析

编号	需求种类	密码应用具体需求
1	物理和环境安全	应保障重要区域进入人员身份的真实性，同时确保门禁系统进出记录数据的完整性； 针对机房视频记录做真实性保护和完整性保护，防止视频等设备数据被篡改。
2	网络和通信安全	应在通信前基于密码技术对通信双方，包括平台管理人员、系统管理员（包括平台系统管理员、安全系统管理员等）、密钥管理员等与相关服务器之间，进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性； 应采用密码技术保障平台管理人员、系统管理员（包括平台系统管理员、安全系统管理员等）、密钥管理员等与相关服务器之间通信过程中重要数据的机密性和完整性。
3	设备和计算安全	为了防止网络身份假冒，可对登录云平台基础设施设备、云管理平台提供安全保护； 需要对登录网络设备及虚拟化网络设备的用户进行身份鉴别，防止用户身份冒用； 需要使用密码技术对系统资源访问控制信息进行完整性保护，防止访问控制信息遭篡改； 使用密码技术保证重要信息资源敏感标记的完整性，防止敏感标记被篡改。
4	应用和数据安全	平台数据和租户业务数据在传输、存储过程中有可能被篡改或窃取，可根据数据的等级和类型对数据实施机密性和完整性保护。 为防止用户登录的身份鉴别信息被截获、假冒或重用，可通过密码技术对登录的用户进行身份标识和鉴别，保证应用系统用户身份的真实性。政务云平台可利用现有的 CA 系统，构建统一的政务密码服务应用平台。政务云平台应接入已有 CA 机构，并提供便捷高效的证书服务。 为防止用户和管理员操作日志被篡改，因此需要采用密码手段对操作日志进行完整性保护。

3. 方案架构

3.1 技术架构

政务云密码应用技术架构，由政务云租户终端密码应用、政务云管道、政务

云平台密码应用、云平台运维管理和密码监管等五部分组成。如下图所示。

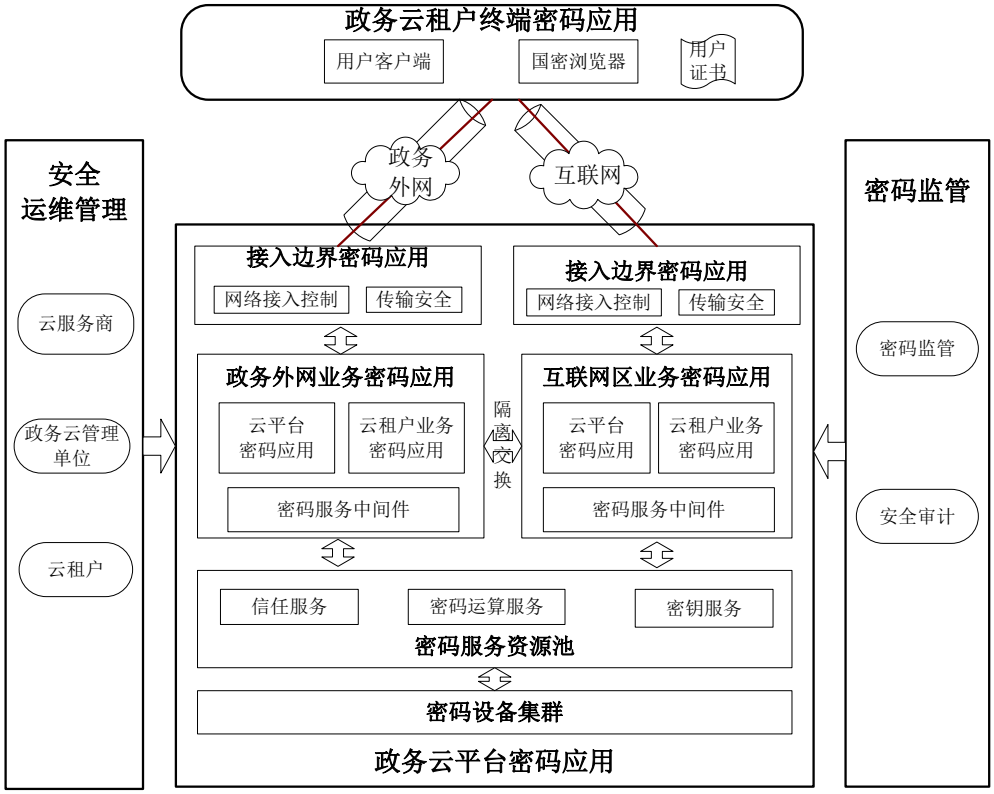


图 3-1 政务云密码应用技术架构

政务云租户终端密码应用指互联网租户终端和政务外网租户终端，负责为政务云用户提供各类业务应用操作功能；政务云管道指政务云租户终端与政务云平台之间的安全传输管道，承载租户终端用户到云平台间业务数据的传输保护；政务云平台密码应用指政务云平台上承载实现的各类密码应用服务，包括接入区边界密码应用、政务外网业务区密码应用和互联网业务区密码应用，通过密码设备集群和密码服务资源池为云平台自身和各云租户单位业务应用提供各类密码服务资源；密码监管指在密码主管部门设立密码监管平台，负责对政务云平台使用的密码设备进行密码监管与安全审计；安全运维管理是指通过云服务提供商、政务云管理单位和云租户三方角色划分与协同工作，保障政务云整体安全防护能力。

3.2 产品部署图

依据政务云密码应用技术架构，部署政务云密码应用产品，实现相应的密码防护功能。产品部署所下图所示。

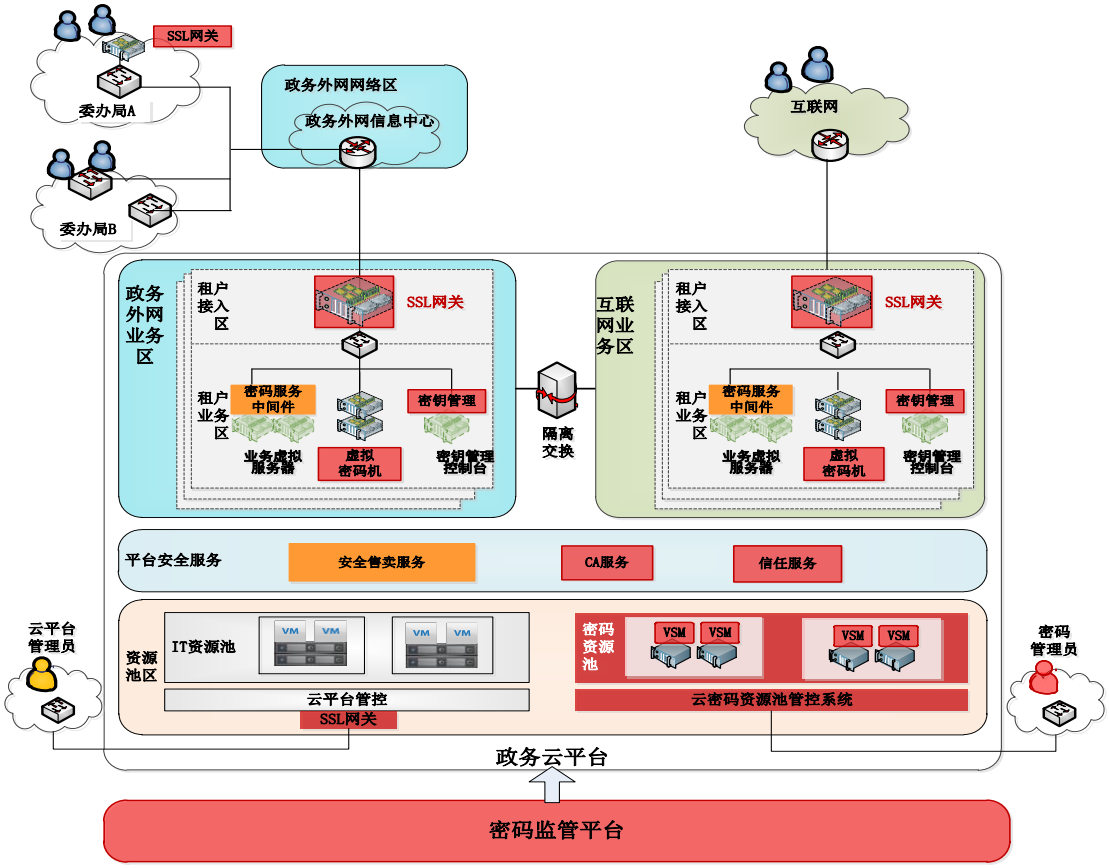


图 3-2 政务云密码应用产品部署图

租户区分为租户接入区和租户业务区。租户接入区为确保政务云租户的业务网络安全，部署 SSL 网关确保传输数据的密码保护。租户业务区可调用密码资源池的虚拟密码机，部署密钥管理系统及在业务虚拟服务器上部署密码服务中间件。密码服务中间件采用已有技术体系标准进行设计，实现政务云平台支撑的各类业务系统对密码服务资源池虚拟密码机的调用。

平台安全服务包括安全售卖服务、CA 服务和信任服务。安全售卖服务主要是提供租户密码安全套件供租户下载。租户密码安全套件是政务云平台为政务云租户提供其需要配置使用的各类密码安全组件，与政务云平台设计的密码机制和对外提供的密码服务配套使用。同时，在政务云平台政务外网区和互联网区分别部署 CA 服务和信任服务等典型支撑密码服务，其中 CA 服务实现数字证书发放、查验等功能，信任服务实现资源管理、授权认证与访问控制等功能。

平台资源池区是政务云平台的基础支撑，包括 IT 资源池、密码服务资源池、云平台管控和云密码资源池管控服务四部分。政务云平台自身密码防护体现在对于政务云平台管理员的日常运维管理也要进行外部接入的访问控制和传输数据

的密码保护。密码资源池为政务云平台上密码应用支撑，用于为政务云租户按其使用需求提供各类可动态扩展的密码服务。云密码资源池管控系统主要对密码资源池进行管控调度。

密码监管区主要是为密码管理部门提供密码监管手段，通过建立密码监管平台实现对云平台内部使用的及对外提供服务的密码设备进行统一监测与管理，能够汇总统计用户业务的密码应用使用情况，为分析决策提供有力依据。

3.3 主要功能

云服务器密码机主要功能

- 提供标准通用密码服务接口，支持商用密码算法 SM2、SM3 和 SM4
- 支持云平台对云服务器密码机的调度与管控
- 支持租户对虚拟密码机的密码密钥管理
- 支持应用客户端对虚拟密码机的安全调用
- 提供基于标准 RESTFUL 接口的数据安全服务，为租户云上应用提供简单、高效的密码服务
- 为应用提供基于国产密码的传输层保护

3.4 主要技术指标

（1）云服务器密码机技术指标

- 双路万兆光口、双冗余电源，实现高可用和高可靠
- 单台物理云服务器密码机可支持 32 个虚拟密码机的运行

（2）虚拟密码机（VSM）技术指标

- 最大并发连接数：≥64
- SM2 签名/验签：≥3200tps/2500tps
- SM3 摘要：　　≥4500tps
- SM4 加密/解密：≥4500tps

（3）虚拟 SSL 网关技术指标

- 单台虚拟 SSL 网关的最大并发连接数 1000
- 单台虚拟 SSL 网关支持多个应用

- 支持集群部署

4. 方案特色

（1）专注云密码技术，具备深厚积累

- 成熟云服务器密码机产品
- 通过国家密码管理局测评鉴定

（2）深入用户场景，准确把握用户需求

- 全方位全流程密码应用防护体系
- 成熟的政务云整体密码应用安全解决方案

（3）标准化工程实施方案，体系化服务保障机制

- 基于政务云商用密码应用指南设计与实施
- 密码资源统一监控调度，实时监管，确保系统运行稳定、可靠

5. 适用领域

电子政务云平台、大数据平台等各类政务应用汇聚的大型应用场景。基于兴唐通信科技有限公司通过国家密码管理局测评鉴定的云服务器密码机系列产品构建体系化的兴唐政务云密码应用安全解决方案。

6. 企业分工

表 2 解决方案相关企业分工

分类	名称	职责	主流产品名录
密码设备和服务提供商	兴唐通信	云平台密码资源池建设与集成运维服务。	云服务器密码机、SSL VPN 设备、IPSec VPN 设备以及租户密码服务套件等
CA 厂商	贵州 CA 等第三方产品	用户证书、设备证书等的签发与管理	CA 证书系统
密码服务中间件	兴唐通信、贵州 CA、海泰等第三方产品）	统一身份认证等典型密码服务支撑	密码服务中间件

国密安全浏览器	北京奇虎 360 科技有限公司	支持国产密码算法的浏览器	360 安全浏览器国密专版
云密码管控	兴唐通信	云密码资源池中云服务器密码机以及虚拟密码机的管理调度服务	云密码资源池管控系统

7. 典型应用案例

兴唐通信科技有限公司研制的 SJJ1811 云服务器密码机已成功应用于“云上贵州”政务云平台密码服务资源池的建设，根据云上贵州政务云密码应用实际需求，基于 SJJ1811 云服务器密码机在电子政务外网区和互联网区分别建设云服务器密码机集群，形成按需自助服务、快速伸缩与服务可计量的政务云密码服务资源池。云密码服务资源池由云服务器密码机硬件资源 HSM 集群、租户密码安全套件及云密码资源池管理系统组成，为云上的政府部门业务、公共业务以及互联网业务提供符合商用密码标准的高可用、高可靠、高安全的通用密码服务。

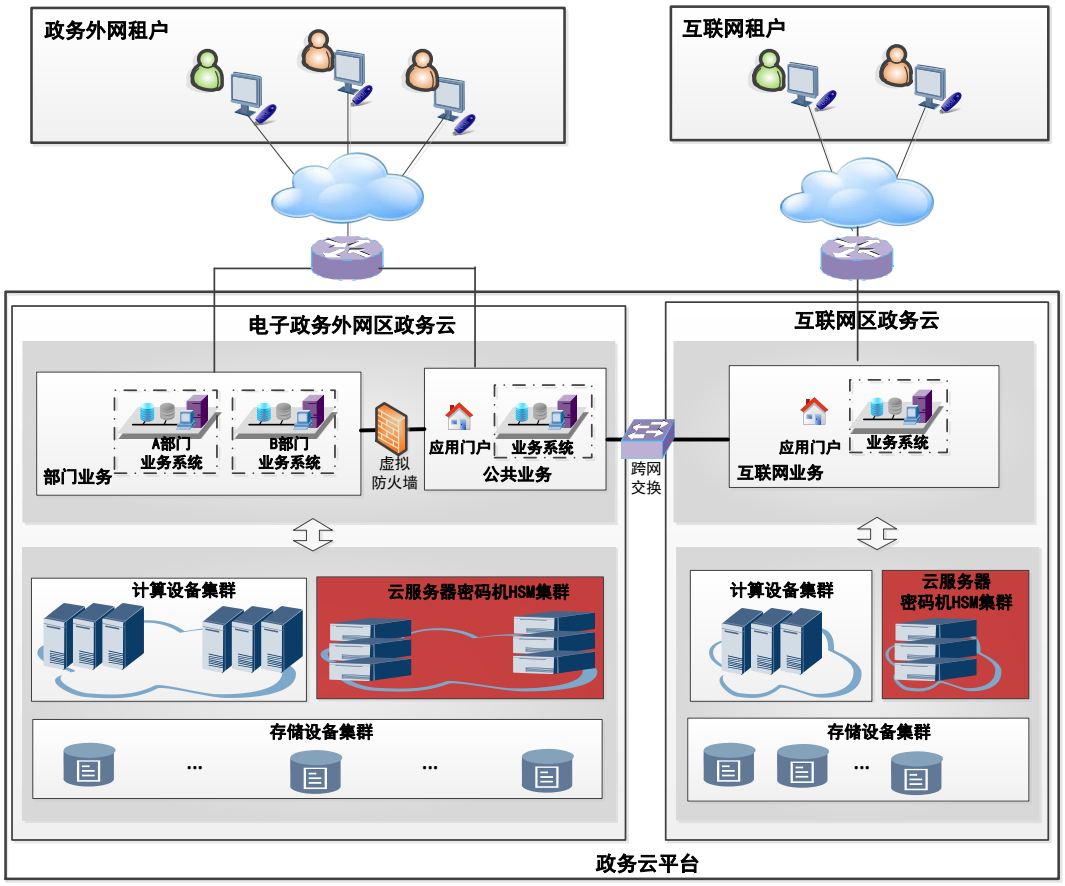


图 7-1 “云上贵州”政务云密码服务资源池部署

兴唐通信科技有限公司

联系人：王健安　　胡伟

电　话：13699262399　　13466362701

010-62301206　　010-62302004

政务云密码应用解决方案

1. 概述

在《国家电子政务总体框架》中明确提出了“以政务信息资源开发利用为主线，建立信息共享和业务协同机制”，该框架明确了在电子政务发展进程中，对于政务信息资源的采集、更新、公开与共享来说，信息得到有效利用的关键问题是如何对信息进行资源共享、协同响应、流畅交互。“云计算”作为一种新兴的网络资源利用方式与传统的信息网络系统存在较大的差异，其主要代表性特征包括按需自助服务、泛在接入、资源池化、快速伸缩性、服务可计量等特点，这些代表性特征能够很好地解决国家电子政务对信息进行存储、提取、共享和使用的需求。

2016 年 12 月底，国务院办公厅印发了《“互联网+政务服务”技术体系建设指南》，明确了“互联网+政务服务”建设遵循国家信息安全等级保护相关规范以及国家密码管理的有关要求，建立健全“互联网+政务服务”安全保障体系。实现电子政务平台有效运行,主要电子政务应用系统互联互通,省、市、 县、乡四级网上行政审批全覆盖,群众关注的重点民生服务事项实现网上办理。在省级工作层面，重点推进政务公共云、政务专用云建设。采用集中化的安全管理策略加强数据安全基础保障设施建设，对于重要业务系统及核心商业秘密信息采用国产密码算法进行加密保护，真正实现自主可控的安全要求。

2017 年 7 月，中央密码工作领导小组办公室印发了《关于做好金融和重要领域国产密码应用试点工作的通知》，要求在政务云领域推广国产密码应用。2018 年 7 月，中共中央办公厅《金融和重要领域密码应用与创新发展工作规划（2018-2022 年）》的通知（36 号文）进一步给出了在金融和基础信息网络、重要信息系统、重要工业控制系统及面向社会服务的政务信息系统等重要领域的密码技术应用规划及相关工作要求、工作任务及分工。

2. 需求分析

密码技术体系面向服务对象，结合不同的应用场景，形成了多种的应用类密码模式，政务云中的密码服务体系，一方面从实现角度，仅作为密码计算的提供平台，缺乏合理的密码应用模式区分以及配套的密码计算弹性计算，另一方面对于密码应用保护的范围和目标也缺乏定义，从而导致以下几点问题。

2.1 政务云与密码的结合纵向缺乏深度

现有云计算中出现的云密码服务，在现有密码设备的基础上实现了分布式服务，为云租户及上层应用提供了基础的密码服务，服务对象集中在 SaaS 层，可定义为应用安全支撑服务；但是从整体应用效果分析，现有云密码服务体系缺乏贯穿政务云平台的密码服务能力，对于 IaaS、PaaS 两层的密码防御比较薄弱，导致密码技术无法为政务云的底层资源、中间层等提供合适的密码服务，限制了密码服务体系与政务云融合的深度，降低了使用密码技术后的安全水准。

2.2 密码技术与政务云的横向耦合脱节

传统密码技术的应用由于其自身安全特性，采用的是独立的单运算方式，相对封闭，但是由于云计算自身是一个分布式资源动态分配的平台，传统的密码计算模式已经很难应用于云计算平台，现有的云密码模式也仅是通过物理设备的负载实现分布服务，核心计算仍然沿用传统模式，与云平台的技术架构无法有效对接，使得密码技术在云计算平台中应用的场景非常有限；因此也阻碍了密码体系在政务云平台中的推广和应用。

2.3 密码服务标准应对不统一

目前在云环境中，各类应用为满足自己的需求采用了不同的密码算法和协议，配置了不同等级、不同类型的密码设备，例如部分应用系统支持国产 SM2 算法，但是其余的系统仍只支持 RSA 算法体系；另外，虽然各产品均遵循国家密码管理局的统一标准，但具体实现方面，在诸如编码格式、参数传递等方面上确存在差异，所以各厂商开发的密码产品在沿用的标准上、提供给上层应用的接口上、

设备管理的方式上均不同，与建设初期的目标相驳，导致系统对接困难、涉密数据交换不顺畅。

3. 方案架构

3.1 技术架构

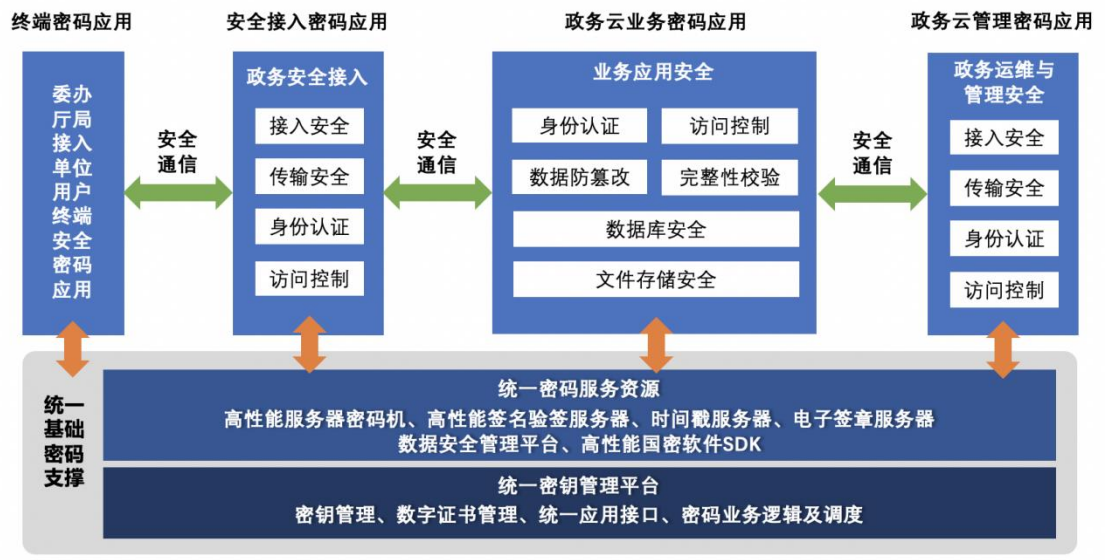


图 3-1 技术架构图

本方案基于国密算法为政务云环境提供密码服务，即由密码服务系统统一向保护系统资源的应用提供加密、解密、签名、认证等基础密码应用服务。

统一密钥管理平台对政务云密码应用提供密钥管理、数字证书管理、统一应用接口以及密码业务逻辑及调度等密码应用所需的基础支撑。

统一密码服务资源包括高性能服务器密码机、高性能签名验签服务器、时间戳服务器、电子签章服务器、数据安全管理平台以及高性能国密软件炼石CipherSuite（SJM1808）。

统一密钥管理平台与统一密码服务资源向政务云中云平台、终端、网络与边界、云管理等提供密码服务，包括：

根据政务云平台以及云平台所承载的业务应用需要，为政务云用户按需提供弹性、按需的加解密等通用密码服务；

基于数字证书管理系统，为政务云中的终端、网络与接入、云平合等提供身

份认证、访问控制、安全传输、安全审计等服务。

高性能密码软件与统一密钥管理结合，为虚拟机和终端提供了 CipherSuite，以供在虚拟环境以及移动终端和物联网终端环境下实现密码能力。

高性能密码软件与数据安全管理平台以及统一密钥管理结合，可为政务云提供基于国密算法的数据库安全以及文档安全的实现，包括数据加密、细粒度访问控制以及安全审计功能。

3.2 主要功能

本方案的设计目标为基于国产密码技术及其应用体系，面向政务专有云计算环境的国密密码保障迫切需求，设计实现以密码功能为基础，硬件密码设备为载体，密码服务为核心，提供加密、解密、签名、认证以及相应密码管理、安全防护等一体化密码服务保障支持的国密密码服务应用系统。具体密码保障功能包括：

（1）保障政务专用云云计算环境中的重要信息系统安全运行、关键数据的安全存储和使用；

（2）保障政务专有云与其他专有云之间数据加密传输；

（3）保障政务专用云与厅局委办本地局域网之间的数据传输安全；

（4）政务办公人员使用移动终端通过无线网络安全接入政务专有云开展移动应用；

（5）公众用户使用各类终端通过互联网安全接入政务外网使用政府提供的社会化服务；

（6）云平台自身计算、存储、网络资源的安全，如管理员的身份安全、虚拟机安全、审计日志安全；

（7）云平台租户和租户应用的安全，如管理员的身份安全、操作命令安全、审计日志安全。

3.3 主要技术指标

1）算法性能指标：

密码算法	执行操作	性能（单线程）
SM2	签名	每秒 2.7 万次
	验签	每秒 1.5 万次
SM3	哈希	2.4 Gbps
SM4	加解密	Gbps

注：以上性能测试结果均基于 Intel i7 处理器

2）运行负载影响指标：

炼石云密码应用解决方案上线后，对原有业务系统性能降低不高于 13%，对数据库性能降低不高于 5%。

比较项目	CPU 占用（%）		负载增加
仅应用与数据库运行	Oracle CPU	58.03	-
	App CPU	41.46	-
开启炼石方案 (SM4 算法)	Oracle CPU	60.86	4.88%
	App CPU	46.58	12.35%

测试数据量说明：

1kb 数据，50 线程，每线程每秒并发 20 次 SQL 请求，每个 SQL 请求会做 100 次数据加解密（加密/解密各 50 次），即每秒对 1kb 数据做 50*20*100=10 万次加解密。

4. 方案特色

（1）基于国密技术构建安全基础设施

建立基于国密技术的底层安全基础设施，应用符合国家要求的密码技术产品加强身份认证和数据保护，确保安全可控。例如提供主账号密码的安全存储机制，使用带盐哈希加密后存储；

（2）建立身份管理权威数据源

确立核心数据源，建立企业级统一身份平台，实现从核心数据源到应用系统间的数据同步，确定并建立人员身份管理流程。实现应用系统帐号生命周期管理。建立统一身份认证标准与规范。

（3）建立统一身份认证中心，实现应用访问单点登录

建立统一认证中心，用户访问统一入口，统一授权模型，基于角色和组。多因子认证集成及认证策略配置。安全审计，基于帐号管理及用户登录及登出等操作行为，用户访问行为审计及报表生成与导出。

（4）建立应用集成接口规范，实现便捷集成

统一密码服务平台作为整体系统对外提供服务的主要功能模块，以为用户提供自身密钥管理与密码运算为主。所有实现的功能可提供对外 RESTful/SDK 形式接口调用函数或者直接通过页面访问相关服务，SDK 提供 C#和 java，简化用户的调用方式与调用过程，实现快速对接，对上层应用屏蔽密码复杂性，实现密码普适性目的。

5. 适用领域

本方案适用于政务专有云计算环境的国密密码保障迫切需求，设计实现以密码功能为基础，硬件密码设备为载体，密码服务为核心，提供加密、解密、签名、认证以及相应密码管理、安全防护等一体化密码服务保障支持的国密密码服务应用系统。

也适用于各个行业企业在公有云、私有云、混合云等场景存储有重要数据、敏感信息等内容，可实现在不改造应用的前提下，实现主体到人、客体到字段的数据加密、权限细控。

6. 企业分工

北京炼石网络技术有限公司负责解决方案及相关配套产品提供，包括如下产品：

（1）CipherGateway 业务应用安全网关（产品型号：SJJ1717）

（2）CipherSuite 密码套件（产品型号：SJM1808）

（3）服务器密码机（产品型号：SJJ1941）

7. 应用案例

客户：北京 2022 年冬奥会和冬残奥会组织委员会

炼石方案目前已应用在“北京 2022 年冬奥会和冬残奥会组织委员会” 面向全球招聘志愿者、工作人员云系统中。保护云上应聘者的个人敏感信息，比如手机号、身份证号、护照信息、宗教信仰等。

项目运行至今进行了两轮大规模招聘，密码及安全机制运行良好，有力保障了重要数据的安全，因此公司收到了来自冬奥组委会的感谢信。

北京炼石网络技术有限公司

联系人：钱晶

电　话：15201490479

010-88459460

政务移动办公密码应用解决方案

1. 概述

新世纪以来，我国政务信息化经过“十一五”全面建设、“十二五”转型发展，基本实现了部门办公自动化、重点业务信息化、政务网站普及化，深刻地改变了政府的运行方式、管理方式，大大提高了政府机关的工作效率、树立了良好的服务形象。

随着移动通信技术的发展，建立在移动通信网络之上的移动政务逐步发展起来。但是移动政务在提高了办公效率，降低了内部沟通成本的同时也带来了大量的安全问题。为解决移动政务所面临的多种安全问题，我公司推出了安全移动办公系统。

本系统所采用的方案遵循商用密码、等保三级及电子政务外网等相关标准规范，构建起覆盖终端、网络、应用、数据和管理的一体化“移动政务”密码保障体系，通过全面应用商用密码有效提高了移动办公的安全性。系统已通过国家密码主管部门审查，已取得商密证书（批准型号：SJT1808 基于 SM 算法安全移动办公系统）。

2. 需求分析

政府单位开展移动办公业务需要构建一体化的移动办公系统，同时也需要解决移动办公面临的安全问题，如恶意 APP 窃取敏感数据、移动终端丢失、网络窃听、数据篡改、办公内网非法接入、业务数据非受控交换、服务端遭受恶意攻击等，只有通过构建全方位的移动信息化安全堡垒，才能支撑移动办公在更大范围和规模上进行推广应用。

3. 方案架构

3.1 技术架构

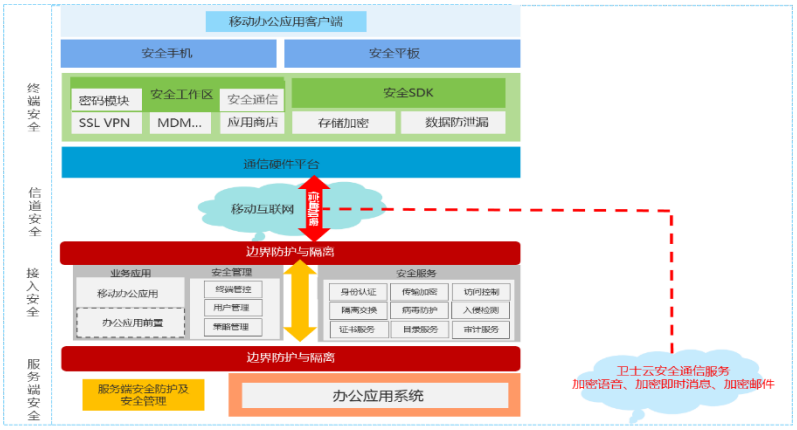


图 3-1 安全移动办公系统架构

安全移动办公系统主要提供安全通信、安全接入和终端管理三方面的能力。系统架构分为四个层面：移动端安全、信道安全、接入安全和服务端安全，实现等级保护标准中安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心的全覆盖。

3.2 产品部署图

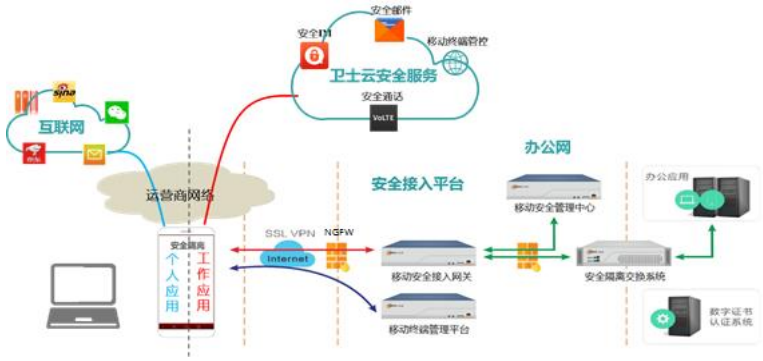


图 3-2 系统组成示意图

安全移动办公系统由安全移动终端、下一代防火墙 NGFW、移动安全接入网关、移动办公安全管理平台（MDM/MAM/MCM）、移动安全管理中心、数字证书系统等组成；移动办公业务应用系统部署在政府单位非密办公网，由第三方厂家提供，需与安全移动办公平台进行适配对接。

3.3 主要功能

- 安全移动终端由国产定制安卓移动终端、商密密码模块和安全移动办公应用组成，支持运行环境隔离、身份认证、数据存储加密和移动终端管控等安全功能。
- 安全移动办公接入平台用于实现移动终端访问单位内部办公网过程中的数据加密传输、身份认证与访问控制和数据安全隔离交换。
- 安全通信是企业级的安全协作平台，通过即时消息、VoIP 加密通话、企业通讯录、安全邮件等打造安全、快捷、高效协同办公体验。

3.4 主要技术指标

（1）主要功能指标

支持基于商密算法 SSL VPN 标准的数据安全传输，密钥协商数据的加密保护采用 SM2 非对称密码算法，报文数据的加密保护采用 SM4 对称密码算法，数据的完整性保护采用 SM3 算法

支持基于支持硬介质形式的数字证书进行接入身份认证

支持对移动终端的密钥、设备、应用、内容进行管理

移动办公终端业务数据与个人数据隔离存储，其中业务数据加密存储

（2）主要性能指标

可创建用户数：不小于 10000 人

同时在线用户 ：不小于 2000 人

密话接通率：不小于 95%

VPN 登录时间：不大于 10 秒钟

VPN 传输速率：不小于 300KB/秒

4. 方案特色

- 方案设计符合国家等级保护要求，系统全面地保护移动办公中敏感数据的流转，从整体上提升系统的安全性，同时也便于安全测评。
- 方案中密码设备全部通过国家密码管理局鉴定，构建起覆盖终端、网络、

应用、数据和管理的 “移动政务”密码保障体系。

- 提供完整的安全保障，方案中移动终端采用的芯片、整机和应用系统均自主可控，接口设计无缝衔接，兼容性、软硬件完美适配。
- 安全移动终端支持业界领先的端到端加密语音业务，实现用户语音通信的一话一密和端到端的加密保护。

5. 适用领域

移动办公和移动信息化正日益成为各级单位履行自身职能的必备工具。因此本系统在未来很长时间内，在党政、军工等领域具有很大的市场前景，并会取得可观的经济效益。

6. 企业分工

安全移动办公系统的安全移动终端产品由华为提供，安全接入平台设备产品及安全通信服务由卫士通提供，网络专线及流量卡由运营商提供，卫士通公司统一采购然后按年向用户收取服务费。

部署位置	产品名称	产品型号
安全移动终端	Mate10 安全手机	HW Mate 10
	Mate20 政务双系统安全手机	HW Mate 20
移动安全接入平台	移动安全接入网关	SJJ1522/V4.1
	移动办公安全管理平台	WG EMM 2.1
	移动安全管理中心	WTA-SMC-MM400-AA-XXB
	下一代防护墙	WFW-FW-B/V2.1
	安全隔离交换系统	WstGap V1.0
	数字证书系统	WTA-CS-PKI-LCB

7. 应用案例

截止 2018 年底，系统已在中纪委、四川省政府、吉林省委、哈尔滨市政府、呼伦贝尔市委、中电科集团等移动办公的项目中得到应用。其中吉林省前郭县移动办公商用密码应用项目荣获 2019 中国物联网安全高峰论坛九大商用密码新应

用案例之一。

中电科（北京）网络信息安全有限公司

联系人：丁月　　丛薇

电　话：13522625886　13601334910

政府机关移动办公安全解决方案

1. 方案背景

随着 Internet 技术和移动技术的不断发展，越来越多的政府机关已依托互联网组建了自己的网上办公系统与业务应用系统，多数单位也已应用了移动 APP 使移动办公成为可能。

在此过程中，如何解决基于开放系统互联下的移动办公数据及文件的安全性、个人身份认证、以及网络数据传输的安全性成为政府机关首要考虑的迫切问题。

2. 安全需求分析

根据政府机关对网络信息系统建设的需要，在实现移动办公安全接入的同时，结合国家政策对相关网络通讯协议和加密算法的要求，其安全接入需求主要如下所述：

（1）业务系统机密数据安全保密性需求

在移动办公或移动业务操作过程中，因终端的种类较多，有各种移动 PC、移动平板和移动手机，对于办公系统或业务系统的敏感机密数据的安全保密性要求较高。要保障这些数据对移动终端是隔离的、安全的，并且不在移动终端设备上存储敏感机密信息（一旦存储即存在被窃取或主动/被动数据泄露的可能）。

（2）网络通讯协议及加密算法的合规性需求

网络传输通讯协议必须符合国家密码管理局颁布的相关国家技术标准，符合《SSL VPN 技术规范》的要求。

加密算法必须使用国家密码管理局颁布的加密算法。对数据加密的对称算法应使用 SM1 或 SM4 算法；用于证书认证的非对称算法应使用 SM2 算法，摘要算法应使用 SM3 算法。

（3）移动设备、网关设备与用户的管理与安全性需求

对所有移动设备、网关设备和移动用户采用统一、严格的身份认证和集中管

理；需实现实时监控网关设备及用户工作状态，并进行详细日志记录；对移动设备上的用户操作进行详细记录；整个系统安装方便、快捷，便于维护和管理。

3. 方案综述

3.1 移动办公安全解决方案说明

根据政府机关的移动办公及移动业务操作的实际需求，我们采用经国密局鉴定通过的 VPN 密码机、支持 SM2 证书的 CA 服务器，以及虚拟手机服务器的组合应用解决方案，解决政府机关在移动办公及移动业务操作过程中的数据及文件的安全保密、网络传输安全保密、人员身份认证、设备集中管理及访问控制等。具体的网络拓扑图及解决方案如下（本方案旨在表述“移动安全接入”，整体完备的信息安全解决方案不再此表述）：

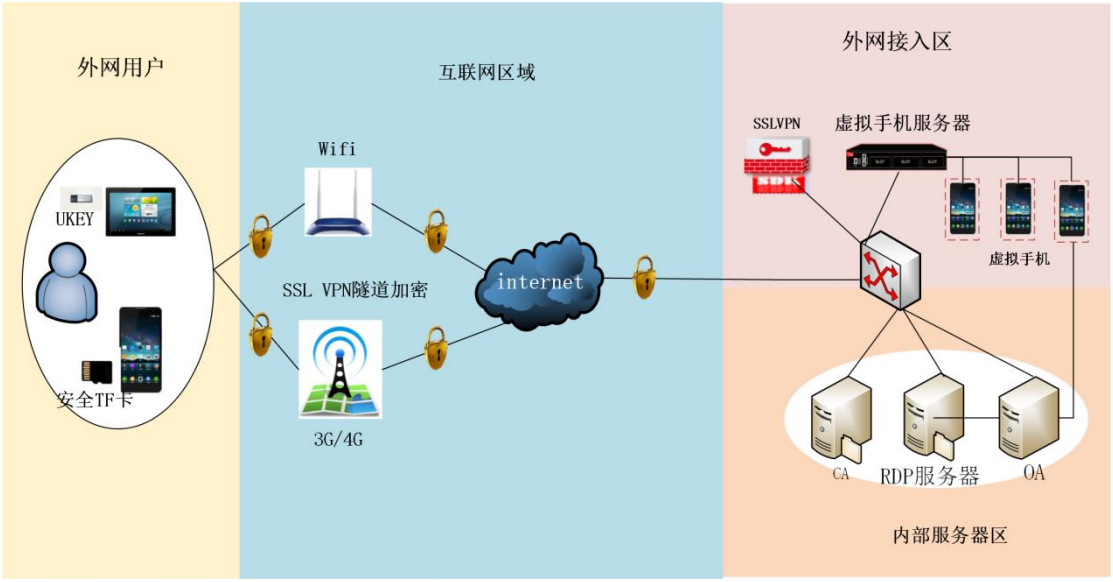


图 3-1 移动办公安全解决方案网络拓扑图

在政府机关内网的互联网出口处部署高端 IPSEC/SSL VPN 综合网关作为安全接入网关。VPN 密码机内置硬件加密卡，支持 SM1、SM2、SM3、SM4 等国产密码算法，符合国密局 VPN 技术规范要求。同时，VPN 综合安全网关集成的防火墙功能可进行网络访问控制及网络安全防护。VPN 综合安全网关对移动用户提供统一的基于 SM2 证书的身份认证、访问授权及隧道通讯服务。当用户通过身份认证后，根据其角色确定相应的访问控制列表，并向终端推送授权的虚拟

手机设备连接配置以访问不同的业务系统。

在政府机关内网部署 CA 服务器，为所有移动用户签发 SM2 算法的证书，使用证书方式对移动用户的远程接入进行身份认证。CA 服务器需符合国密局《SM2 数字证书规范》。

在政府机关内网部署虚拟手机服务器，提供虚拟手机池为移动用户接入使用。支持虚拟手机设备的统一管理，移动应用的统一管理，移动用户使用虚拟手机的行为安全策略管理。可根据策略让虚拟手机池中的虚拟手机设备安装不同的应用，根据角色分配虚拟手机设备的连接配置，虚拟手机服务器符合等保要求中对移动信息系统建设的要求。

移动用户在平板、手机上安装安全虚拟手机客户端，在使用 SM1 或 SM4 算法加密的隧道中连接虚拟手机池中的虚拟手机来进行远程安全接入访问，使用写入 SM2 证书的安全 TF 卡进行身份认证。移动用户在移动 PC 终端上安装 SSL VPN 客户端，在使用 SM1 或 SM4 算法加密的隧道中连接内网的 RDP 服务器的远程桌面或应用进行远程安全接入访问，使用写入 SM2 证书的 USBKey 进行身份认证。安全 TF 卡及 USBKey 均自带加密芯片，支持 SM1、SM2、SM3、SM4 国产加密算法。

部署方案设备清单：

天融信安全接入网关	SSL-VPN
天融信安全虚拟手机平台	Top-SVP
国密 CA	
国密 USBKey、安全 TF 卡	

3.2 移动办公安全解决方案优势及特点

（1）移动办公应用及业务的数据和文件与个人终端彻底分离，在个人终端数据 0 留存，个人终端上看见的仅是图像，而工作数据及文件集中在政府机关内部数据中心。

数据在内部网络存储，易于机关单位集中防护；

手机端只展示虚拟手机画面，0 数据留存，手机丢失也不用担心数据流失；

工作场景数据在内网备份，更换手机后可快速恢复工作环境。

（2）政府机关相关的移动应用始终在内网运行，外网的移动终端上仅传输屏幕图像和触控操作。

无需担心网络安全攻击造成的数据泄露，即使被拦截获取，也是一些加密的图像数据，无意义；

对移动设备的网络攻击（恶意 WIFI，ARP、DNS 欺骗等），木马病毒等无法威胁到运行在企业内网的移动应用；

拷屏操作将被系统审计机制记录并报警。

（3）运维简单：政府机关相关的移动应用在内网统一管理、部署、升级，无需对移动用户的移动设备进行复杂管理。

（4）移动设备兼容性好，安全虚拟手机客户端可在主流的 Android 手机、平板上运行。

4. 应用案例

某信息中心为实现移动办公及移动业务操作，提出需求，既要能方便地进行远程移动办公和移动业务操作，又希望工作数据在个人的移动终端上的安全性要得以保障。

根据某信息中心的需求，我们在信息中心网络的互联网出口处部署了高端 SJJ1209 IPSEC/SSL VPN 综合安全网关，用于移动用户的远程安全接入。在信息中心内网中部署了虚拟手机服务器，提供虚拟手机池，其中的虚拟手机为远程接入的移动用户提供办公 APP 和业务 APP 来进行远程办公和业务操作。在需要进行移动办公和移动业务操作的移动终端上安装安全虚拟手机客户端及写入了 SM2 证书的安全 TF 卡，移动终端使用安全 TF 卡内的 SM2 证书进行身份验证，并与 VPN 网关建立国密隧道，通过国密隧道访问虚拟手机池内的虚拟手机进行远程移动办公和移动业务操作。

对于信息中心而言，我们提供了一个集中化的易于维护和管理的高效工作平台，所有的虚拟手机都托管在信息中心内网数据中心服务器上由管理员统一维护管理，管理员对信息中心的移动办公应用进行统一的发布管理，对安全漏洞进行

统一的处理应对。同时移动应用和数据均不离开数据中心，始终限制在内网，与外网完全隔离，移动终端设备零数据留存，只是展示操作画面，工作数据安全得以保障。

对于移动用户而言，通过安全虚拟手机客户端，可以随时随地通过安全的国密隧道访问信息中心分配给自己的虚拟手机，进行移动办公和移动业务操作，大大提升工作效率。并且安全虚拟手机客户端只是一个展示远程虚拟手机画面的瘦客户端软件，不会对移动用户手机进行强有力的管控，信息中心在确保移动办公信息安全的同时又很好的兼顾了移动用户个人隐私。

北京天融信网络安全技术有限公司

联系人：罗元

电　话：13810670323

政务服务一网通办商用密码应用解决方案

1. 概述

为深入推进“互联网+政务服务”，加快建设全国一体化在线政务服务平台，2018 年 6 月，国务院印发《进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案》（国办发〔2018〕45 号），7 月印发《国务院关于加快推进全国一体化在线政务服务平台建设的指导意见》（国发〔2018〕27 号），旨在全面推进政务服务“一网通办”，真正实现“只进一扇门”，根除奇葩证明，让企业和群众“最多跑一次”。

为落实国务院提出的建设全国一体化平台精神，各地政府也陆续出台了推进政务服务“一网通办”相应的工作实施方案，要求实现政务服务事项“一站式”网上办理，推动网上政务服务大厅与实体大厅、线上与线下政务服务融合发展，形成一体化的互联网政务服务平台，进一步拓宽互联网、移动端、自助终端等多种服务渠道，为群众提供精准化、智慧化服务。

当前，基于开放匿名的网络发展起来的电子政务业务应用，不可避免地需要解决网络世界的安全与信任问题，尤其是实现一网通办应用所引发的责任问题，更是必须要严肃考虑和认真解决的。这要求在网络应用中建立可靠的安全认证信任体系，因此，商用密码是推进政务“一张网”落地实施的安全基石！

2. 需求分析

为实现网上政务服务事项的统一申请、统一受理、集中办理、统一反馈、全流程监督的目标，需要解决用户网络数字身份的真实可信，需要解决用户数字身份的跨部门、跨业务、分等级的全生命周期管理，需要解决用户多种身份凭证的使用便捷及兼容等问题，同时加强信息、服务的安全性、提升客户的方便性。一网通办商用密码应用解决方案，既能提供健全完整的身份认证体系，还有效提升用户访问体验和系统的安全性。

3. 方案架构

3.1 技术架构

商用密码一网通办应用的技术架构如图所示。

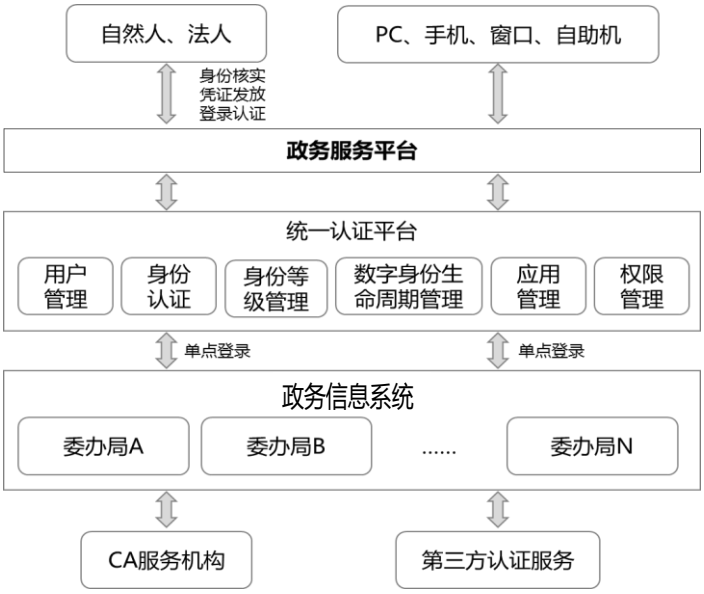


图 3-1 技术架构图

自然人或法人通过 PC、手机、窗口、大厅自助机等多种渠道访问政务服务平台办理业务，统一认证平台为政务服务平台提供分等级的用户身份管理、多凭证的身份认证管理、事项办理的权限管理和单点登录等安全支撑。

3.2 产品部署图

产品部署如图所示。自然人、法人通过外网访问，由统一认证平台提供身份认证和单点登录服务。

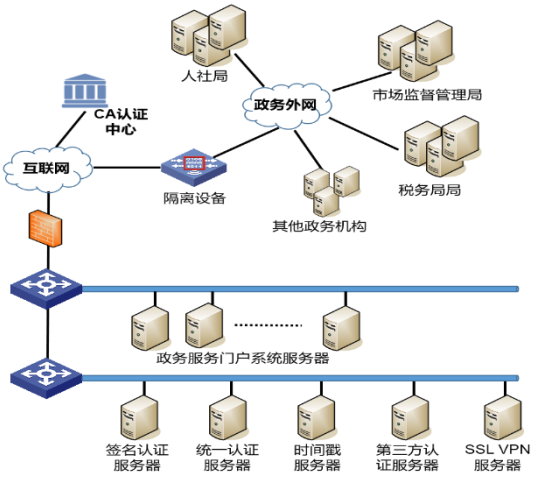


图 3-2 产品部署图

3.3 主要功能

方案提供的主要功能包括用户管理、凭证管理、认证等级管理、单点登录等功能。

用户管理：提供统一的用户体系，支持用户的管理及与应用系统同步。

凭证管理：支持用户多种凭证管理，包括用户名口令、政务数字证书、第三方认证（支付宝、微信）以及工商电子营业执照等。

认证等级：支持双因子认证等多种认证等级管理，根据鉴证的安全强度不同，可以分为 L1、L2、L3 和 L4 四个认证等级。其中，L2 及以上的认证等级满足安全等级保护 3 级对身份鉴别的要求。

单点登录：支持用户一次登录认证成功后，访问其他政务系统时不需要二次认证。

3.4 主要技术指标

用户认证性能指标：响应时间不超过 3 秒，每秒成功处理事务个数（TPS）不低于 1000。

单点登录性能指标：用户单次身份认证登录时长不超过 2 秒，用户单点登录完成时间不超过 3 秒，单点登录并发处理能力大于 800 次。

4. 方案特色

本方案具有易实施、易应用、易运维、易扩展、高安全等特点，在遵循国办全国一体化在线服务平台的系列认证标准基础上，充分满足法人、自然人手机办事、网上办事、大厅窗口办事以及政务实体大厅自助终端办事等多种渠道的可信身份认证需求，通过与各委办局的单点登录整合，方便了最终用户在业务办理过程中一次认证，全网漫游。此外，本方案采用了国产商用密码算法，确保认证、电子签名和信息传输过程中的安全可靠。

5. 适用领域

本方案主要适用于政务领域各省级、地市级一网通办的建设，提供用户分等级认证管理等服务。

6. 企业分工

本方案主要由数字认证提供方案设计、产品部署等工作。方案提供的产品清单如下：

序号	名称	提供单位	备注
1	签名认证服务器	数字认证	实现身份认证、电子签名及验证
2	统一认证服务器	数字认证	实现身份等级管理、用户管理、授权管理和单点登录
3	时间戳服务器	数字认证	提供可信时间服务
4	第三方认证服务器	数字认证	与其他第三方认证服务对接，实现多认证管理
5	SSL VPN服务器	数字认证	建立可信安全通道，实现网络加密传输
6	数字证书	数字认证	由第三方CA机构签发，作为用户网络可信身份凭证

7. 应用案例

本方案应用于北京市“一证通”统一身份认证体系，该项目是全国首批上线的 5 个政务信息系统整合共享应用试点典型案例，实现了全市法人分级身份认证、统一账户管理和试点应用的单点登录，已完成与国家政务信息资源共享交换平台的对接，实现对全国法人用户的身份核验。

北京数字认证股份有限公司

联系人：任家萍

电　话：17801108503

某部委密码应用解决方案

1. 概述

某部委全体工作人员使用蓝信移动工作平台（以下简称蓝信）作为移动办公应用系统。此系统符合等保三级要求，但因提升安全等级需要，对此系统进行了国密化改造，增加国产密码软硬件模块，应用国密算法，增强系统安全性。

2. 需求分析

目前用户单位移动终端利用无线的方式访问电子政务平台的应用，存在系统安全隐患，主要有以下几点：

- 终端接入不够可信
- 身份认证过于简单
- 链路通信不够安全
- 敏感数据保护有待加强

需求分析如下：

- 终端可控：实现对各类移动终端信息进行审核识别和安全管理，防止非法设备接入网关访问内网业务系统。
- 强身份认证：针对不同的终端类型提供适合的身份认证方式，有效加强用户身份认证，防止系统被非法访问。
- 链路安全：建立安全链路通道，数据加密传输，防止网络传输过程中的信息泄漏，保护信息内容的安全。
- 存储安全，对敏感数据在客户端和服务端均进行存储加密，防止由于终端丢失、黑客攻击等情况造成的数据泄露。

3. 方案架构

3.1 技术架构

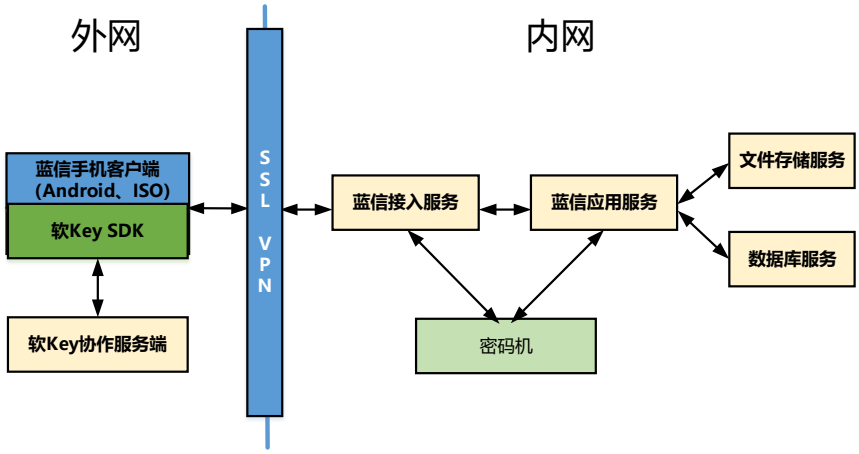


图 3-1 技术架构图

手机客户端通过集成软 Key SDK，与软 Key 协作服务端交互，共同实现密钥协作生成、签名验签、密码计算的功能。

3.2 产品部署图

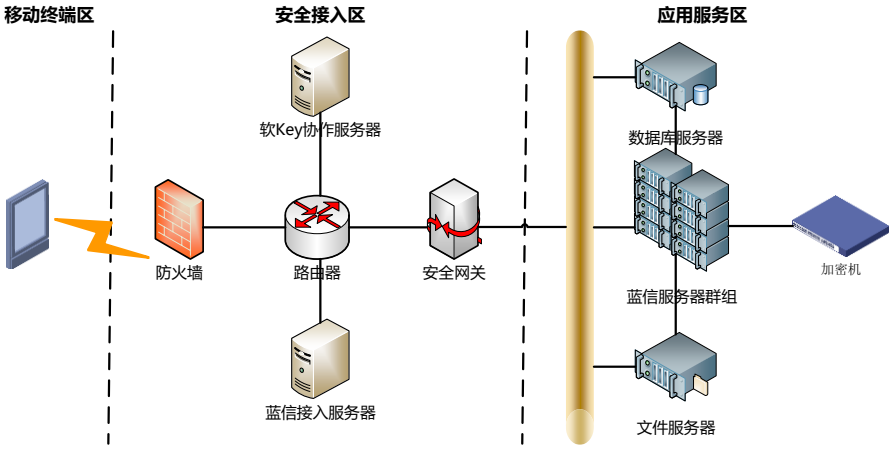


图 3-2 产品部署图

- 移动终端区

智能手机、PAD 等移动终端的蓝信客户端集成具有商密产品型号的软 KEY。软 KEY 作为客户端密码核心，提供身份认证密钥对、加密密钥对、会话密钥的生成、管理、以及密码运算等功能。

- 安全接入区

移动安全接入区包括蓝信接入服务器、软 KEY 协作服务器、安全网关等。使用 SM2 进行非对称密码运算，使用 SM4 进行对称密码运算。软 KEY 协作服务端与移动终端的软 KEY 协同完成客户端密钥生成、数字签名、密码计算等功能。

- 应用服务区

应用服务器主要是蓝信服务器群组，加密机采用具有商密型号的硬件产品。

3.3 主要功能

统一通讯

蓝信以组织通讯录为基础，提供了强大的通讯能力，包括传统通讯和及时通讯。即时通讯支持文字，语音，表情，地理位置，图片，文档，音频，视频等类型信息。可以创建 2000 人的超大群组。支持查看组织发布的图文消息，查询已收到的所有图文消息。

统一应用

蓝信为用户提供了移动端统一的应用入口。蓝信内置了通知管理、工作文档、会议管理、请假管理等多款原生应用。蓝信开放平台提供了标准接口，可以快速集成第三方应用。

3.4 主要技术指标

并发性：支持至少 8000 路移动终端同时接入。

扩展性：支持集群架构，可随需扩展，提高系统吞吐率。

易用性：采用图形化的人机交互界面，人性化设计，操作简单，配置快捷，管理方便。

4. 方案特色

传统 Ukey 方案的不便捷性限制了用户的使用体验，无论是 TF 卡型、SIM 卡型、蓝牙型、音频口，型改造成本和后期维护成本都会很高。而软 Key 密码模

块，可直接用于移动终端，安全等级相同，维护成本低，是移动办公方案的最佳选择。

5. 适用领域

大型、超大型的政府客户。对安全的移动协同电子政务有较高要求的客户。有专属化和定制化服务需求的客户。

6. 企业分工

分类	名称	职责	主流产品名录
业务平台厂商	蓝信	提供移动工作平台产品	蓝信移动工作平台
加密算法厂商	中科院信工所	提供国密加密模块及解决方案	密码机、软 Key 服务器
安全设备厂商	奇安信	提供配套安全产品	SSL VPN、天机

7. 应用案例

客户	核心场景	说明
某交易所	行政办公	保障敏感信息在组织内部安全传递，防止信息外泄，为交易所提供了可靠的信息传递途径。同时，对接了交易所 20 余个行政相关业务，如资产管理、快递签收、用餐管理、访客管理、大厅预定、设备保修、差旅服务、加班管理、工作督办、领导动态、换班签批、在线考试、舆情监控、零报告等。
国家级某金融监管机构	行政办公	对内囊括下设的 16 个职能机构、2 个事业单位以及各地市 41 个下级机构，对外协同全国近 400 个下辖金融公司。围绕办文、办会、办事，在移动端提供通讯录、即时通讯、广播号、待办提醒、会议会务、通知、问卷调查等行政办公能力，极大地降低了对内对外管理协同的成本，显著提升了效率。
某国有银行信用卡中心	行政办公	解散所有的微信工作群，用蓝信实现内部安全沟通。所有部门均创建了自己部门的广播号，对内新闻信息分享做的有声有色。利用蓝信开放开发平台，开发了外勤签到、商管监控、商管绩效等轻应用，解决了办卡推广人员的外勤打卡，汇总日常办卡数据，个人绩效查询等能力，让领导、员工在在手机端完成以前只能在内网完成的业务。

蓝信移动（北京）科技有限公司

联系人：张跃鹏　　裴利杰

电　话：13269123929　18601089048

交通行业二维码乘车密码应用安全解决方案

1. 概述

地铁涉及国计民生领域，与人民群众日常出行及地区经济发展息息相关，已成为驱动区域经济发展的强劲动力，地铁信息系统是国家重要基础设施的组成部分，地铁信息化安全建设是国家十三五网络安全和信息化工作的重头戏，是保证国家重要基础设施信息化建设健康发展的需要。近年来地铁已经成为人们日常出行重要的公共交通工具，为缓解高峰期乘客排队购票现象，提升乘客搭乘地铁体验和出行效率，二维码乘车为乘客提供一个全新的便捷乘车体验。乘客下载注册地铁 APP，不用预付押金，无须预先充值，先使用，后扣费，覆盖面广，乘客只需配备 IOS 和 Android 智能机便能安全享受到扫码进、出站的方便与快捷。

2. 安全需求分析

二维码乘车系统，乘客通过手机 APP 产生二维码，在闸机口通过扫码方式过闸乘车，根据地铁二维码乘车的特性，需要从技术上解决如下安全问题：

1、如何确认乘客真实身份？

2、如何对乘车二维码的安全分发及使用，防止乘车二维码被非法复制、盗刷？

3、如何保证乘客手机在脱机情况下的正常乘车？

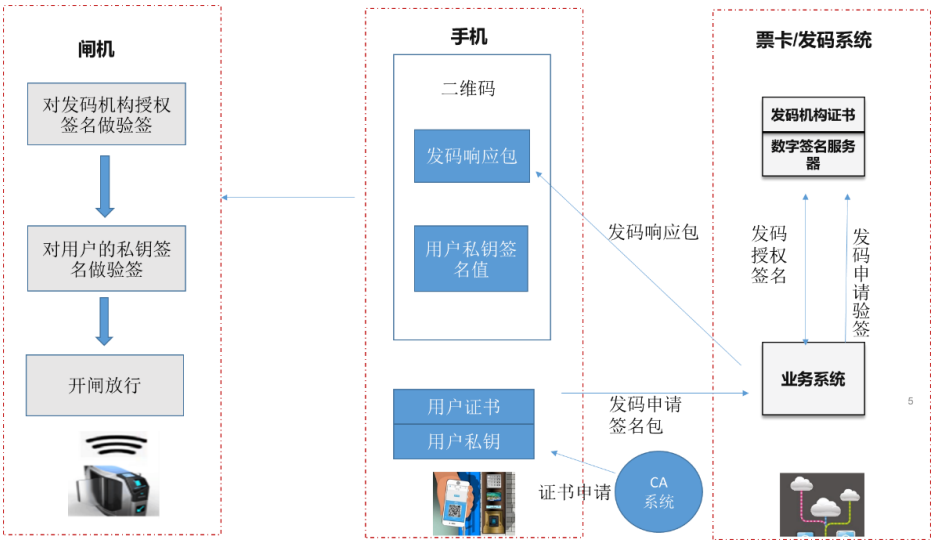
4、如何确保乘客乘车过程及对产生的乘车费用的不可否认性？

5、如何确保在线车费支付及与第三方支付机构的安全清分结算？

6、如何防止乘客手机 APP 信息泄露？

3. 方案架构

3.1 技术架构



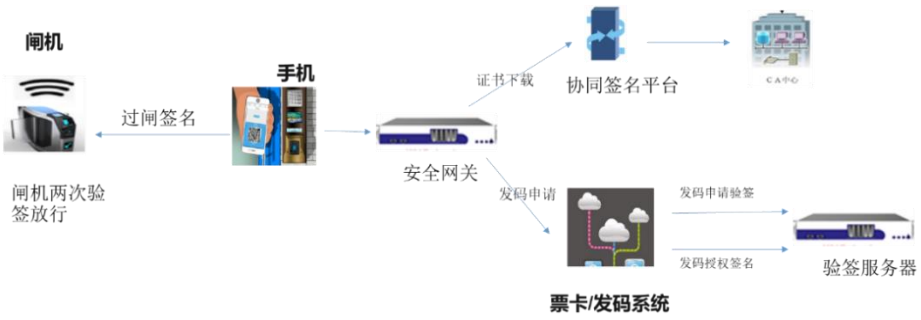
为保障扫码乘车过程的安全，将基于国产 SM2/3/4 密码算法，以可信的身份认证为核心、以数字证书技术为基础、以数字签名技术为保障，建设一套 PKI 可信身份认证体系，在二维码申请、发放、产生、验证等重要环节使用数字签名技术，防止乘车二维码被非法篡改、复制、盗刷及确保每笔交易的可追溯性，数据在传输过程中采用国密的 SSL/TLS 加密技术，确保乘车交易数据在互联网环境中明文不落地，实现数据的安全可控。

扫码过闸安全方案将贯穿从乘客身份鉴定、二维码申请、发放、验证、乘车数据记录、扣款交易记录、地铁和第三方支付公司的结算等关键流程中。当乘客首次使用地铁 APP 注册开通扫码过闸功能的同时，通过协同签名技术为乘客签发一张有效的个人数字证书，数字证书与乘客手机硬件信息及账户信息进行绑定，APP 在与后台服务平台进行通信传输数据时会通过数字证书进行安全认证及通信加密。乘客在申请二维码授权时用乘客证书做数字签名，服务端下发的二维码授权包使用发码机构的数字证书做数字签名，闸机验证二维码时会对乘客的数字签名及二维码授权包的签名信息进行两次签名验证，若验签都通过才能开闸放行，确保了乘车二维码的产生、分发、消费过程的安全性，防止乘车码被非法复制、盗刷。

由于地铁站环境复杂，用户手机可能处于无网络服务情况，方案支持用户手机脱机扫码过闸。在用户手机脱机情况下，利用手机端密钥做数字签名生成二维码，闸机端验证手机密钥签名通过后开闸放行，当用户手机联网之后 APP 会与后台对本次出行数据完成协同签名操作，后台对协同签名验证通过之后完成扣款流程。

地铁与第三方支付公司的数据通信采用数字证书的方式做身份认证，清算数据全部采用数字签名的方式校验。地铁机构与第三方支付公司的对接签名接口使用硬件的签名服务器，保证了签名私钥的安全性及签名运算的高效性。

3.2 产品部署图



在地铁部署两套 SZT1901 型号的数字证书认证系统，为所有乘客提供数字证书的生命周期管理；在地铁部署两台 SJJ1515 型号的安全认证网关，在 APP 与票卡系统之间建立安全的加密隧道，保障所有交互数据安全传输；在地铁部署两台 SRJ1913 型号的签名验签服务器，与票卡系统进行对接，对用户的发码过程做签名验签，保障关键交易的数据的完整性、不可否认性及事后的可追溯性；在地铁部署两套 SHT1733 型号协同签名平台及 SHM1705 型号的移动密码模块，为客户端 APP 提供数字证书下载及协同签名，保证客户端数字证书的存储及使用的安全性。

3.3 主要功能

通过数字证书的安全策略在地铁信任域内建立一套完善、安全的身份识别体系，结合数字签名技术、SSL/TLS 安全传输技术，保障地铁 APP 过闸使用过程中的身份认证、数据安全传输、关键数据的完整性和操作不可否认性等问题。

3.4 主要技术指标

根据城市乘坐地铁的人数及城市地铁闸机总数计算，证书签发系统每秒的发证量设计不低于 100 张，证书签发总数不低于 2000 万张，APP 生成二维码并发数不低于 200 笔/秒，二维码过闸验证时间不高于 0.5 秒。

4. 方案特色

安全的密钥保护机制，方案采用了更安全便捷的协同签名技术，密钥安全级别达到了《密码模块安全检测要求》第二级安全等级。

APP 安全加固，采用一种基于云计算服务的密码技术，应用被 Java 程序代码混淆、C/C++代码混淆、底层接口加壳进行加固，产生的数据均使用专利加密技术进行加密，从而保证地铁 APP 数据的安全，与安全容器外进行隔离。

用户行为模型及机器深度学习，通过在系统使用过程中逐步采集日常乘客行为习惯、行为特征并归纳出用户画像的优势，构建数据模型和机器学习模型，为每个乘客构建击键行为特征画像，对用户身份进行鉴别，并将这一机制应用到地铁扫码过闸系统中。

终端异常交易感知，实时监测地铁 APP 终端安全态势，并把采集的数据发送到监测平台，由平台对收到的海量安全、交易数据通过大数据技术进行分析，感知二维码扫码乘车过程中终端安全异常、交易异常行为，并进行主动告警。

5. 适用领域

二维码消费已经成为主流的一种支付方式，方案中通过国产密码的应用，全面的保护了乘车二维码从产生、分发、使用、消费、结算等整个生命周期的安全。二维码支付不仅适用于地铁乘车过闸，在公交扫码支付、高速扫码支付等交通领域同样适用。

6. 企业分工

武汉地铁扫码乘车方案中二维码安全的国产密码应用由北京信安世纪科技

股份有限公司参与的方案设计、方案实施、项目上线保障等工作。方案适用的产品清单如下：

序号	供应商	产品名称	数量	单位
1	北京信安世纪科技股份有限公司	SZT1901 信安数字证书认证系统	3	套
2		Linux ARM 平台安全中间件	1	套
3		SJJ1515 信安应用安全网关系统	3	套
4		SRJ1913 信安数字签名服务器系统	3	套
5		SHT1733 信安移动统一认证安全管理平台	3	套
6		SHM1705 移动安全中间件 MSDK	1	套
7		定制开发服务	1	项

7. 应用案例

武汉地铁上线二维码乘车半年，注册用户 200 万，签发了数字证书 200 万张，每天使用二维码乘车交易量约 40 万笔。项目的安全稳定运行进一步落实了地铁信息安全战略和产业发展规划，促进了我国信息安全密码产业在技术、市场、服务、品牌的整体提升。

北京信安世纪科技股份有限公司

联系人：邵素芬　　康茹

电　话：010-68025518-8118　010-68025518-8531

测绘行业密码应用解决方案

1. 概述

地理信息资源是国家重要的基础性、战略性信息资源，事关国家安全和战略利益，广泛应用于经济建设、社会发展和国防建设。近年来，随着地理信息应用的不断深入和普及，地理信息采集获取、网络传输、加工处理等日益智能化和自动化，地理信息行业投资主体与应用主体渐趋多元化、复杂化，给地理信息的安全保密带来严峻挑战，亟需通过密码应用等手段提高信息安全防护水平。

2. 需求分析

由于采用专线方式进行数据的建设成本过高，现多采用互联网，或互联网+VPN 方式进行数据回传，这为整个系统带来安全隐患。一是，采用互联网回传数据，测绘核心业务系统必须直接或间接（通过防火墙的“端口映射”）暴露在互联网上，这为潜在的攻击者带来可乘之机。二是，地面基准站依靠普通路由器进行拨号数据上传，存在终端被劫持的安全隐患。随着《网络安全法》的颁布，以及《测绘地理信息领域重要信息系统商用密码应用规划（2016-2020 年）》的实施，急需从潜在安全隐患、安全合规两个维度提升测绘信息系统的安全性。

3. 方案架构

以国产商用密码技术为基础，结合安全认证管理系统、安全接入网关、安全接入终端设备等商用密码产品的应用，通过网络化实施，实现无需定制开发即可满足基准站与数据中心之间的身份鉴别、通信加密等安全需求。

3.1 技术架构

本次方案设计的整体架构如下图所示：

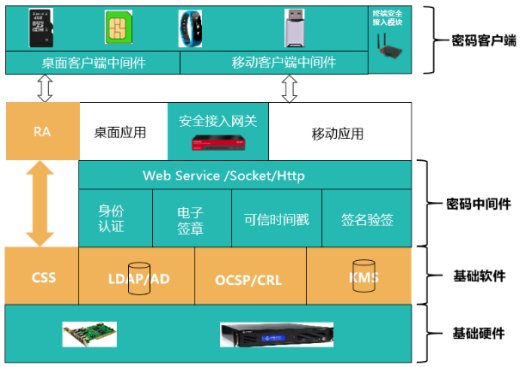


图 3-1 方案设计框架图

3.2 产品部署图

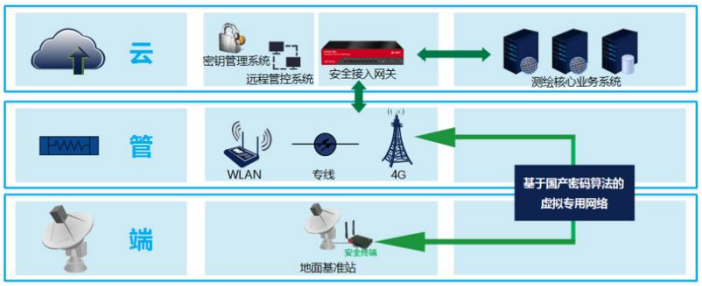


图 3-2 测绘行业基准站远程数据加密回传解决方案

如上图所示：安全终端与安全接入网关之间在互联网、VPN 连接的基础上，利用内置的商用密码安全芯片，对通信链路进行加密，算法采用国家密码管理局审批的 SM1/SM4 对称算法。同时，安全终端与安全接入网关之间利用国产商用非对称密码算法 SM2 实现双向身份认证，确保终端不被劫持、伪造。

安全接入网关可以采取主路/旁路部署模式，部署在数据中心的网络边界处，只有通过安全接入网关的身份认证才能访问到核心业务系统，从而实现了核心业务系统的隐藏，降低了暴露面。

该方案的部署不改变系统的原有拓扑结构，不需要定制开发，通过将密码设备网络接口化的实现机制，降低了实施成本，提升用户的接受程度。

3.3 主要功能

- 身份标识:采用 PKI/CA 系统颁发的数字证书作为系统中用户的身份标识。
- 身份鉴别：身份认证机制基于 PKI/CA 数字证书认证体系，采用数字证书作为整个系统中所有实体的身份标识，采用国密的 SSL VPN 协议作为身

份鉴别协议，通过双向身份认证确保系统中各实体身份的合法性。

- 访问控制：该方案中涉及的安全接入网关以及安全接入终端的访问控制采用基于 RBAC 的强制访问控制机制。

3.4 主要技术指标

以方案中的安全接入网关设备为例，其主要技术指标如下：

- 支持证书类型：符合国家密码管理局《基于 SM2 密码算法的数字证书格式规范》的公钥证书。
- 支持算法类型：支持 SM2 密码算法，密钥模长 256；支持 SM3 密码算法；支持 SM1 密码算法；支持 SM4 密码算法。
- 性能指标：256 位 SM2 签名速度：8000 次/秒；256 位 SM2 验证速度：4000 次/秒；随机数生成速度：20Mbps。

4. 方案特色

基于国产密码算法的 CA 系统作为身份认证信息生命周期管理机制；基于 SSL 协议的双向身份鉴别机制；基于硬件特征码的终端准入机制；基于“协议白名单”的行为准入机制；以“硬件型接口”代替软件接口型设计；一次一密，加密机制更安全。

5. 适用领域

该方案主要适用于测绘行业以及其他涉及信息资源加密传输的应用场景。目前世纪先承已经在测绘行业具备了一定的项目实施经验。

6. 企业分工

此类应用案例公司在实施阶段主要负责如下工作内容

（1）梳理用户的网络拓扑结构，根据网络实际情况设置安全接入方式。

（2）根据安全接入终端和安全接入网关的工作特性，结合用户的网络拓扑

结构在不破坏用户合理的网络拓扑结构的情况下设计有效的安全接入方式。

（3）根据实际需要对提供的产品进行统一的命名，方便管理。

（4）安全策略制定：安全设计方案保护安全接入网关和网络免受非法用户以及垃圾流量的攻击，按保护对象分主要包括以下几类：WEB 管理界面控制；远程 SSH 控制；本地防火墙策略设置；关闭无用服务端口。

该方案所涉及的产品以及相关技术指标如下表所示：

产品名称	产品图片	关键指标	应用场景
安全接入网关（数据中心版）		产品形态：2U 机架式；网络接口：千兆，2WAN+4LAN 最大并发连接数：200 万；国密算法：SM1/SM2/SM3/SM4 加密性能：SM1: 410Mbps SM4:150Mbps； 安全功能：SSL VPN，防火墙，安全审计； 并发用户数：50-1000	数据中心
密钥管理系统		产品形态：嵌入式硬件；网络接口：千兆，2WAN+4LAN 国密算法：SM1/SM2/SM3/SM4；安全功能：密钥颁发，密钥撤销，安全审计	数据中心
安全终端（工业现场版）		产品形态：嵌入式硬件；网络接口：百兆，1WAN+1LAN 无线协议：802.11 b/g/n；国密算法：SM1/SM2/SM3/SM4 加密性能：SM1:3.38MBps SM4:337KBps； 安全功能：SSL VPN，防火墙，安全审计； 并发用户数：1-10	工业数据采集 物联网 智能家居
安全终端远程管控系统		产品形态：嵌入式硬件；网络接口：千兆，2WAN+4LAN 系统管控：固件升级、进程管理；网络管控：上行网络设置、下行网络设置 IP 地址设置；安全设置：准入规则设置、安全连接设置密钥更新	数据中心
客户端软件		产品形态：软件；支持平台：Android,iOS,Windows,Linux 国密算法：SM1/SM2/SM3/SM4；密码设备：TF 卡,UKEY,软件实现（SM1 除外）	定制开发

7. 应用案例

目前该方案已经在广西壮族自治区测绘地理信息局、广东省测绘地理信息局以及云南省测绘地理信息局进行了具体的应用，用户反响良好

北京世纪先承信息安全科技有限公司

联系人：魏华飞　　李宗伟

电　话：18611199112　18611370032

010-62967270　010-62967270

区块链电子发票密码应用解决方案

1. 概述

电子发票作为新兴产业，自 2013 年开始试点，2015 年国家税务总局在全国范围内推广，电子发票开票量逐年上升，2018 年开票量已经达到 30 亿张。但是电子发票仍然存在一些挑战，如网络安全的真实性问题，即易于复制和打印，重复报销问题；众多平台标准不统一，数据无法共享问题；以及电子发票的隐私保护安全等问题。

区块链电子发票密码应用解决方案为电子发票相关问题提供了新思路，利用区块链分布式去中心化，不可篡改，高度透明的公共账本等特性，解决目前电子发票在流转过程中共享难、归集难，报销难、监管难等问题，对电子发票的安全应用具有重要意义。

2. 需求分析

利用区块链技术实现电子发票系统，要解决电子发票用户身份认证、业务通信安全、数据隐私保护等问题

（1）电子发票平台需要对用户进行身份认证和访问控制，保证身份真实且具有访问权限的用户对电子发票平台进行操作，防止未授权用户恶意操作。

（2）电子发票平台需要解决在各个系统流转过程中的数据传输安全问题，确保发票数据的完整性、一致性和不可抵赖性。

（3）电子发票平台需对发票票面信息进行签名加密，在对部分发票信息做隐私保护的同时形成参与各方的完整签名服务链条。

3. 方案架构

3.1 技术架构

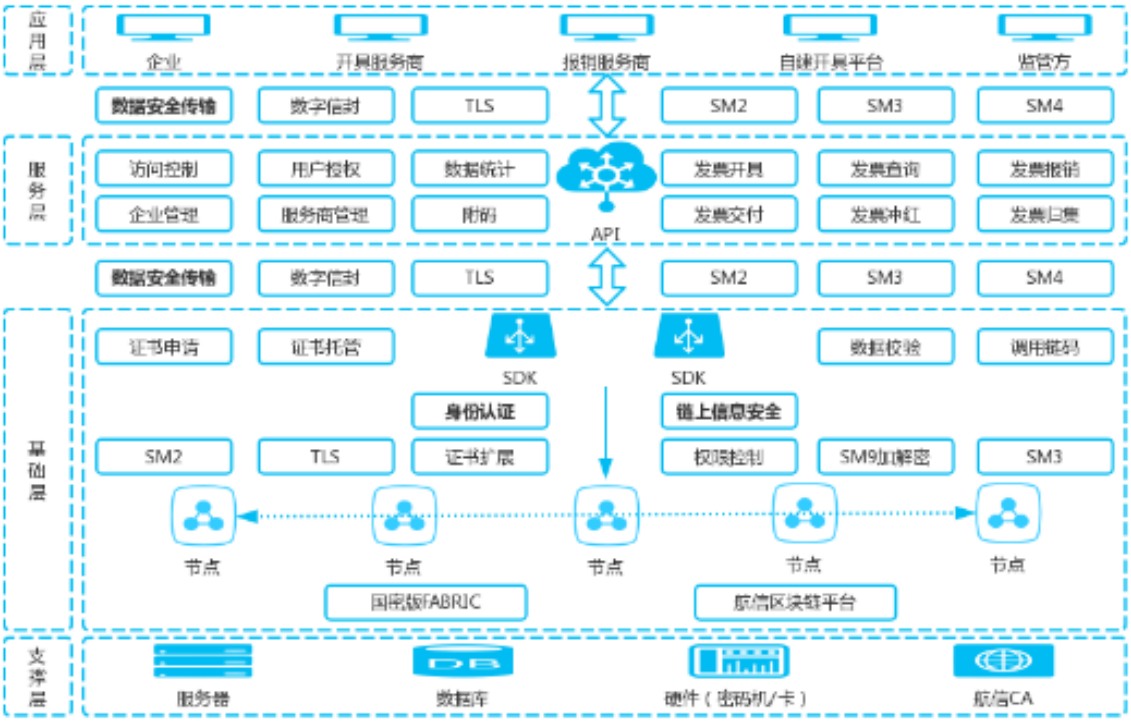


图 3-1 技术架构图

区块链电子发票方案是一种基于联盟链建立的跨机构技术解决方案，联盟链是需要注册许可的区块链，具有一定的准入门槛。通过对联盟成员进行严格资质审核，控制节点数量，确保数据只在一定范围内可访问，从而避免了恶意节点带来的数据泄露风险，同时对重要数据进行隐私保护，只有在特殊节点上，才可查看隐私数据，其他节点只能看到数据摘要，故保证了隐私数据的安全性。

区块链电子发票采用国密 SM2、SM3 和 SM4 算法，符合国内安全可靠政策需求。为企业颁发基于国密 SM2 算法的数字证书，区块的哈希摘要值通过 SM3 算法运算，各区块链节点之间通过国密 SM2 和 SM4 算法的数字信封机制保障通信安全。同时，支持第三方 CA 属性证书及基于角色的访问控制模型，支持细粒度的权限管理。采用 PKI+IBC 相结合的隐私保护机制，PKI 数字证书可以实现强的身份认证，而 IBC（国密 SM9 算法）标识密码可以简便加密，可以较小的代价保障网络安全。

3.2 产品部署图

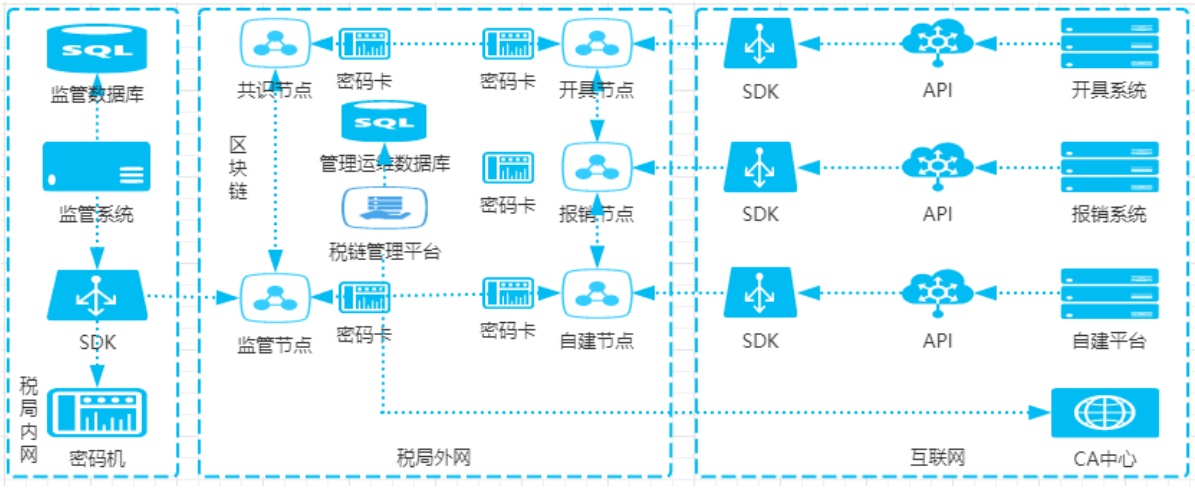


图 3-2 产品部署图

整个系统部署情况如上图所示：

（1）税局内网部署监管系统及配套设备。监管系统监控整个区块链平台运营状况，通过 SDK 组件同步链上监管节点数据，从监管节点获取账本里的交易数据，并调用密码机进行隐私保护。

（2）税局外网部署区块链管理系统和 API 接入平台。管理系统管理区块链电子发票平台基础环境，API 接入平台为其他平台节点提供标准业务接口，区块链环境密码算法依靠加密卡实现。

（3）互联网部署开具系统、报销系统以及自建平台，作为节点可根据相应权限通过 API 平台执行交易请求，各节点使用密码卡加解密。监管系统和区块链管理系统需要调用航信 CA 平台执行证书相应操作。

3.3 主要功能

区块链电子发票平台由 3 个子系统组成，各系统业务功能如下：

（1）区块链电子发票开具系统为企业提供电子发票开具、查询、管理等服务，主要功能包括发票开具、交付、查询、商品管理、客户管理等。

（2）区块链电子发票监管系统主要面向税局用户，涵盖“管理+审计”功能，税务管理功能包括企业管理、服务商管理、发票管理及票源管理等关键业务。系统运维审计功能可以审计节点日志，同步节点数据，监控节点行为，支持自定义

告警规则并据此进行报警预警，支持对异常节点进行锁定、暂停、注销等操作。用户也可自行创建数据导出模板，创建可视化视图，用以更直观的查询和分析审计数据。

（3）区块链电子发票 API 平台实现开具服务商、报销服务商、自建企业平台的接入，提供标准的发票业务接口，包括发票开具、归集、查询、报销申请、报销状态更新等。

3.4 主要技术指标

（1）开发一套基于区块链的电子发票系统，包含电子发票开具系统、电子发票监管系统、电子发票开放平台系统。

（2）支持不少于 100 个共识节点以及 100000 个受票企业；发票查询以及企业信息查询、报销记录查询延迟小于 5 秒；节点达成共识小于 30 秒。

4. 方案特色

本方案相对于传统电子发票解决方案有如下优势和特点：

（1）对电子发票全流程进行管理。通过区块链技术对电子发票全生命周期包括领票、开具、流转、报销等进行记录和管理，实现电子发票全流程的可追溯。

（2）实现各平台间的发票信息共享。作为区块链节点，各第三方平台遵守相同的技术标准和协议，在区块链网络上进行互联互通，到达服务分离，最终实现信息共享。

（3）协助税局对电子发票的有效监管。作为区块链中的监管节点，税局拥有较高权限获取发票数据进而对数据进行分析，实现税局对电子发票低成本、高效率、可信赖的穿透式监管。

5. 适用领域

区块链电子发票密码应用解决方案具体业务场景如下：

中小型开票企业可通过网页、手机 APP、客户端等多种方式开具电子发票，大型企业可按照标准接口进行现有系统对接。同时发票申领、纳税抄报等环节在

线完成，纳税人无须往返税务机关办理。

受票方通过邮箱或短信接收发票信息，并可随时登录平台查询下载发票文件，也可与企业内部 ERP 系统相结合直接报销入账。

税务机关对企业信息、发票票源进行管理，对发票数据进行查询、分析，自动预警，及时发现违法违规情况。

6. 企业分工

区块链电子发票解决方案全部由航天信息股份有限公司完成。

6.1 标识密码机(SJJ1631 SM9)

标识密码机主要实现标识与密钥的转换，提供各类传统密码算法与 SM9 标识密码算法， SM2 签名速度≥6000 次/s、SM2 验签速度≥3000 次/s、SM9 签名速度≥1500 次/s、SM9 验签速度≥600 次/s SM3 杂凑速度≥300Mb/s、SM4 加解密速度≥250Mb/s。产品规格为 482*650*89mm。

6.2 江南天安密码卡（E4A-251-M1）

密码卡负责密钥管理，包括消息验证、数据加密、签名的产生和验证等。支持 SM2 算法，签名速度为 80000tps，验签速度为 25000tps。SM3 杂凑速度≥1200Mb/s、SM4 加解密速度≥1000Mb/s、产品规格为 200*68mm。

7. 应用案例

2018 年 1 月，依托青岛税局作为监管方，试点工作顺利开展并成功接入第三方服务商与财务软件；4 月在北京、青岛、安徽、湖北、宁夏成功完成了系统的部署和联调，目前区块链节点 18 个，入链发票 100 余万张。

航天信息股份有限公司

联系人：李旻实

电　话：13811922871　　010-88896560

金融行业

网上银行蓝牙型智能密码钥匙密码应用解决方案

1. 概述

网上银行是传统银行业与现代信息网络技术紧密结合而形成的一种新型的金融形态。为了保证这一新形态的良好发展，近些年来我国陆续颁布了一系列的法律规范其发展，例如，《中华人民共和国电子签名法》、《电子银行业务管理办法》等。在法律的推动下，基于国产密码的安全产品被越来越广泛的应用在金融领域。

2. 需求分析

互联网特别是移动互联网已经成为现代社会生活中不可或缺的一部分，但随着互联网的发展，使用者在进行网上交易和通信时，其信息安全日益受到网上黑客、网络侦听设备、病毒及其它形式的威胁。金融领域作为国计民生的基础领域也暴露在这样的危险下，伴随着网上银行的普及和越来越的客户选择使用手机银行，对网上银行和手机银行的转账环节攻击成了重点“灾区”，例如，钓鱼网站骗签导致了所见非所签，而基于传统的手机短信码和动态令牌的转账交易保护形势已经无法适应新形势下的安全威胁。

在这种背景下，我公司研制了新型蓝牙 KeyPod 产品，商用密码产品型号 SJK1447，以应对越来越复杂的使用环境，保证银行用户在进行转账操作时的资金安全。

3. 方案架构

3.1 技术架构

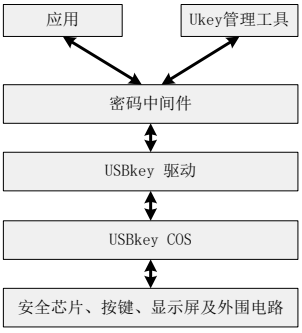


图 3-1 产品架构图

COS（片上操作系统）：COS 是 USBKey 的关键。COS 是位于安全芯片中的一套嵌入式软件程序。

密码中间件：USBKey 属于安全产品，必须为应用者提供安全的密码服务，为众多上层应用提供统一的调用接口。

3.2 产品部署图

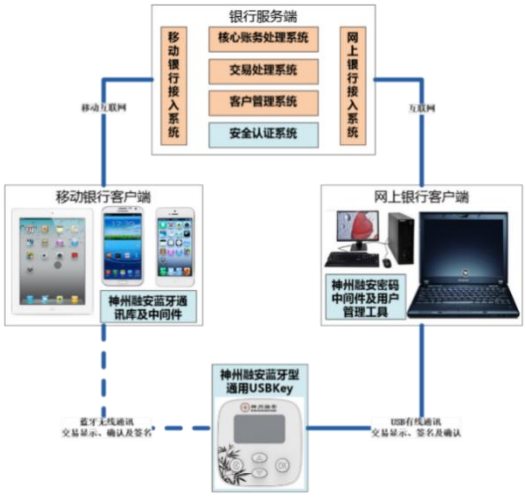


图 3-2 产品部署图

3.3 主要功能

跨终端使用：采用 USB + 蓝牙双重通信协议既能够支持传统 PC 网银使用又能够支持移动端的手机银行使用。

可信执行和运算：基于国产密码算法，在可信终端显示签名内容、确认签名内容、输入敏感信息、保护敏感信息，保障身份认证和交易过程安全。

可信显示：采用了按键和 LCD 显示屏的设计，通过增加输入和输出功能提供一种可交互的使用环境实现所见即所签。

3.4 主要技术指标

本产品支持 SM2 证书存储，最多支持存放八张证书（签名证书和加密证书）及其对应的密钥对。

1、性能指标：

- SM2 生成公私钥速度 ：0.1 秒/次
- SM2 签名速度：20 次/秒
- SM3 算法性能：650Kbps
- SM4 加密速度：299Kbps
- SM4 解密速度：298Kbps

2、安全中间件支持的操作系统及浏览器：

- WindowsXP 及以上版本的操作系统、MAC OS X 10.6 及以上系统、Linux 系统、国产麒麟系统、IOS6.0 及以上系统、Android4.4 及以上系统。
- IE 浏览器、Edge 浏览器、Firefox 浏览器、Chrome 浏览器、Safari 浏览器以及其它主流浏览器。
- 硬件接口符合 USB 1.1 规范，在 USB1.1、USB2.0 或 USB3.0 接口上都能正常工作；支持经典蓝牙协议和蓝牙 BLE 协议。

4. 方案特色

4.1 系统设计的安全性

产品在硬件设计上充分考虑安全因素，选择安全可靠的元器件作为核心组件来组成和实现产品，在功能设计上需要从安全的角度出发来考虑和完善产品的功能。

系统设计遵循国产密码技术应用规范，采用支持国产密码算法的安全产品，

设计具有自主技术、自主知识产权的安全产品。

4.2 系统的可靠性

作为提供给银行使用的安全认证类产品其使用必须可靠，能够满足不同人群、不同环境、不同气候的使用，在保障安全性的条件下，提供可靠的功能。在异常操作或误操作的情况下，产品能够自动回复到安全状态，并能继续提供正确的功能。

4.3 产品的可操作性

大多数产品用户是计算机的普通使用者，这些用户的日常使用习惯和安全知识、计算机知识参差不齐，更多追求应用的便捷性和易用性，而在这些特性上很多方面是和安全性相矛盾的，因此需要在系统设计上平衡这两者之间的关系，在首先保证安全性的前提下兼顾考虑用户的体验。例如，蓝牙快速无感连接技术，能够极大的提升用户使用手机银行的满意度。

4.4 系统的可维护性

产品的设计一般伴随着升级，尤其是软件产品的升级是相对普遍的，产品设计时，必须考虑后期产品的维护升级。另一方面，产品设计时，考虑产品可能存在的问题，进行模块化设计，方便产品模块的升级，减少模块升级引起的系统风险，提升产品可维护性。

5. 适用领域

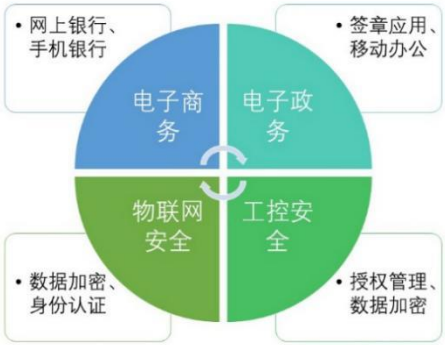


图 5-1 适用领域

6. 企业分工

以银行为例，在项目实施过程中融安会根据银行自身的业务需求对项目实施定制化的开发，以保证能够完美的兼容银行的现有系统，主要工作如下图 6.1 所示：

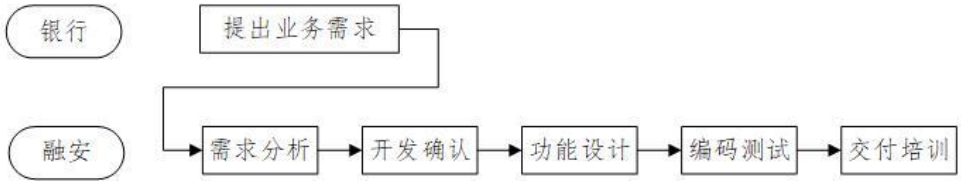


图 6-1 实施流程图

7. 应用案例

中国农业银行、吉林省农信联社、湖南省农信联社、青海省农信联社、广州农商银行、长城华西银行、温州银行、黄河农商行等。

神州融安科技（北京）有限公司

联系人：岳云龙

电　话：15801143145

010-62127688

网上/手机银行密码应用解决方案

1. 概述

随着信息化与传统银行业的深度融合，近年来网上银行的发展突飞猛进，呈现出用户规模不断扩大、交易规模阶跃式迅速增长、网银替代率增加的显著特点，据统计网银业务的广泛应用使得银行柜面业务替代率已达到 80%以上，并且还在不断地发展。银行本质是经营风险的企业，提供服务的过程中必须管控好各类风险，才能更好地为用户服务。

中国人民银行科技司关于征求对《网上银行系统信息安全通用规范》修订版通用意见的函（银科函【2011】130 号）中指出经第三方中立测试机构检测通过的 OTP 令牌，可以作为网上银行或手机银行的专用安全设备使用。

国家密码管理局也出台了《动态口令认证密码应技术规范》，对一次性动态口令密钥管理、生产加工等方方面面做出了明确要求。依托于该规范，密码企业必须使用国产密码算法对网上银行进行交易保护，避免了因非国产密码算法漏洞后门等带来的风险，有效的保护了交易安全。

2. 需求分析

在银行网银系统中的安全防护中，最为核心的就是保障资金的安全，一切安全方案和手段实施的目的都是围绕这个核心。作为一个面向普通用户的应用系统，必须在保证安全的同时，具有足够的易用性，降低使用门槛。

针对网银资金交易的特点，针对资金交易的风险主要体现在：修改交易内容，包括资金的发起方、接受方、额度等关键金融信息，使得攻击者从中获利。

可以综合采用以下技术进行安全防范：

- 信息防篡改：采用数字签名技术，对关键信息进行签名；
- 信息加密：对传输信息进行加密处理；
- 用户方（发起方）确认：针对一笔交易，确认用户身份，可以通过动态口令技术实现。

- 交易绑定：一笔交易一个口令，一次有效。

由于网银交易发生在公共网络环境，其中只有用户手里的令牌是唯一脱离网络环境的安全密码设施，也是保护资金交易的核心安全产品。

3. 方案架构

3.1 技术架构

系统技术框架如下图所示：

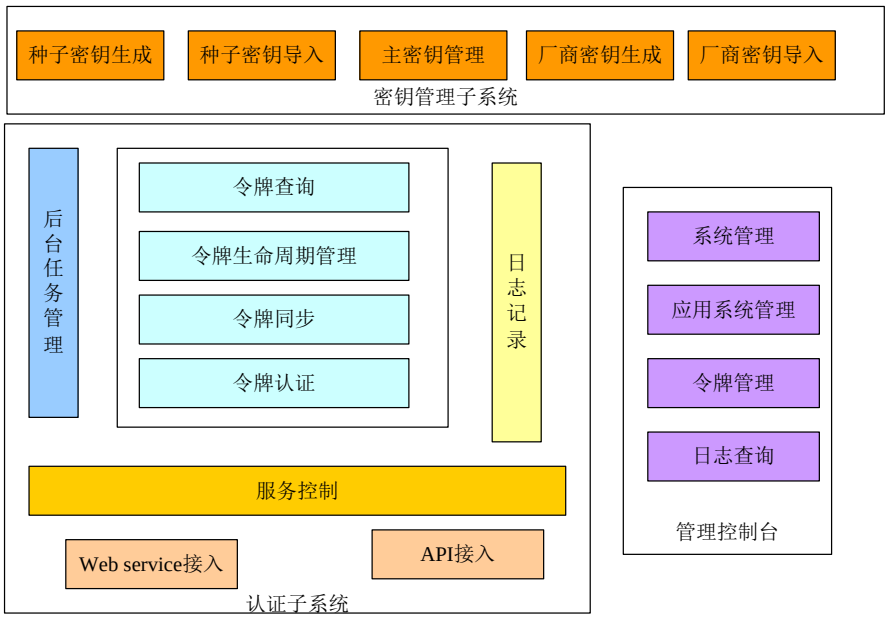


图 3-1 技术架构图

认证时动态令牌负责生成动态口令，认证子系统负责验证动态口令的正确性，密钥子管理系统负责动态令牌的密钥管理，管理控制台负责系统整体管理。

外部应用系统负责将动态令牌生成的动态口令按照指定的协议或使用专用接口 API，将报文发送至认证子系统进行认证，认证子系统对口令进行验证后，将验证结果返回给外部应用系统。

3.2 产品部署图

产品部署如下图所示：

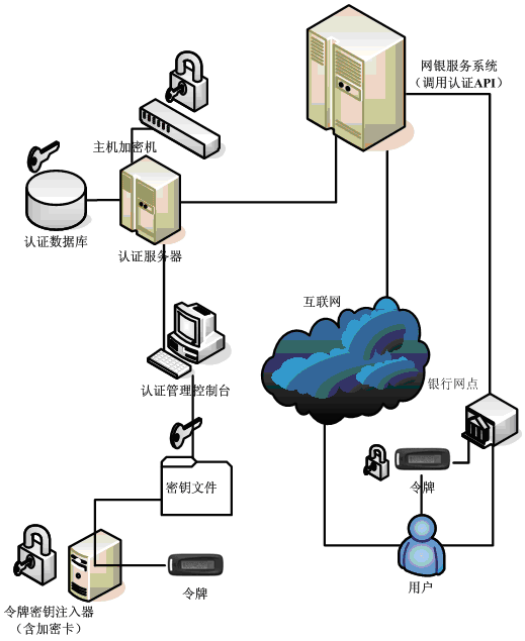


图 3-2 产品部署图

密钥管理：

动态密码身份认证系统的核心密钥生成、传输和存储由主机加密机和卡完成。密钥生产过程的算法和密钥安全由加密卡完成，认证中心服务器的算法和密钥安全由加密机完成，认证中心数据库中密钥数据的安全由加密机完成，密钥文件的传输由加密机和加密卡共同完成。

认证交易过程：

（1） 用户阅读令牌上当前分钟的动态密码；

（2） 用户通过银行网银系统向认证中心发送身份信息、动态密码和静态密码；

（3） 认证中心根据用户的身份信息，获得有效的动态密码、静态密码和接收到的内容进行对比，确认用户身份。

3.4 主要功能

如前所述，本方案的核心就是保护用户资金交易安全，当用户发起资金交易时，必须输入动态口令，该口令由用户携带的动态口令牌产生，动态口令牌与用户账户捆绑，可以唯一确认用户身份。同时在交易系统中，该口令与一笔交易唯一捆绑，具有唯一性，一次性，可以确保资金交易安全可靠。

3.5 主要技术指标

（1） 认证服务速率：>=3000TPS；

（2） 令牌时间漂移：<=120s/年；

（3） 口令变动时间：60s；

（4） 令牌连续工作时间：>=5 年。

4. 方案特色

算法国产化

本方案密码运算采用国产算法 SM3，在商用密码体系中，SM3 主要用于数字签名及验证、消息认证码生成及验证、随机数生成等，其算法公开。据国家密码管理局表示，其安全性及效率与 SHA-256 相当。

密码计算硬件化

OTP 令牌采用国产密码芯片，芯片经国家密码管理局检测并认证，具有高保密性和安全性。

交易一次一密

OTP 时间窗口为 60 秒，SM3 计算的密码一次有效，用后即失效。

交易终端无关性

本方案对最终客户使用的终端不进行限定，PC、平板、手机都可使用，终端的不同操作系统均可使用。

5. 适用领域

本方案适用于金融、电信等需要对交易安全进行高等级防护的场景。同时也可作为身份认证的第二因素使用。

6. 企业分工

本方案涉及产品使用方（如银行）、产品方案商（国密企业）和电子加工厂。其中产品方案商负责产品设计、组织生产、发货到使用方；电子加工厂根据方案

商的要求，在保密设备（加密机）的环境下生产加工产品；使用方按照重空凭证对产品进行接收、检验、发放和使用。

产品清单：OTP 令牌、产品签收单、合格证。

7. 应用案例

中国银行网上银行项目

北京集联网络技术有限公司自 2011 年起，在中国银行网上银行项目中共发放了 3000 多万只 OTP 令牌，极大地促进了网上银行、手机银行的发展，保证了交易安全。

中国邮政储蓄银行网上银行项目

中国邮政储蓄银行网上银行采用了 OTP 令牌+Ukey 的方式进行推进，我司到目前为止共提供了近 600 万只 OTP 令牌，使用效果良好。

北京集联网络技术有限公司

联系人：赵秋霞

电　话：13911634751

62963311-305

金融行业动态口令密码应用解决方案

1. 概述

随着互联网的迅速发展，电子交易越来越普及。电子交易的应用包括：电子银行（网上银行、ATM 应用、POS 应用、电话银行、手机银行、卡支付）、网上证券、第三方支付、电子商城等。

金融行业电子交易业务由于其独特的虚拟性和广域性，在为客户提供高效便捷服务的同时，也要面对来自外部、内部的各种风险。 由此产生了一系列安全认证设备产品，例如：动态令牌、短信令牌、刮刮卡、手机软令牌、挑战应答令牌、证书等。

监会办公厅银建办发[2013]242 号要求:国内银行动态口令密码应用方面应执行国家密码管理局颁布的《动态口令密码应用技术规范》,动态口令密码平台需要满足此规范。

2. 需求分析

近几年来，电子银行的发展从多种电子渠道的并行到融合的趋势，渠道的融合可以使业务发展和营销更加灵活。为了更好地支持各种电子渠道的业务发展和融合，需要建立一套适合于所有电子渠道的统一认证平台，来统一处理用户的认证、交易的认证、风险监控和防范、统一的日志等。

具体需求如下：

- 使用双因素身份鉴别方式
- 用户动态口令一次一密
- 使用动态口令对用户身份鉴别进行保护
- 使用动态口令对用户的交易行为进行保护
- 令牌首次使用之前需进行激活，激活后令牌种子发生变化
- 令牌不能被未授权用户盗用
- 统一身份鉴别

建立的动态口令证平台、要支持动态令牌跨渠道应用及跨令牌厂商的令牌管理，以及满足监管要求。

3. 方案架构

动态口令认证平台为三层架构，如下：

3.1 技术架构

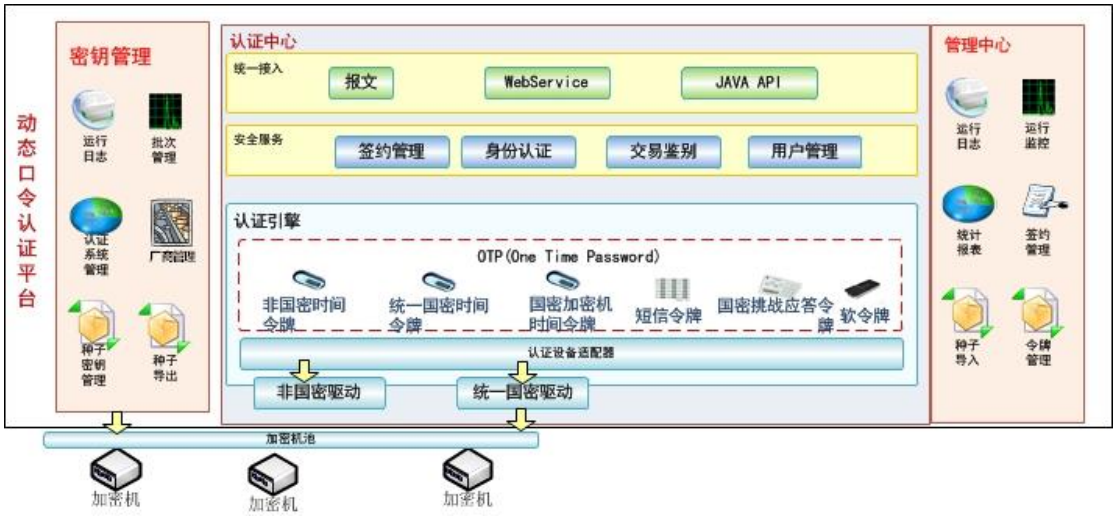


图　3-1 技术架构图

平台分为密钥管理中心、认证中心、通用管理中心三个模块；对外提供 JAVA/C/PYTHON 多种开发语言的 API 满足不同应用渠道的接入；内部支持国密标准算法，国际算法的驱动满足不同监管要求；令牌的种子密钥由加密机生成。

3.2 产品部署图

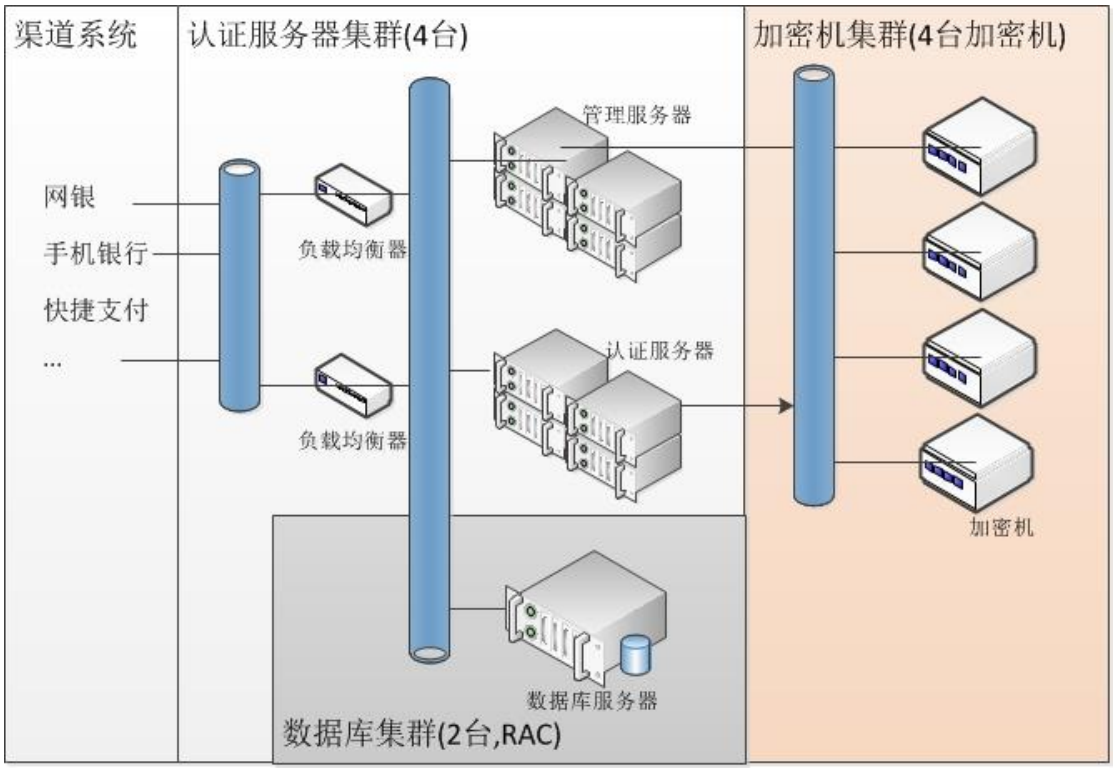


图　3-2 产品部署图

认证和管理独立部署，保证使用的应用、数据库、加密机高可用性。

3.3 主要功能

平台要具有种子管理、令牌厂商管理、令牌类型管理、认证服务、日志操作等功能。

密钥管理系统：密管系统是用于动态口令令牌种子密钥生成、存储和分发的安全管理系统，其中种子密钥的生成和传输需要与动态口令加密机共同完成，保证种子密钥妥善保护。

认证中心：整个平台的核心，对外提供统一的接口和多种协议，快捷方便地有有所需的客户系统接入。

通用管理中心：以 web 形式提供管理界面，为用户提供认证工具数据的维护、日志、报表、统计和用户关系的查询。

3.4 主要技术指标

口令认证的交易每秒处理量大于 3000 秒。

4. 方案特色

算法安全

国产密码算法支持(SM3/SM4),动态口令 GM 标准支持(GM/T 0021-2012)。

首次使用激活

用户首次使用之前需进行激活，激活目的：

验证令牌是否正常工作无损坏。

更新令牌内部及系统后台种子密钥，保证种子密钥不会在生产环节泄露。

模块化安全服务

不影响现有业务前提下快速增加一种认证设备。

自适应认证

分析用户行为智能调整用户认证策略。

5. 适用领域

动态口令认证平台广泛应用于银行、券商等金融领域的电子交易以及大型企业内部办公系统的建设。

6. 企业分工

项目实施中各企业负责采购相应型号的加密机。

7. 应用案例

动态口令认证平台成功应用于国有大型银行、商业银行以及券商和企业，以中国银行为例 ：

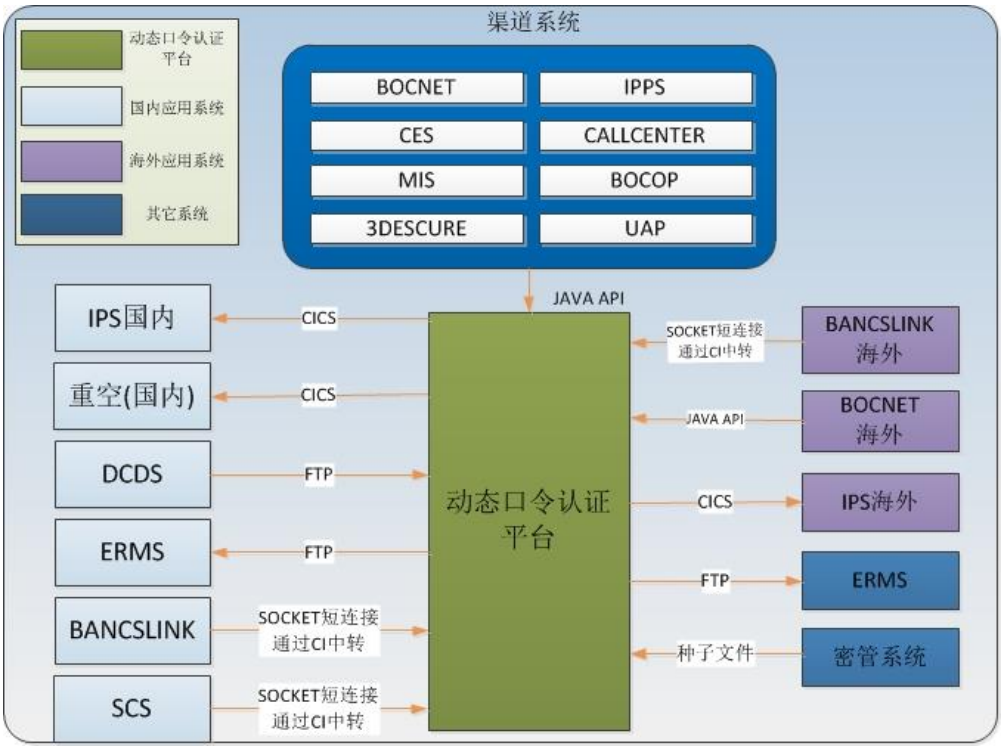


图　7-1 案例架构图

该平台是中国银行的基础认证平台，国内、海外亚太、欧非、美洲区的网上银行应用系统使用其认证服务，包括 BOCNET、管理信息服务平台 MIS、3Dsecure、账号支付 IPPS、电话银行 CALLCENTER、中银开放平台 BOCOP、UAP、CES 等多个渠道系统接入。

北京宏基恒信科技有限责任公司

联系人：章雄健　　潘斌

电　话：13552403987　13901366308

010-65546118　010-65546118

金融行业统一密码认证平台安全解决方案

1. 需求分析

随着我国改革开放的不断深入和社会主义市场经济体制的逐步建立，国家信息化进程不断加快，国家经济、管理、社会事务以及公民个人信息在存储和传输过程中的安全问题日益突出，使用国密保护非国家秘密信息的需求越来越强烈。

在金融行业中,安全是金融信息系统的生命,金融信息的安全是根据金融系统的实际应用而定的,它可以将密码学、密钥管理、身份认证、访问控制、应用安全协议和事物处理等信息安全技术综合在金融信息系统安全工程中加以运用,并且可以在系统运行的过程中发现并纠正系统所暴露出的安全问题。金融行业为用户提供多种线上服务的同时，也面临更多的密码、数据、业务安全威胁，实现国密在金融领域的全面应用是迫在眉睫。

2. 方案架构

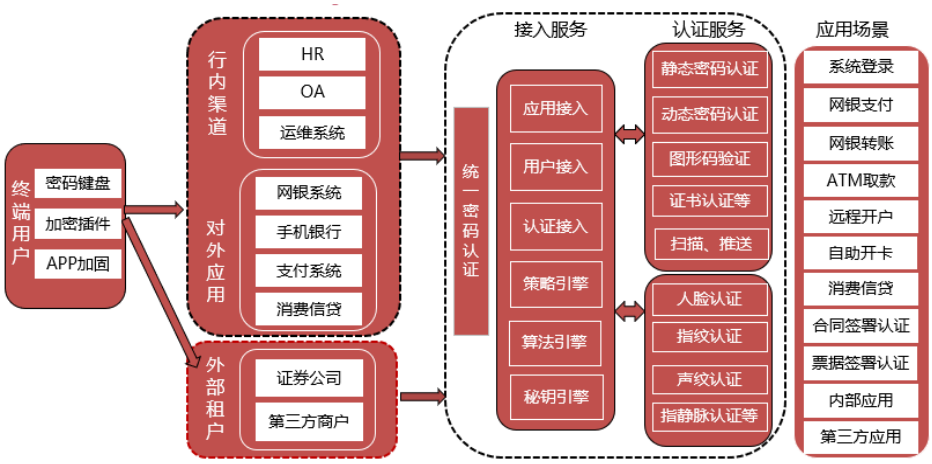


图 2-1 方案架构图

3. 方案描述

综合考虑金融行业管理、认证、安全现状，未来业务应用扩展需求。安讯奔自主研发统一密码认证平台，为金融行业提供一套集统一的用户管理、密码认证管理、客户端安全保护、端到端传输安全、渠道推广为一体的综合服务，解决金融行业最迫切的管理、

认证、安全痛点；实现用户、密码认证和安全的集中管理。通过统一密码认证平台对金融行业内部系统、外部系统和外部租户提供多种密码认证服务，无需应用系统直接对接多种密码认证引擎。具体的用户需求和对应的解决方案见下表：

用户需求	解决方案描述
统一用户	整合用户在各应用系统中的账号，统一为同一客户号，并统一密码。
统一密码认证方式	整合各种密码认证方式：静态密码、动态密码、证书认证、行为验证码、指纹、人脸、声纹；使渠道统一同密码认证平台交互，不再各自同多种认证服务直接交互。 用户开通某种认证方式后，其他系统可通过授权方式全部开通，无需再单独注册用户名、密码。
统一认证、授权	通过统一入口，进行联邦单点登录，根据用户身份、已开通服务，分配用户相关权限，进一步进行渠道整合、渠道协同。
密码安全	输入安全：通过密码驱动级密码键盘防护，保证密码输入时的安全；国密存储保障，端到端国密传输加密保障 传输安全：在现有 SSL 加密通道基础上，基于服务端生成密钥对的方式，前端通过非对称加密算法，加密密码或敏感信息，一次一密，实现端到端数据安全。
组合认证	可根据认证策略设置，不同业务场景、状态下，使用不同认证方式，或组合认证方式。
服务端密码加密	密码通过加密机加密存储，密钥存储在加密机中。
密钥算法管理	支持多种密钥算法（国密、商密）管理，可根据需求配置相关算法。同时支持与银行加密机 HSM 的无缝集成。
生物特征值管理	支持生物密码特征值存储和管理，可根据需求动态更新特征值。
云平台服务	可对内部应用、外部应用提供平台服务；同时可以租户方式对第三方进行服务输出；
移动端安全	安讯奔提供移动端安全加固技术，保证移动端环境安全。

4. 方案优势

统一密码认证平台，通过统一用户、认证通道，使业务系统和认证引擎分离，业务系统同统一密码认证平台交互，实现业务系统和认证的松耦合，密码认证引擎服务更新，业务系统不再需更新；生物密码、非生物密码方式以模块化方式嵌入统一密码认证平台，接入新的密码认证方式（如指静脉），不影响现有密码引擎服务。

统一密码认证平台，可用于多种应用场景进行身份认证和鉴别：登录、交易、远程

开户；电子合同签署、电子回单查询、身份验证确认电子票务真实性等。

认证策略管理，可提供多种密码规则：一、静态密码长度、复杂度、更新周期等；二、不同业务场景采用不同强度的密码认证组合，如登录时静态密码认证，大额交易时“动态口令+人脸识别”；三、用户应用环境异常，也可升级认证强度，如地点异常，加强认证；四、生物密码可根据不同应用场景设置不同阈值，灵活可控。

PC 端交易信息二维码推送至移动端确认的认证方式，可进一步防止交易信息被篡改，保证交易的安全性。

统一用户、统一认证、统一密码方式的基础上，进一步进行渠道整合、协同。

移动端安全加固，Root/越狱检测、检测进程完整性、检测键盘记录器、检测调试程序、检测模拟器，防止系统发起的屏幕截图，保移动端应用环境安全。

5. 适用领域

适用于全球性或区域性金融机构、政府机关和大型企业等。

6. 部分成功案例

花旗银行、恒丰银行、兰州银行、北京银行、哈尔滨银行、上海银行、恒丰银行、郑州银行、张家口银行、唐山银行、中关村银行、德阳银行、浙江农信、宁波银行、鹿城农商行、中国机械设备工程股份有限公司、北京电视台等。

北京安讯奔科技有限责任公司

联系人：詹錦莊

电　话：13928090400

金融业务系统国产密码应用解决方案

1. 概述

2012 年，工信部和公安部通告了 RSA1024 算法被破解的风险，为保证金融行业各基础信息系统安全，中国人民银行要求各银行对网上银行等信息系统进行国产密码算法改造。

2012 年，中国人民银行向多家银行发布了《银行业国产密码应用总体规划》及《总体方案》征求意见稿；同年，人民银行转发了发改委的试点通知并建议网银用户 5000 万以上的银行参与网银系统国密算法改造试点项目。2014 年国务院转发了多部门联合制定的《金融领域密码应用指导意见》（国办发【2014】6 号），要求各金融机构 5 年内完成在网上银行、移动支付、网上证券等重点领域国产密码算法的全面应用。

2. 需求分析

按照中国人民银行关于推进国产密码在金融领域应用的实施方案，银行需在网银系统对安全工具、安全基础设施进行国产密码算法的应用改造，改造需求包括：

- 需使用包含国密数字证书和国密算法的 USBKey（智能密码钥匙）；
- 需使用基于国密算法的动态令牌；
- 需使用通过使用国密专用浏览器建立国密 SSL（Secure Sockets Layer，安全套接层）隧道连接到网银系统；
- 需使用基于国密算法对交易等数据进行电子签名。

3. 方案架构

3.1 技术架构

信安世纪网上银行国密改造方案中，银行可根据具体自身情况选择改造方案，全部涉及或部分涉及国密数字证书、国密动态令牌、单向/双向国密 SSL、国密电子签名四个改造内容。逐步完成国产密码算法在网上银行系统中的使用。本方案技术架构如下图所示：

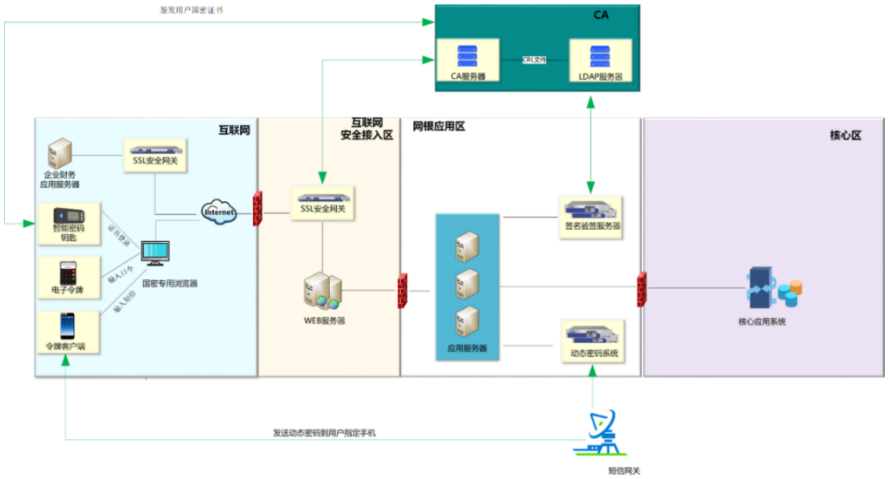


图 3-1 技术架构图

3.2 产品部署图

本方案产品部署图及产品部署区域如 3.1 章节中的技术架构图所示，用户使用 USBkey/动态令牌/动态令牌手机端通过国密专用浏览器登录网银系统，其他需要部署或国密升级的产品包括数字证书系统、SSL 安全网关、动态密码服务器、签名验签服务器。

3.3 主要功能

（1）基于国密数字证书登录网银系统和电子签名

用户 USBkey 存储国密证书和 SM2 算法密钥对，用于登录网银系统和对交易等数据进行国密电子签名，并通过签名验签服务器验证签名，实现身份合法性认证，保证网银交易数据的完整性和不可否认性。

（2）使用动态口令登录网银系统

采用基于国密算法的动态令牌或手机令牌作为客户端密码生成，并与动态密码服务器共同完成动态密码验证。

（3）构建单向/双向国密 SSL

普通用户使用国密专用浏览器、企业财务公司等直连银行的用户使用部署在企业端的 SSL 安全网关与银行端 SSL 安全网关建立单向或双向的国密 SSL 加密网络通道，保证数据传输安全。

4. 方案特色

完整性

本方案提供从客户端安全工具、国密专用浏览器到服务端的全套国密改造安全解决方式。

灵活性

本方案涉及内容可按照银行内具体情况灵活选择和设计国密改造内容，并可分步完成。

无感知

本方案对于最终网银用户是透明的，在用户无感的状态下，实现国际算法和国密算法完美切换。

无改动

本方案对原有网银架构几乎不需做任何改动即可完美实现。

5. 适用领域

此方案除契合银行网上银行系统、移动支付系统等银行信息系统国密改造外，还适用于证券网上交易系统、期货网上交易系统、保险电子保单系统等应用场景。

6. 企业分工

方案内涉及的企业名称、职责、产品及国密型号：

产商名称	职责	产品	国密型号

北京信安世纪科技股份有限公司	提供国密改造方案、实施、安全产品	签名验签服务器	SRJ1904 签名验签服务器
		动态密码服务器	SRT1606 动态令牌认证系统
		动态令牌	SRK1402 动态令牌
		数字证书系统	SZT1901 数字证书认证系统
		SSL 安全网关	SJJ1515 SSL VPN 安全网关
天津赢达信科技有限公司	提供国密专用浏览器	安全浏览器	SHR1601 安全浏览器

7. 应用案例

信安世纪基于此方案协助网上银行国密改造一期 4 个试点中的中国农业银行、民生银行、鹤壁银行完成了网上银行国密改造，并承接了网上银行国密改造二期 30 个试点中的包括建设银行、交通银行、光大银行、北京银行等在内 25 家银行国密改造项目，截止到目前，此方案已在 90 多家银行进行了应用实践。此外，信安世纪对本方案进行了升级和少量修改，用于协助证券行业国密改造一期试点中的银行证券进行国密算法的改造。

北京信安世纪科技股份有限公司

联系人：邵素芬　　康茹

电　话：010-68025518-8118　010-6802 5518-8531

线上业务司法纠纷商业密码应用解决方案

1. 概述

随着移动互联网技术的飞速发展和广泛应用，移动终端成为各类应用的主要入口。金融行业信贷业务也逐步由线下迁移到线上，享受移动互联网带来的用户体验上升、业务受理便捷等好处；与此同时，金融机构法务、风控、业务部门面临一系列困难和挑战，主要包括：

- 传统身份认证机制存在的不足，如 USB Key 携带不便，兼容性差；密保卡、短信验证码存在的安全性强度不足；
- 电子合同需确保与纸质签章、签字合同具备一致的法律效力；同时，电子合同本身提供防篡改和防抵赖；
- 若产生司法纠纷，电子数据面临维权难、举证难及取证难。

在此背景下，以满足《电子签名法》第十三条与第十四条为立足点、以商用密码技术为核心、以便捷性为前提的线上业务司法纠纷解决方案应运而生。

商用密码技术贯穿于解决方案，提供了敏感数据安全性、业务报文完整性、用户身份的真实性、用户行为的防抵赖性、电子证据的安全性和完整性。为移动业务的开展提供了至关重要的安全基石。

2. 需求分析

线上金融业务的开展，依赖于用户身份真实性的校验；用户行为真实意愿的体现，并通过电子合同及电子证据进行记录；纠纷过程中对电子证据的取证，以及基于电子证据的维权。整个过程中，安全需求描述如下，包括安全性、身份认证、完整性、第三方责任认定。

安全性需求

依托移动终端实现数字证书的申请、下载、存储与数字签名，需确保数字证书本身在移动端无法被攻击者复制、监听、盗用。以确保线上业务发生过程中，

只有预期终端设备可产生数字签名，无法伪造。

身份认证需求

为实现用户身份的强认证，使用手机保存的数字证书针对电子报文进行数字签名的同时，用户需提供密码或指纹实现双因素认证。

完整性需求

完整性需求包括两个层面。首先，电子交易报文的完整性，防止攻击者通过劫持移动终端设备伪造交易信息；其次，电子合同的完整性，确保电子合同签署后，任意改动均能够被发现。

第三方责任认定

无论是终端用户还是业务受理机构，都希望能通过中立、可信第三方进行责任认定。一方面，可以在发生业务纠纷时，提供有效的证据供司法裁定；另一方面，可分担互联网创新业务带来的业务风险。

3. 方案架构

3.1 产品逻辑架构图

根据图 1，可组建线上业务司法纠纷解决方案，包括云证通移动证书系统及其配套的集成于移动终端的 SDK、无纸化电子签章系统、电子保全二级系统；同时，数字证书认证服务、时间戳服务、电子保全一级系统、在线取证系统、电子数据司法鉴定中心的以云服务形式介入业务的不同流程；而司法鉴定中心将会对电子证据的 HASH 值进行实时保存，以实现在纠纷发生时，出具电子数据司法鉴定报告。

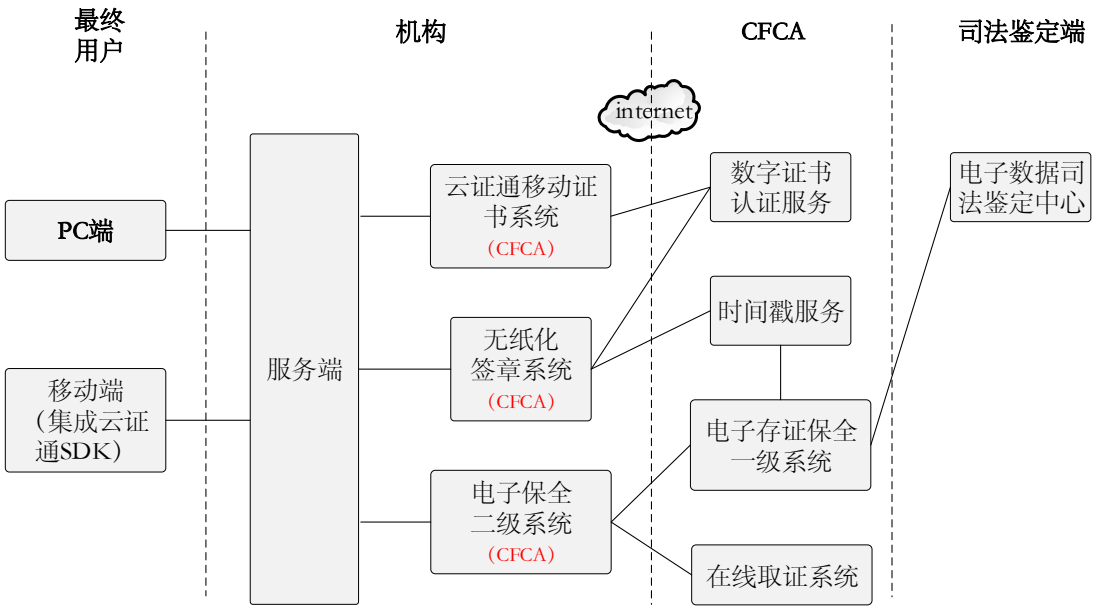


图 3-1 产品逻辑架构图

3.2 主要功能

云证通系统

管理移动终端数字证书的申请，颁发，下载以及数字证书签名等，签名过程中实现设备认证、用户认证、真实意愿认证的有机结合；

无纸化电子签章系统

用以生成具有司法效力的电子合同，使用移动终端数字证书、印章图片对电子合同进行数字签名并合成签章；

二级证据保全系统

业务系统通过集成 API 实现电子数据的签名及固化，电子证据及签名值将被系统保存，相关数据摘要信息将同步至 CFCA 一级证据保全系统用于日后取证。

3.3 主要技术指标

- 全流程使用国密算法，包括 SM2、SM3 和 SM4；
- 移动终端数字证书利用 SM2 密钥分离式保存和使用的相关特性，充分满足《电子签名法》第十三条的相关规定；
- 兼容操作系统为 IOS7.0 及以上、Andriod4.0 及以上的设备；

- 纯软件实现，不依赖于额外物理介质。

4. 方案特色

本方案做为企业开展移动互联网业务的基础设施，具备以下特色：

- 覆盖线上业务全生态链

围绕着线上业务开展的全生态链的整体解决方案，包括业务受理、电子证据固化、电子签名法落地、争议与纠纷化解等。确保线上业务合法、合规地开展，有效化解线上业务开展给各机构带来的司法风险。

- 整合“零、乱、散”的电子数据

线上业务开展过程中生成的每一环节并保存于不同系统的电子数据证据进行关联、统一保存及第三方存证，确保在争议发生时原始数据未被篡改，基于原始数据，可回溯业务开展的具体步骤。

5. 适用领域

不同行业领域开展移动互联网业务时，均可使用该解决方案。方案本身可以根据不同的业务需求进行模块化提供。其应用场景的主要特点包括：

- 需要进行安全级别较强及安全性要求较高的身份认证；
- 需要签署电子协议，用以明确合同签署方权利与义务。并且该电子协议需要有法律效力；
- 业务受理过程产生的电子数据可被第三方机构进行司法保全。

6. 企业分工及产品清单

采购方、应用系统开发商（若有）、测试人员及 CFCA 将参与项目实施过程，包括需求调研、方案设计、编码实现、产品实施与调试、用户验收测试、项目上线等。

CFCA 提供的产品包括云证通移动证书系统、云证通客户端 SDK、无纸化电子签章系统和电子保全系统；CFCA 提供的服务包括 CA 认证服务、时间戳服务、

证据保全服务和取证服务。

7. 应用案例

当前，线上业务司法纠纷解决方案已在近两百机构成功上线，客户包括中国人民银行、招商银行、中国石油、顺丰速运等，涉及银行、保险、证券、物流、招投标等行业，为合作方线上业务保驾护航。

中金金融认证中心有限公司

联系人：周铎

电　话：17601203377

010-80864120

物联网与工业互联网

工业互联网密码应用解决方案

1. 概述

当前工业互联网安全威胁复杂多样，产业基础还尚显薄弱，面临较大的安全挑战。密码技术作为保护网络安全的核心技术和基础支撑，提出工业互联网安全解决方案，构建纵深防御整体密码应用体系，确保工业系统业务安全可控。

2. 需求分析

工业互联网安全需求主要包括：对适配工业现场环境、低功耗模式等工业系统端级别设备与访问用户身份认证的需求；对系统中不同网络速率和连接要求的通信网络的传输认证和传输加密要求；对于关键工艺参数等敏感数据的存储安全需求；针对不同安全等级区域边界访问隔离建立横向或纵向密码隔离。本解决方案适用于需要此类需求的项目。

3. 方案架构

针对工业系统存在的安全问题，兼顾安全需求及技术实现路线，在现场控制层、过程监控层、生产管理层等进行密码安全加固，基于密码应用需求理解，以典型 SCADA 系统为例，设计工业互联网系统密码应用安全防护架构。

3.1 技术架构

结合等保 2.0 对工业系统安全扩展要求，对工业企业的安全计算环境、安全区域边界、安全通信网络等主要安全需求，形成工业互联网密码应用整体技术方案，技术架构如下图所示。

图 3-1 技术架构图

3.2 产品部署图

安全设备部署方式如下图所示：

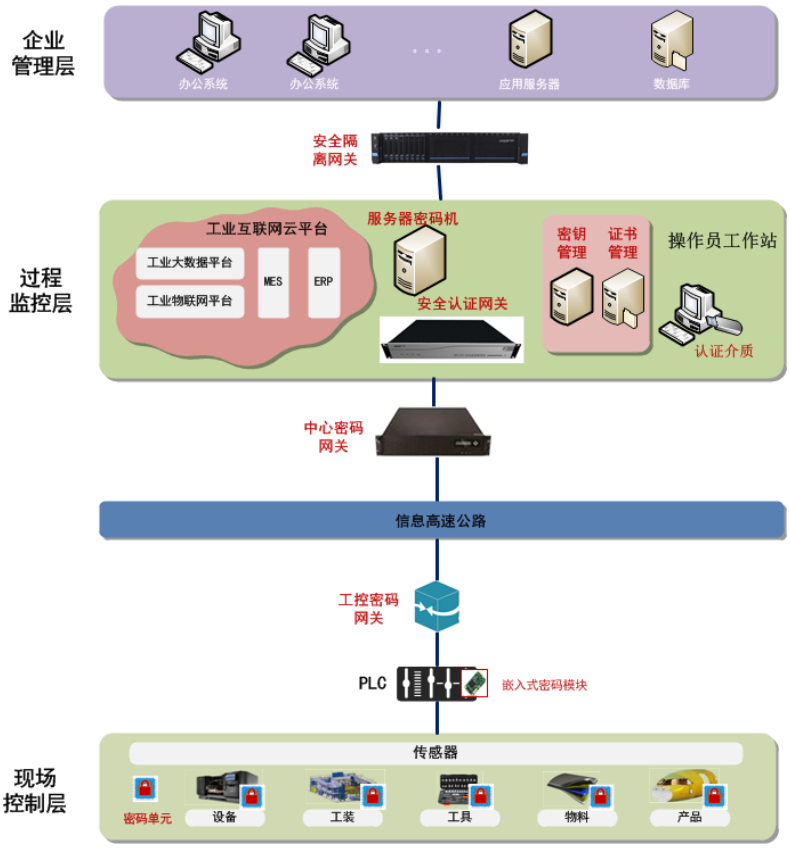


图 3-2 产品部署图

以嵌入式安全模块、工控密码网关、中心密码网关、安全认证网关、安全隔

离网关等密码产品为载体，配合密钥管理与证书管理子系统等平台支撑，为工业控制系统提供全方位的安全保障。既可针对终端控制设备，提供支持内嵌式硬件密码模块、工控密码网关等，实现现场控制层工控协议密码安全；也可针对中心侧提供中心密码网关实现网络传输密码安全保障，对中心的业务服务器提供调用式服务器密码机，用于组态应用软件的业务机密性、完整性、不可否认性保护。以安全认证网关实现控制系统不同角色用户的身份鉴别和授权访问，同时可提供密码安全隔离设备，实现边界的受控访问与数据安全防护。

3.3 主要功能

功能 1:实现现场控制层和过程监控层设备之间的身份认证。

功能 2:实现现场控制层设备数据机密性和完整性保护。

功能 3:实现过程监控层海量终端接入和数据加密保护。

功能 4:实现过程监控层与生产管理层之间的正反向隔离传输保护。

3.4 主要技术指标

支持算法：SM1,SM2,SM3,SM4

认证资质：国密二级

支持 5000 个终端用户同时连接

网络吞吐率大于 650Mbps

4. 方案特色

符合安全等级保护 2.0 新要求

构建基于纵深防御整体密码安全防护体系

适配多种应用场景、实用性强

5. 适用领域

该系统可为装备制造、原材料生产、电子制造、航空航天、化工等重点行业提供“工业设备安全、工业主机安全、工业生产网络与管理网络安全、工业数据

安全”的安全综合防护平台。与入侵检测、智能分析、态势感知、指挥调度等其他业务能力结合的多层次纵深防御体系已得到既有项目有效验证，可为工业互联网实际应用提供无感密码安全防护。

6. 企业分工

解决方案中涉及体系化的安全产品均可由兴唐通信科技有限公司提供；也欢迎与更多工业产品供应商、安全厂家的多种形式合作。

7. 应用案例

为某国家重点水利项目建设工业系统安全解决方案。该系统已正式上线经数月正常运行，各水闸站与总部均无故障，得到了领导和专家一致好评。该系统能够在不影响业务系统正常运行的前提下满足工业安全应用需求，可用于指导工业系统安全综合防护平台广泛部署和建设。

兴唐通信科技有限公司

联系人：王健安　　胡伟

电　话：13699262399　　13466362701

010-62301206　　010-62302004

物联网国密安全标识系统安全解决方案

1. 需求分析

5G 时代的到来，让物联网应用取得飞速的发展，各种智能摄像头、智能家居设备、工业智能控制设备、智能穿戴设备都呈现爆发式增长的态势，便利人们生活同时也带来诸如拒绝服务攻击、通讯协议凭证伪造、信息泄露等安全隐患。

2018 年政府机关发布的密码应用相关发展规划文件指出：“推进自主可控密码发展，组建以密码技术为核心、多种技术融合的网络安全体系，建成密码基础设施支撑的新网络安全环境。”其中网络密码应用中提到：完善 5G、广播电视行业密码支撑体系，推进直播系统、IPv6、物联网等领域中的密码应用。因此物联网领域亟需引入基于密码技术的安全标识解决方案，以解决物联网领域数据交互和身份安全，避免物联网终端被非法、假冒用户入侵窃取数据。

2. 适用范围

本方案适用于新建物联网环境，通过配合物联网终端厂商在终端出厂前完成安全介质的烧录，进而实现物联网终端的合法性校验，避免由于身份伪造引起的数据泄露。

3. 方案架构

天融信基于物联网国密安全标识系统（TID）的安全解决方案可以提供物联网可信密码标识技术从而保障物联网设备身份唯一性。通过设备鉴权、安全密码管理、安全加速等主要核心功能，帮助用户解决物联网环境身份认证、传输加密、信息防篡改的安全需求。针对厂家产线情况（如：数据采集传感器、智能摄像头、智能电表等物联网终端）提供定制化的终端身份烧写服务，实现物联网终端从出厂标识分发到业务环境中身份认证的安全闭环。本方案从终端身份安全与信息传输安全维度，为用户提供一套包含标识分发、连接认证、密钥管理三部分的技术

方案。

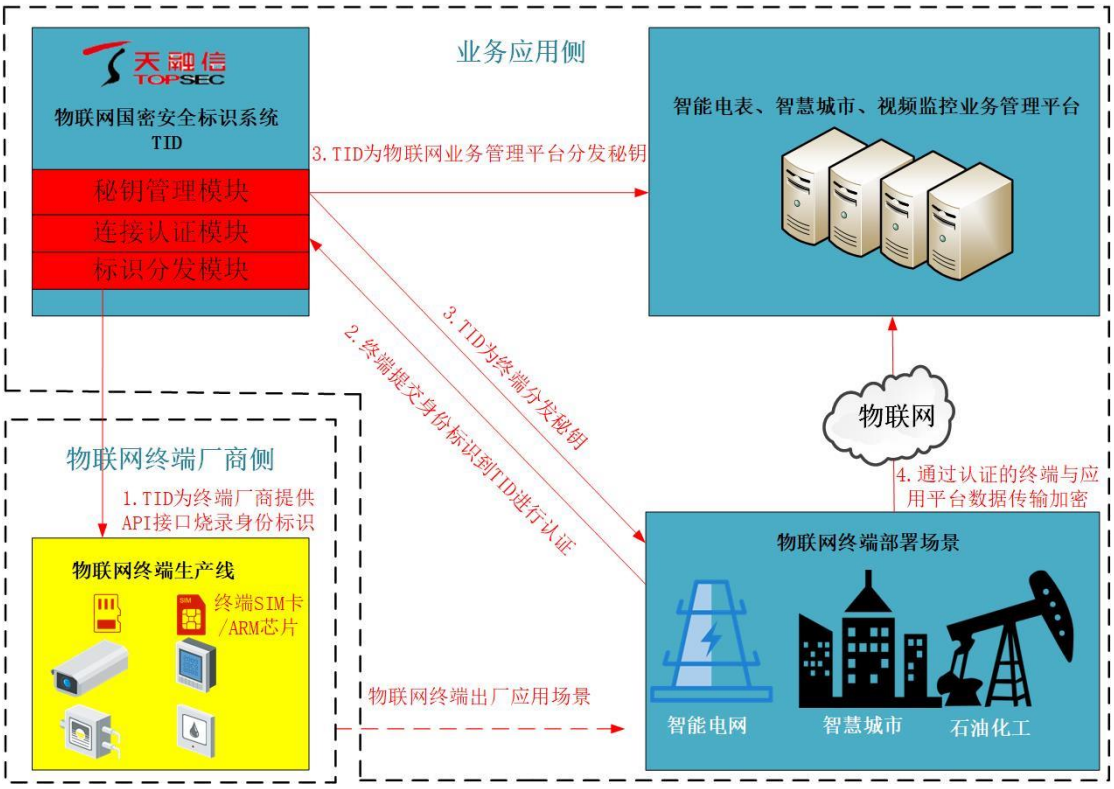


图 3-1 物联网密码应用示意图

物联网国密安全标识系统的实现需要物联网终端厂商与用户紧密配合，TID 以硬件形态部署于用户的业务环境中，对物联网终端厂商开放 API 接口实现物联网终端出厂身份标识分发。用户侧只需购置 TID 硬件设备并通过该设备对物联网终端的 SIM 卡/ARM 芯片实现 TID 烧录即可。

标识分发：TID 业务软件通过物联网终端产线 API 接口，对物联网终端内的通用 SIM 卡或专用安全芯片烧录 SM9 国密安全标识，并封装到物联网终端通讯芯片中，为物联网终端提供全球唯一的身份 ID。

连接认证：物联网终端调用存储在物联网终端 SIM 卡/ARM 芯片中的 SM9 国密安全标识，并提交给 TID 认证模块完成身份认证。

密钥管理：TID 具备符合国密产品技术要求的秘钥管理模块，为物联网终端和业务管理平台分发公钥和私钥，实现通讯双方传输过程中的信息加密。

通过物联网国密安全标识系统解决方案可以构建完整的物联可信认证体系，为每一个物联网设备提供全球唯一、不可抵赖的国密身份标识，为物联网设备在

多应用场景中提供定位和根据信息、行为溯源的能力。结合 SM2/3/4 国密算法实现物联网数据的加密传输，防止物联网数据在传输过程中被监听、篡改。防止黑客仿冒感知节点，如伪造、篡改安防节点指令进而发起攻击，可以防止黑客对代码升级包的篡改，防止用户敏感数据泄露。

4. 方案优势

有效防御身份冒用风险 TID 可与物联芯片/存储厂家合作，提供芯片级的安全存储方案和物理安全防护能力，有效防御由于物联网硬件窃取带来的各类身份冒用、伪造凭证安全风险。

实现终端追踪溯源 TID 提供完善的 SM9 安全标识管理方案，确保方案安全等级。为每一个物联网终端提供唯一、不可抵赖的国密身份标识，通过物联网终端身份标识，对设备身份进行有效追踪、溯源。

轻量化密钥管理 身份标识与秘钥信息占用极小的物联网终端系统资源，在保障物联网终端安全的基础上不影响其工作效率。

低成本高安全 用户只需购置一套 TID（物联网国密安全标识系统），便可具备对于海量物联网终端的、基于国密密码标识的安全防护能力。

5. 适用领域

5.1 智慧城市

智慧城市部署大量的室外传感器、IP 摄像头，环境恶劣、弱安全防护，但是其数据敏感，一旦数据泄露会造成重大隐患。通过 TID 可以对传感器的本地数据和传输进行加密，确保即使物理丢失黑客也无法查验本地数据/获取根密钥。

TID 还可以防止黑客窃取设备后登入设备、破解密码、伪造设备、仿照数据或攻击云平台，为智能手机与物联网互动在保证安全的前提下提高用户体验

5.2 智能电网

智能电表分散在户外，安全无保障，存在仿冒和数据篡改风险，因此需进行终端防窃电设计和有效的身份认证以防非法接入；同时异常事件自动上报，窃电

行为精准定位；电表数据在上报过程中需要进行加密，防监听和防泄露；而电力网络则需要防止高级安全威胁、DDoS 和病毒等攻击以防业务中断、经济损失。

TID 可以防止黑客仿冒智能电表或篡改智能电表数据，对接入管理平台的智能电表进行唯一身份认证，对电表上报传输过程中使用国密算法安全加密。

5.3 石油化工行业

为了应对炼油化工一体化、园区化、基地化发展趋势，保障园区日常管理，炼化企业陆续部署了一系列辅助系统，包括视频监控、入侵报警、数据采集传感器、门禁管理、生产巡检、火灾报警等系统，各种辅助终端广泛部署在炼化园区内，存在采集数据泄露和缺乏身份认证机制的安全风险。

TID 可以对接入云平台的安防节点进行唯一身份认证，对双向通信进行安全国密加密使能。还可以防止黑客仿冒能源数据采集传感器节点，如伪造、篡改安防节点指令进而发起攻击。

企业职责划分

名称	职责
北京天融信网络安全技术有限公司	物联网国密安全标识系统

北京天融信网络安全技术有限公司

联系人：张超

电　话：15811035593

物联网安全密码应用解决方案

1. 概述

近年来，物联网安全事件层出不穷，给国家安全、公民生命财产安全和个人隐私安全带来重大威胁和隐患。密码技术和基于密码技术的 PKI 数字证书技术的应用，为物联网安全所需的身份鉴别、访问控制、数据完整性、保密性和抗抵赖等提供了安全技术保障。

2. 现状和风险分析

2.1 物联网典型架构

物联网以“云、管、端”为主流系统架构模式，如下图所示：

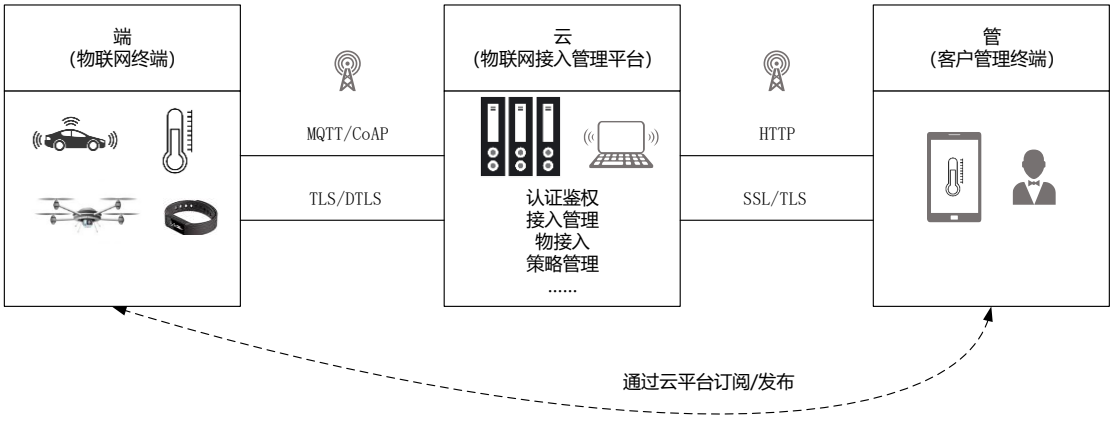


图 2-1 物联网架构图

2.2 安全风险分析

目前物联网“云、管、端”的身份识别措施非常薄弱。物联网终端设备大多仅以设备出厂编号作为身份标识，通过预置密钥的 HMAC 认证作为身份验证方式，极易被破解、复制或重放攻击，物联网接入平台通过 HMAC 来向物联网终端设备发送控制指令，一旦预置密钥泄露，物联网终端设备将完全失控。手机 APP 的身份认证大多还停留在用户名+密码+动态验证码的低安全级别，存在较大安

全隐患。

3. 方案设计

本方案将密码技术、PKI 数字证书技术、TEE 技术、SE 技术结合物联网云、管、端进行场景落地和实施落地，以密码技术作为安全基石、以 PKI 数字证书技术标识物联网各端身份、以专用密码硬件设备/SE/TEE 为密钥、数字证书安全存储和密码运算安全执行的载体，形成物联网安全密码应用的最佳实践。

3.1 技术架构

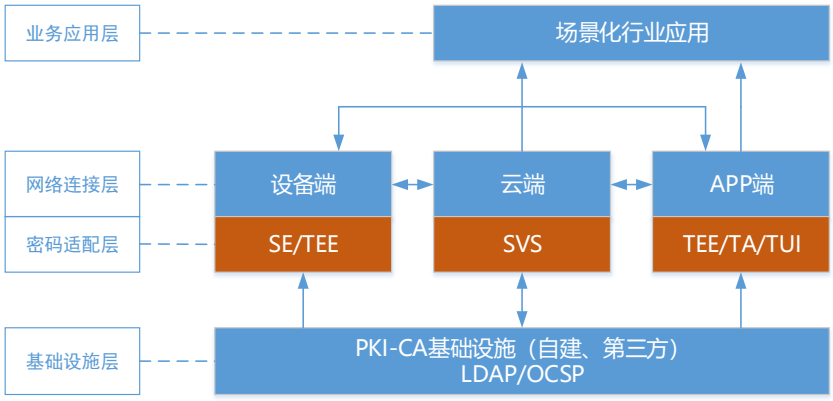


图 3-1 技术架构图

3.2 产品部署图

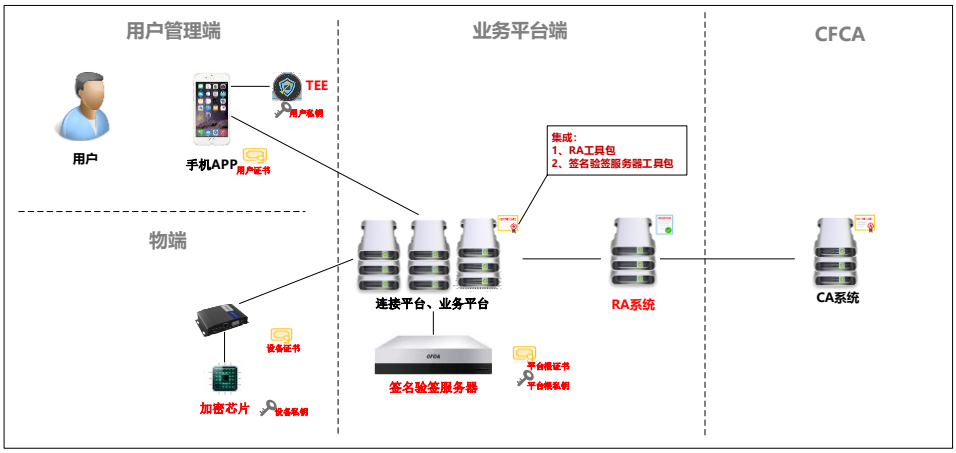


图 3-2 产品部署图

用户管理端的手机支持 TEE（可信执行环境），TEE 向手机 APP 应用提供安全接口用于生成随机数、公私钥对、CSR，同时 TEE 负责用户私钥安全存储、关键业务签名验签、用户生物特征识别等功能的安全执行。

设备端集成 SE（加密芯片），随机数生成、公私钥对、CSR 生成，私钥安全存储和签名验签等密码运算由 SE 完成，设备中集成证书应用 SDK，完成设备和 SE 之间的密码应用接口调用。

业务平台端部署 SVS（签名验签服务器），完成与物联网设备终端和用户 APP 之间交互信息的签名和验签。部署 RA 系统对接第三方 CA 系统，负责设备证书和用户证书的在线全生命周期管理。

3.3 主要功能

采用国密算法对云、管、端交互数据进行加密、解密，确保物联网数据的机密性、完整性和隐私保护；

采用 PKI-CA 数字证书技术标识物联网各端身份，结合国密签名、验签算法，确保物联网各端可信身份和行为的可追溯和不可篡改；

国密算法、数字证书技术和 TEE/SE 对接所需的中间件开发；

通过在业务流程中将随机数和时间戳嵌入签名报文中，有效避免重放攻击。

3.4 主要技术指标

描述	要求
支持用户和设备规模	大于 100 万设备；大于 1000 万用户

4. 方案特色

基于 PKI 构建物联网云、管、端安全体系

结合云、管、端实际软硬件情况，提出了结合业务流程的 PKI 身份认证方案，结合实际项目验证，确保方案的可落地性。

充分考虑用户体验和安全性结合

用户通过操作 APP 进行操作，基于 TEE 软件可信执行环境进行密码运算、

证书应用和生物识别，基本不改变原有业务体验。

在物联网设备端集成加密芯片（SE），实现高安全级别的私钥存储、密码运算和数字证书身份验证。

在业务流程设计中通过加随机数、时间戳等方式，避免重放攻击等安全威胁。

支持国密算法

本方案的设计，支持在云、端、端均基于国密算法进行设计和实现，符合国产密码算法各行业推广的趋势和要求。

5. 适用领域

车联网、智能门锁、智能家居、智慧安防、智慧地锁等。

6. 企业分工

角色	职责	提供产品
应用开发商	相关系统开发	业务平台、APP 等
设备商	物联网设备与系统适配	相关终端设备
加密芯片/TEE	配合应用开发商集成	芯片、TEE 和 SDK
CFCA	PKI-CA 基础设施	RA、平台端 SVS

7. 应用案例

树根互联	重要工业设备的远程监控场景
中兴通讯	5G 基站与管理平台之间安全通信场景
德国大众汽车	车辆与 TSP 平台联网信息交互场景

中金金融认证中心有限公司

联系人：王自冲

电　话：18612237006

010-80864104

汽车制造行业商用密码应用解决方案

1. 概述

随着中国成为全球第一大汽车生产地，已经有 100 个汽车品牌在中国市场竞相逐鹿。近年来，随着汽车制造企业信息化建设的不断深入，在制造、设计研发高度信息化、网络化的趋势带动下，企业引入了多种信息应用系统，如 OA、ERP、CRM、PDM、PLM 等。这些应用系统已经成为了企业高效运作的重要基础，覆盖了企业研发设计、营销、生产、财务、人力资源、办公管理等业务，但是，伴随着信息技术带来的竞争优势,企业内部也面临着很大的信息安全风险。

根据权威机构调查显示，80%以上的安全威胁来自企业内部，具体的风险如下：

数据源安全：企业的核心数据，如设计图纸、管理资料等，基本上都是通过多人协作生产而得到的数据资产，任何人都可以查看，这些信息一旦泄露会使企业蒙受巨大的损失。

数据传输安全：企业各级单位之间文件传递采用企业内部邮箱和内部即时通的方式来实现信息传递，传递通道为互联网，传递过程中的文件都是以明文的方式，文件也没有细粒度控制。

数据对外交互：企业需要与外界进行数据交互，涉及企业内部核心信息都是以明文方式发出，对发出的数据失去控制。

2. 需求分析

汽车制造企业目前主要有以下特点：

- 企业规模庞大，分支机构繁多，信息管理难度较大。
- 企业信息环境复杂，应用系统数量庞大，信息环境复杂。
- 产业链较长，设计外部数据信息接入以及对外交互数据信息需求频繁。
- 在数据安全管理和数据应用效率两方面的难以均衡。

在企业的日常运转中，营销管理体系与设计研发体系为企业的核心。

（1）营销管理体系

市场、销售、管理环节中的核心信息内容主要包括一些常用文档如 word、PDF 等，涉及到的实际工作如下：

- 核心商业信息由相关业务执行部门搜集、整理、编制和创造，例如客户信息，销售商机、市场策划文案等，此类内容随着这个操作环节被植入到电子文件中；
- 信息管理人员会得到电子文件并因此而接触到相应内容，通过信息管理体系内部其他部门可以获取到承载商业信息内容的电子文件；
- 因业务的需要，商业运作部门内部人员需要将承载内部信息内容的电子文件外带到合作机构、客户机构和流通渠道体系。

（2）研发设计体系

研发、设计为主的核心技术信息主要依托于 Pro/E、UG、CATIA、AutoCAD、Solidworks 等设计软件以及少数的编码类 VC、VB 等开发软件，核心技术信息内容在电子产品生产企业中，涉及到的实际工作如下：

- 技术人员，根据企业目标进行研发和设计，研发和设计成果主要以电子文件形式存储、交换；技术管理人员对成果进行审核过程中也将接触到文件内容；
- 审核通过的研发或设计成果在生产、委托加工、对外技术交流、技术推介活动过程都将对承载着核心技术信息的电子文件进行外泄。

3. 方案架构

3.1 技术架构

本方案提出的解决办法是采用 B/S 管理与 C/S 控制相结合的软件体系来完成相应的目标要求，系统集中管理功能在服务器端部署，电子文档加解密及其控制在用户终端或文档加解密的应用计算机上实现；逻辑架构具体描述如下：

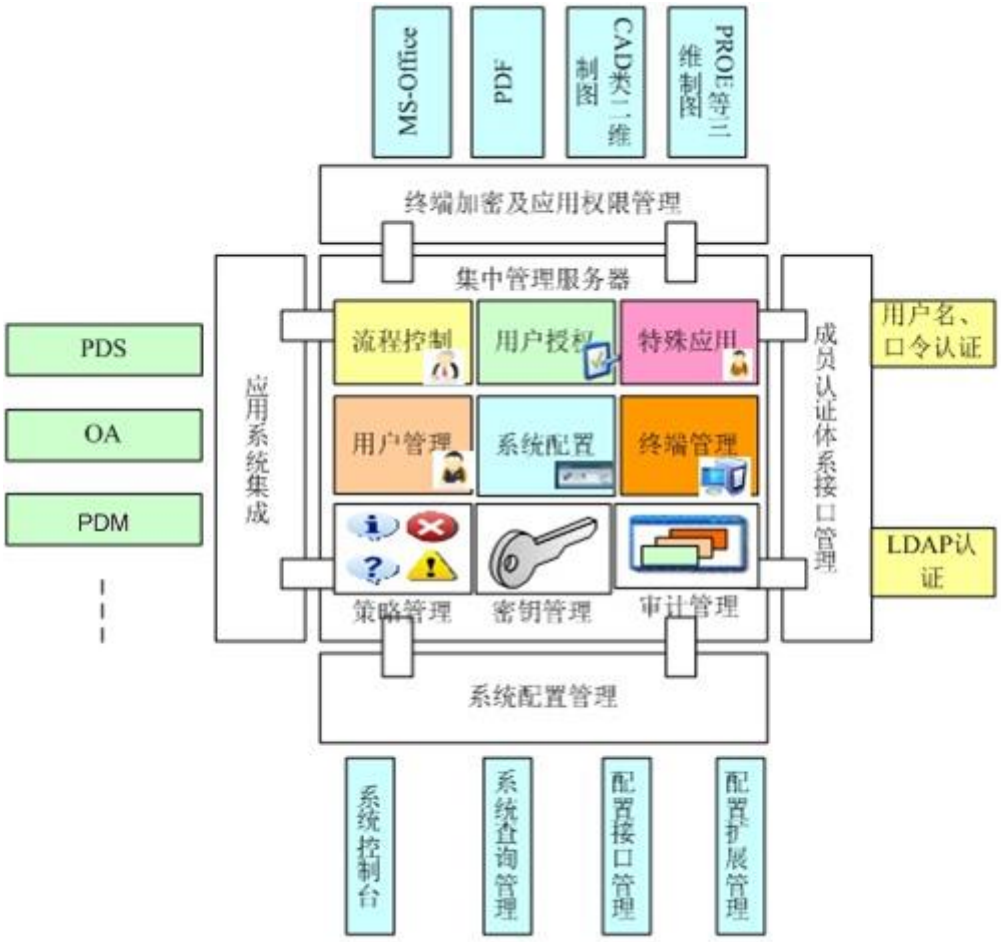


图 3-1 加密软件逻辑架构设计方案示意

集中管理服务器,用以支持整体系统的安全策略管理、用户管理、系统配置、终端管理、策略管理、系统加密算法及密钥管理以及系统日志和审计管理等。

针对不同类型的终端文档通过终端加密和具体应用权限管理来统一实现支持和管控，通过与客户端控制软件进行交互配合完成终端使用用户身份识别，以及对于不同类型的终端电子文档的加解密控制、用户权限控制、文件外发和终端加密文档操作记录日志回收等功能。

3.2 产品部署图

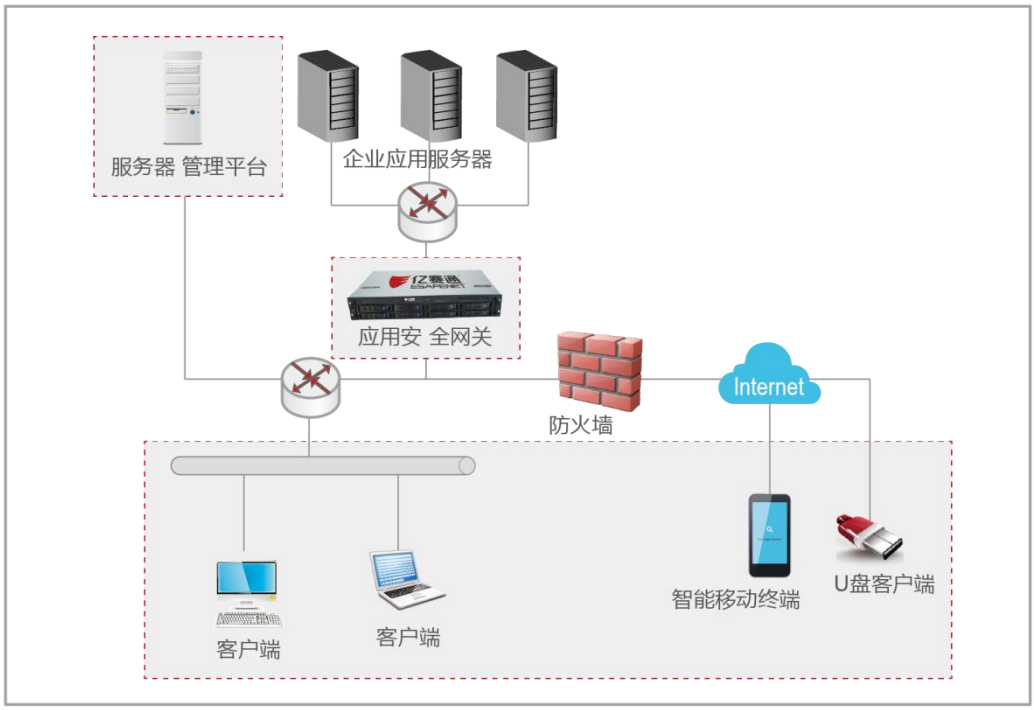


图 3-2 产品部署图

从实施角度分为服务器管理平台、客户端、应用安全网关三大部分：

服务器管理平台：产品集中管理平台，用于系统管理及运维，建议双机热备。

应用安全网关：用于保护应用系统数据。

客户端：用于对电脑终端（Windows、Linux、Mac）、智能移动终端（Android、Linux）数据进行安全防护。

3.3 主要功能

透明加密

透明加密是一种自动加密技术（强制性），所谓透明是指文档加密、解密过程对使用者来说是无感知的。客户端根据策略实时监控应用程序对指定类型文件的读写操作（读解密、写加密），实现文档的实时动态加解密，文档加密后，在受控范围（安装客户端的合法用户）内透明使用，脱离受控环境无法使用，从而有效解决用户核心数据文档在生产过程中面临的数据泄密风险。

权限管控

通过对文档加密授权及角色对应，控制文档在内部受控使用，避免越权使用带来的泄密风险。数据作者可以根据需要设定数据的传播范围（用户、部门、项目组等）和查看权限（只读、打印、修改、阅读次数、阅读时长），也可以根据企业需要建立权限模版，对文档批量授权。

外发管理

通过对文档加密、授权及封装，控制文档在外部传播和使用时造成的泄密风险。数据作者可以根据需要设定文档的查看权限（只读、打印、修改、阅读次数、阅读时长），外部用户拿到文档后需要通过安全身份认证后才能查看该数据，没有通过认证的无法查看和使用数据。

应用安全网关

通过软硬一体化结合的方式为应用系统提供安全保障，应用安全网关可以为应用体统提供安全准入和数据加解密双重防护，安全准入通过终端身份识别、应用系统仿冒、传输隧道加密、终端访问日志等多方面进行应用数据安全访问控制，数据加密通过对应用系统核心数据进行上传解密、下载加密，解决企业核心数据离线安全使用。

3.4 主要技术指标

规格指标

序号	名称	参数
1	支持的操作系统	服务器支持 Windows Server 系列 客户端支持 WindowsNT 系列的操作系统
2	支持的数据库	支持目前多数主流的数据库，如 Oracle、SqlServer 等
3	支持常用文件格式	常用办公类软件：.doc\docx\ppt\pptx\xls\xlsx\pdf 等
4	支持的硬件接口	标准的 PCI 插槽和 USB 1.1 和 USB2.0
5	每个服务器支持的最大并发数	800（测试环境：Intel E3 @3.4GHz；16G 内存 ；1000M 网络）
6	每个服务器支持的最大用户数	5000（测试环境：Intel E3 @3.4GHz；16G 内存 ；1000M 网络）

密码设备

采用支持国密算法 SM2、SM3、SM4 的飞天诚信 epass3000GM 型号密码设备软硬一体的方式研制的电子文档安全管理系统。

在系统中涉及的密钥主要有用于加密存储在数据库中的敏感信息的主密钥、加密传输中敏感信息的传输密钥以及加密文件、加密数据或消息的数据密钥，主密钥是通过密码设备（加密锁）物理保护的。

4. 方案特色

终端对电子文档的保护力度和产品本身的安全稳定性非常高。对于电子文档分发、打印、复制受到控制以及脱离了本企业的文档有效的控制，杜绝涉密信息二次泄露、非法修改。

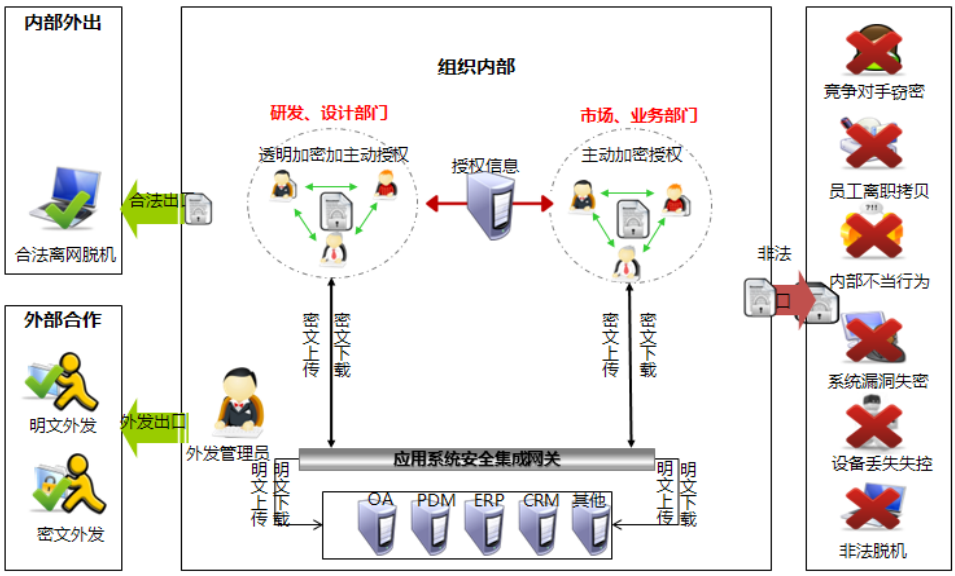


图 4-1 系统部署效果示意

不改变使用者对协同工作中的信息文件的使用操作习惯（如：使用习惯的应用程序操作、浏览信息文件；信息文件的加解密操作对于使用者来说是透明的等）；

易用性：使用简单，不需要培训就可以使用；

使用方便：操作方便，是以图像界面方式显示；

可延展性：能够轻松实现对所有文件类型的支持，完全支持企业发展的需要。

5. 适用领域

5.1 销售、市场、管理部门分级授权

对于销售、市场、行政管理部门日常所产生的核心办公类电子文档，由于其特殊性，需要经常大量的在企业内各部门之间流转，推荐采用文件分级授权的管理模式。通过细粒度权限控制，可以有效防止文件在企业内部流转过程中二次扩散，文件授权过程如下图所示：

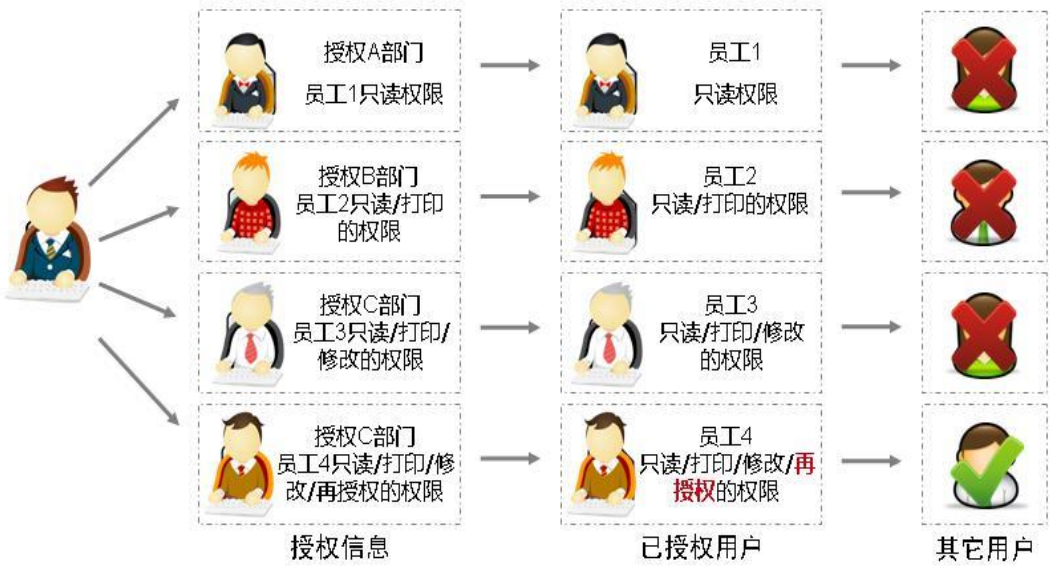


图 5-1 文件流转控制

5.2 研发设计部门电子文件强制加密

对于研发、设计产生的设计图纸、源代码等核心电子文件，系统采用强制动态加解密的方式进行保护，实现对核心信息的全生命周期管控，其实现效果如下图：

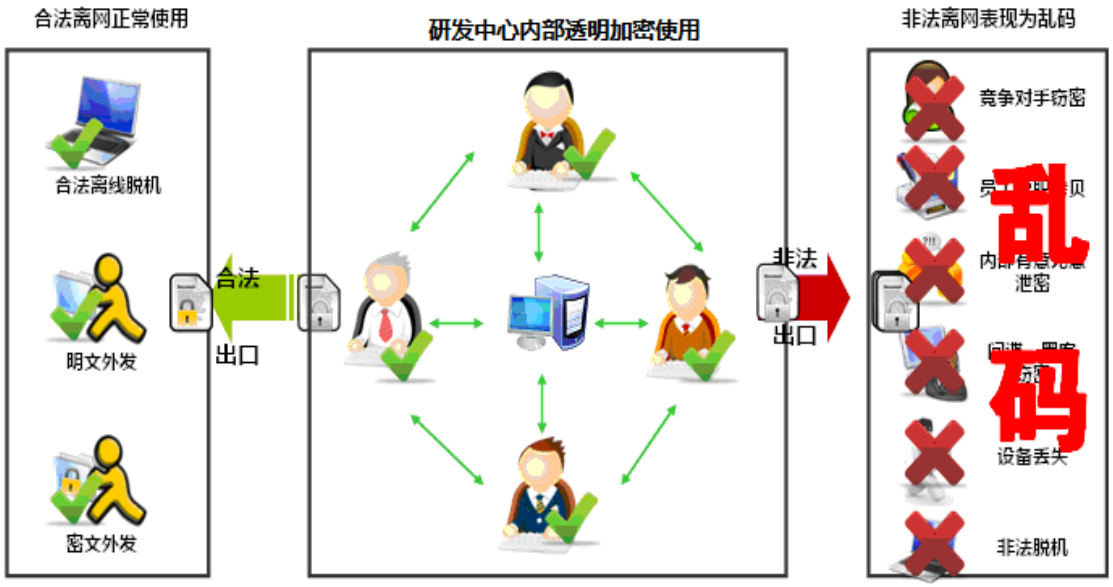


图 5-2 文档透明加密效果图

5.3 电子文件对外交互

当企业内部需要与企业外部进行文件交互时，对于需要外发到企业以外的文档，可采用对文件进行特殊控制方式实现对文件的安全控制。

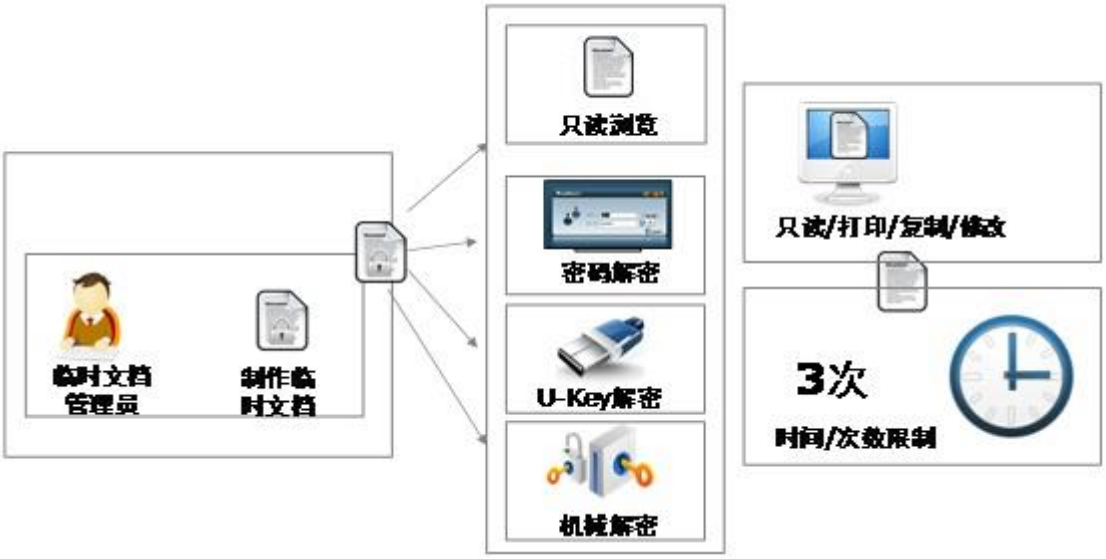


图 5-3 文件对外交互应用示意

5.4 应用系统集成

保护 PDM、ERP、OA 等应用服务器中的文件的安全交互，终端数据防泄露的同时，实现服务器后台数据明文存储：

- 对 PDM、ERP、OA 等重要应用服务器进行安全加固，实现重要数据后

台服务器明文上传存储、合法终端前端密文下载使用；

- 非法用户下载目标服务器数据一律加密下载，防止数据外泄。

6. 企业分工

亿赛通公司将对软件改进的性能予以详细说明，升级方式可以采用推送/自行安装、远程指导安装或现场指导安装进行。功能发生重大变化的版本升级，除予以详细说明外，在必要的时候公司还将采取现场指导升级的方式为客户服务，并提供系统的培训服务，以保证用户应用系统的正常运行。如：

（1）提供产品文档（技术白皮书、产品规格、解决方案、使用文档）

（2）对项目各个系统提供一年的免费维保服务（含易损件的免费更换、定期巡检、现场故障排查维修等）；

（3）提供定制服务。

7. 应用案例

东南汽车数据泄密防护项目	
部署范围	研发中心，国产化部，品管部，生管部、生技部、资料室等
加密范围	透明加密：CATIA，AUTO CAD，RxHigh，viewcompanion，Microsoft Office Manager，Microsoft Office Document Imaging，画图，VP，Rx High，UG。权限文档：WORD、EXCEL、PPT、TIF、PDF、TIFF 上传到服务器上自动生成权限文档，全体员工只读权限
实施效果	设计图纸采用强制加密，防止员工/外来人员私带泄密 办公类文档由资料室专人归档到指定服务器上自动生成权限文档，通过业务系统链接供员工查看 加密及权限文档只有资料室专人才有权限脱密及还原 面向外部（客户、供应商）发送文件，由资料室专人制作外发文件才能外发

亿赛通科技发展有限责任公司

联系人：张艳茹　　冯育坤

电　话：13261928861　　13269394036

010-57933600　　010-57933600

数据保护

数字版权管理（DRM）密码应用解决方案

1. 概述

DRM 领域背景：

数字版权管理（DRM）技术主要用于保护内容拥有者或服务提供商提供给用户消费的内容，这些内容包括音/视频内容、文件等，使得只有获得授权的用户才能够按照内容拥有者或服务提供商设置的权限或商业规则消费这些受保护的内容。当前，DRM 技术普遍采用国外专利技术、国外密码算法及产品，不利于我国数字版权保护体系的自主可控。互联网视频运营环境复杂、授权模式多样化、4K/HDR 视频多分辨率编码及 HDR 动态元数据编码、VR 多视角编码、终端智能化等对现有的数字版权保护与监管体系提出了新的挑战，满足互联网+环境中 4K/HDR、VR 等视频内容运营需求的版权保护与监管体系尚不健全。基于此，迫切需要突破基于国产密码的多媒体版权保护应用与支撑技术，建立基于国产密码的多媒体版权保护与监管体系。

国家及行业在该领域的与安全相关的政策法规主要包括:

（1）《广播电视安全播出管理规定》（国家广播电影电视总局令第 62 号），国家广播电影电视总局于 2009 年颁发。该规定从基本保障、日常管理、重要保障期管理、应急管理、监督管理、法律责任等方面，全面规定了安全播出相关运维管理要求，我国所有从事广播电视播出、传输、覆盖等业务的单位均采用该规定进行保障安全播出开展的技术维护、运行管理、应急处置及其他相关活动。

（2）《广播电视相关信息系统安全等级保护基本要求》，国家广播电影电视总局于 2011 年颁发。对广播电视相关信息系统安全等级保护基本要求进行规范，规定了不同安全等级的广播电视相关信息系统的基本保护要求,包括技术要求、物理要求和管理要求三部分。

（3）《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)

（4）《国家信 息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)

（5）《关于信息安全等级保护工作的实施意见》(公通字[2004]66 号)

（6）《信息安全等级保护管理办法》(公通字[2007]43 号)

（7）GB/T 22240-2009 《信息安全技术信息系统安全等级保护定级指南》

（8）GB/T 22239-2008《信息安全技术信息系统安全等级保护基本要求

商用密码应用的意义：

（1）加强国内厂家的开发支持国密算法芯片的技术能力；

（2）培养国产芯片市场，降低芯片生产成本；

（3）有利用建设国家主管部门组织的安全性检测机构；

（4）有利于我国数字版权保护（DRM）体系的自主可控。

2. 需求分析

DRM 通常应用于双向网络的端到端内容保护，其系统实施所面临的安全风险包括：

（1）网安全威胁，比如，各种网络攻击、木马等；

（2）设备安全，设备包括头端设备和终端设备，其安全风险包括：硬件威胁，接口安全，操作系统安全，应用软件安全等

（3）内容安全

数字电视内容安全在内容的存储、传输、播放过程中都会面临安全威胁。

- 内容在服务端如果明文存储，那么容易收到攻击，从而获取内容明文；
- 内容如果明文传输，那么内容容易在传输过程中被非法录制；
- 在传输通道上，也容易被非法内容干扰或插播；
- 在终端，如果有明文的内容在 buffer 中或存储设备中，那么内容可能会被录制分发；
- 如果设备输出接口不保护，内容也会从接口上被录制；
- 在终端，如果内容保护软件安全性不够，也会被破解，从而导致内容或密钥泄露。

解决上述所遇到的安全问题，都需要有密码做基础支撑，来保护网络的安全，设备的安全和内容的安全。本方案全面采用国产密码算法 SM2,SM3 和 SM4 来保护音视频内容的安全。

3. 方案架构

3.1 技术架构

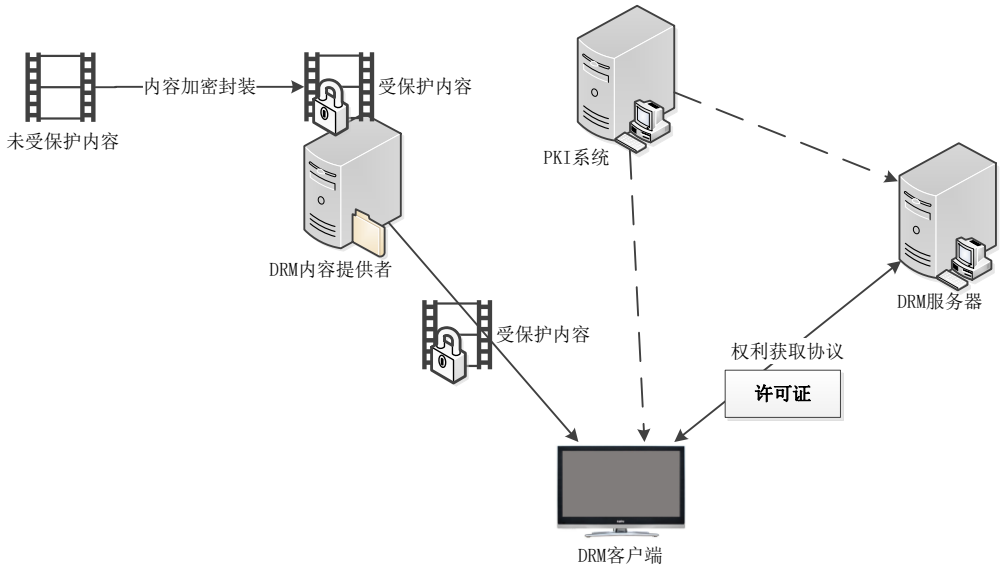


图 3-1 方案架构图

这是一个端到端的互联网电视数字版权管理系统，主要包括 DRM 服务器、DRM 客户端、PKI 系统和 DRM 内容提供者，对互联网电视内容进行有效的数字版权管理。

内容在 DRM 内容提供者（服务提供商或内容提供商）处进行了加密（采用 SM4 算法），加密后的内容送给 DRM 客户端；DRM 服务器产生许可证，它描述了被授权设备和内容的使用权限等信息（许可证采用 SM3 做信息完整性验证，分别采用 SM2 和 SM4 对许可证的不同密钥和数据进行了加密）。权利获取协议定义了 DRM 服务端和 DRM 代理进行安全通信和传递许可证的技术方法（采用 SM3 和 SM2 做信息完整性验证和数字签名）；信任与安全体系定义了基于 PKI 系统的信任技术机制，证书采用 SM3 和 SM2 算法。

3.2 产品部署图

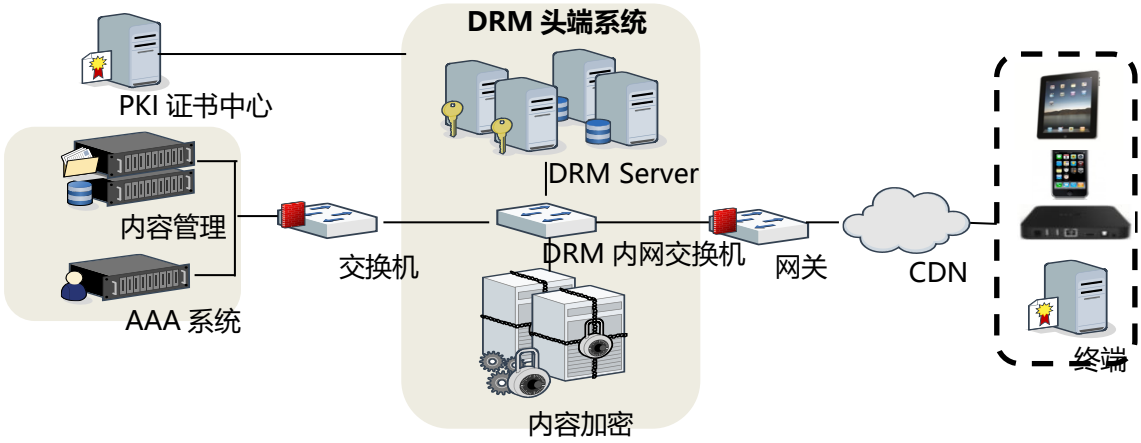


图 3-2 方案部署图

DRM 头端部署在运营商处或云端，与运营后台系统(内容管理，AAA 系统等)进行交互。PKI 证书可采用第三方提供，也可以由 DRM 提供商提供。

（1）网络安全

DRM 头端系统独立子网，与外部的接口采用硬件防火墙进行隔离，对外部访问进行设备认证等

（2）设备安全

设备的登陆需要访问控制（强口令、权限），所用的 OS 进行的安全的裁剪并移除不需要的功能、关闭不用的端口，并设置可访问 IP 和端口/协议等

3.3 主要功能

- 内容加密：对直播和点播的音视频内容进行加密（SM4）；
- 授权：给播放用户按购买情况授予使用权限。当用户播放加密的内容时，如果终端本地没有授权，那么终端向 DRM 头端系统申请授权（SM2,SM3,SM4）。
- 双向认证：头端和终端在通信的过程中进行相互认证（SM2 和 SM3）

3.4 主要技术指标

- DRM 授权服务器同时支持的终端并发数，可通过集群方式解决。

- 授权加密机的效率，可通过多台并行解决。
- 直播加密机的实时性，也可通过多台并行解决。
- 安全性，通过第三方机构提供的安全测试

4. 方案特色

- 针对永新视博的 DRM 解决方案 SecureMax，其特色和优势包括：
- 方案全面采用国产密码算法 SM2, SM3 和 SM4，其中，头端配备硬件加密机，通过了国密测试并获得国密产品型号证书
- DRM 系统可根据用户量进行动态自适应（动态负载均衡）
- 支持主备和灾备配置
- 可进行云端部署
- 支持各类终端类型，包括 PC，手持设备和机顶盒等
- 支持不同安全级别的解决方案，包括软方案、硬件方案和增强硬件方案
- 符合 ChinaDRM 标准，SecureMax 系统通过了广电 ChinaDRM Lab 的标准符合性和安全性测试
- 各个安全级别的方案，其安全性均通过了国际第三方 Farncombe 的测试认证
- 具有规模部署的成功案例

5. 适用领域

本方案适用于公共服务领域的数字电视、互联网电视和互联网视频行业。

用于行业中的内容版权管理，以保护运营商/服务提供商和内容提供商的合法权益。

6. 企业分工

方案实施过程中的相关企业包括：

- 芯片提供商，终端芯片和安全芯片
- 设备提供商：头端专用设备如加密机，终端运营商控制设备如机顶盒

- DRM 方案提供商：提供 DRM 端到端的解决方案供应商
- 系统集成合作厂商：运营或提供服务所需要的其它后台系统，比如：运营管理系统，内容管理系统等
- 运营商/服务提供商：提供音视频直播或点播等服务提供者

以永新视博 DRM 系统 SecureMax 为例，其产品清单包括：

1) 证书加密机
2) 授权服务器
3) 数据库
4) 直播/点播加密机
5) 终端软件/硬件

7. 应用案例

目前国内 DRM 系统整处于初级阶段，已经出现了一些应用和部署需求。

永新视博 DRM 系统 SecureMax 已经有一些应用的案例，但到目前为止，国密算法的 DRM 系统还没有实施部署。主要原因是一些外部条件不完全成熟，比如，具有国密算法的数字电视终端和机顶盒芯片启动较晚。目前永新视博正在积极推进国密算法的 DRM 系统的部署。

北京永新视博数字电视技术有限公司

联系人：张晶

电　话：1355292869

数字版权保护密码应用解决方案

1. 概述

互联网和多媒体技术的快速发展，使得数字化媒体的传播越来越迅捷。由于数字化作品易于修改、复制和二次传播的特点，网上存在大量的盗版和侵权问题，严重侵犯了内容原创者和提供商的知识产权以及经济利益，使得数字版权的保护问题越来越重要。在此背景下，能对数字化信息内容进行存取控制和版权保护的数字版权管理（Digital Rights Management, 版权保护）技术便应运而生。它是一项涉及到技术、法律和商业各个层面的系统工程，为数字媒体的商业运作提供了一套完整的实现手段，同时确保了数字媒体内容能够被合法的使用。

基于国内版权管理发展状况，结合广播电视、互联网领域视频媒体对版权管理的技术要求，采用国产密码算法对广电领域电视直播信号、互联网视频等进行版权保护，版权保护领域是国家"十三五"规划当中非常重要的一个方面，因为随着媒体融合的加速发展，内容的保护、内容创新将越来越重要。内容创新，除了技术、业务制作的创新以外，还有非常重要的一个机制的支撑是版权保护，如果版权得不到很好的保护，内容得不到很好的保护，就很难谈生态的创新、业务的创新、内容的创新。

2. 需求分析

2.1 安全防护需求

随着广播电视业务信息化、网络化的发展，过去的盘带拍摄、制作、播出已全面数字化，传统意义上的制作、播出安全已全面扩展至信息系统的信息安全领域。同时随着融合媒体以及云计算的出现，为整个广电行业的信息安全带来的巨大的挑战。2013 年韩国 KBS、MBC、YTN 等多家主流电视台计算机网络遭到攻击造成全面瘫痪，此次攻击造成了上述电视台的网站无法登陆，电视节目编辑设备死机，录制存储的部分节目遭到破坏等。

2.2 版权保护需求

在国内，据统计，2016 年网络视频盗版侵权带来的潜在的广告展示和版权付费损失超过 150 亿元。据不完全统计，每年因盗链、网盘侵权损失的流量及数量超过 2 千万次，因盗版损失的会员收费预计在 20 亿元左右。视频盗版对正版品牌价值、广告会员投入、版权付费、带宽消耗四方面造成直接损害，严重影响正版网络影视的发展。

目前国内网络与信息系统在电台、电视台、传输网中的应用越来越广泛，网络电视台、IPTV 等新媒体的影响力日益增强，作为国家重点行业的基础信息网络和系统，广播电视领域的信息安全关乎到国家安全、经济发展和社会稳定。

2.3 密码功能需求

根据版权保护的业务逻辑，采用密码算法进行保护，需要提供的密码功能主要集中在以下几个方面：

身份认证：识别系统中所有的设备，配合鉴权系统确认用户或者设备的合法性、配合计费系统确认用户或终端是否具备使用权限；

内容加解密：服务端需要对视频内容进行加密、转码以及内容分发，终端需要对视频内容进行解密、解码输出到屏幕。

密钥分发：服务对视频内容进行加密保护后，需要将加密的密钥安全地传送到终端，以便于终端使用此密钥对相对应的内容进行解密。

3. 方案架构

数字版权管理（Digital Rights Management,版权保护），就是对各类数字内容的知识产权进行保护的一系列软硬件技术的结合，用以保证数字内容在整个生命周期内的合法使用，平衡数字内容价值链中各个角色的利益和需求，促进整个数字化市场的发展和信息的传播。版权保护的核心就是通过安全和加密技术锁定和限制数字内容的使用及分发途径，从而达到防范对数字产品无授权复制和使用的基本目标。版权保护应贯穿数字媒体的整个生命周期，包括：内容制作、内容存储、内容发行、内容接收、内容播放、内容显示等。不同的版权保护系统虽然

在所侧重的保护对象、支持的商业模式和采用的技术方面不尽相同，但是它们的核心思想是相同的，都是通过使用数字许可证来保护数字内容的版权。用户得到数字内容后，必须获得相应的数字许可证才可以使用该内容。

3.1 技术架构

版权保护系统的功能模型主要分为三个部分：内容服务器、许可证服务器和客户端。三个模块必须协同工作，才能构成完整的数字版权管理系统。系统基于密码技术、授权技术等构建。

内容服务器基于对称密码算法对音视频等数字内容进行加密，内容加密封装格式符合 ChinDRM 相关技术标准；同时可基于运营系统定义的内容消费场景设置内容使用规则；许可证服务器根据版权保护客户端的请求将内容加密密钥、内容使用规则等按照规定的内容授权机制封装成许可证发送给版权保护客户端。

版权保护客户端在播放内容时需根据内容元数据信息从版权保护服务端申请内容播放许可证；根据从版权保护服务端获取的许可证中的内容加密密钥及内容使用规则进行内容的解密播放。

版权保护服务端和版权保护客户端之间基于 PKI 技术建立信任关系，基于此信任关系进行安全通信，实现双方之间的身份认证和许可证安全传递。

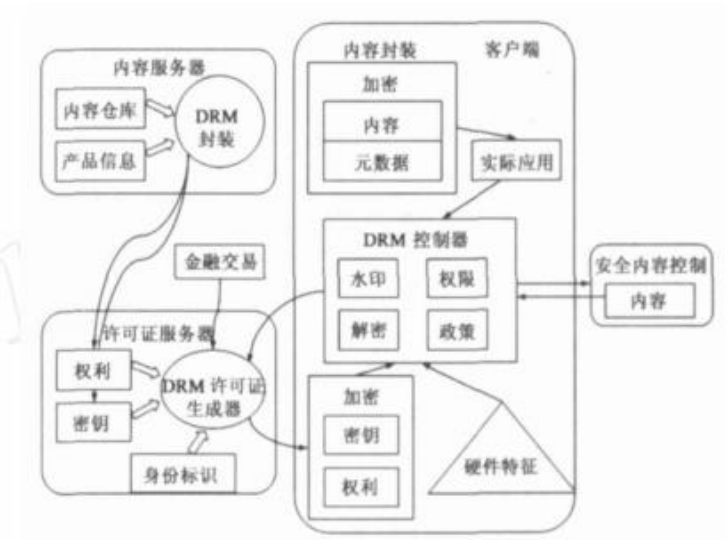


图 3-1 技术架构图

3.2 产品部署图

版权保护系统的部署如下图：

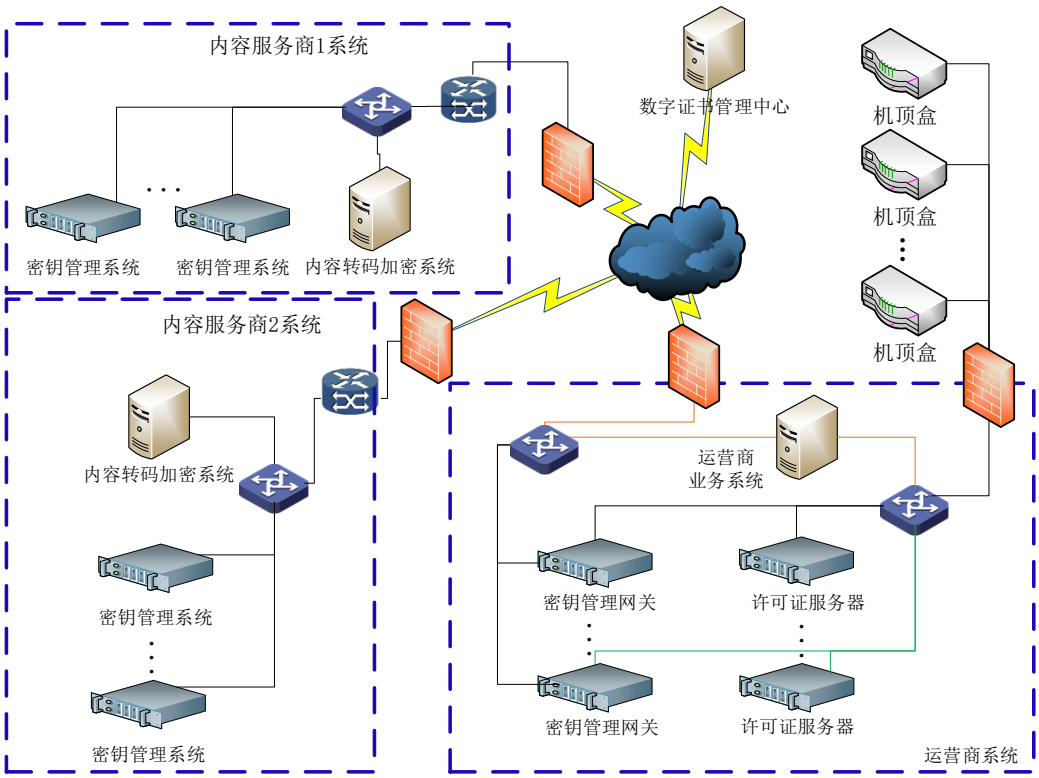


图 3-2 方案部署图

密码设备及版权保护的业务系统部署分为以下三个部分：

内容服务商系统：内容服务商主要使用密钥管理系统实现内容加密系统加密密钥的生成和管理、分发等；为防止单点故障，密钥管理系统在部署时可以采用热备或冷备部署方式。

运营商系统：运营商主要使用许可证服务器、密钥管理网关对内容密钥进行获取、管理、分发及对终端的授权；终端一般是机顶盒或智能终端（手机、平板、PC 等）内部集成了密码运算模块，实现申请密钥及内容解密、解码等功能。运营系统中的密钥管理网关和许可证授权系统是 DRM 系统中最重要的功能部分，同时也是受到访问压力最大的部分，运营商应根据实际终端数据及并发访问量规划使用的设备数量，密钥管理网关和许可证授权系统支持主辅工作模式，即主模式下会主动向其他辅助设备推送关键数据，确保密钥信息一致；并通过此方式支持扩容，实现负载均衡，防止出现单点故障。

认证中心：认证中心负责为系统中每个设备分发数字证书，为系统中的各类设备建立信任基础，同时，为运营商系统提供证书认证、有效期查询等服务。

3.3 主要功能

3.3.1 内容加密封装

内容加密封装一般指对内容进行分段加密，将视频内容标识、许可证获取URI、内容加密算法、初始向量等客户端用来获取许可证解密内容的必要参数封装在内容或其索引文件中。当前主流的分段加密机制包括 HLS 加密封装、CENC 加密封装、MPEG-DASH 分段加密等。

3.3.2 内容授权

许可证服务系统基于密钥与密钥使用规则关联的机制实现内容的许可授权。DRM 服务端采用内容加密密钥加密数字媒体内容，将内容加密密钥和其它与内容相关的密钥（如会话密钥、业务密钥、存储密钥等）采用层级密钥加密的方法加密后与各密钥对应的密钥使用规则一起打包成内容授权许可证发送给 DRM 客户端，DRM 客户端按照层级密钥体系中各级密钥的使用规则使用密钥，实现对数字媒体内容的解密播放。下级密钥使用上级密钥进行加密保护，每一个密钥都有对应的密钥使用规则，下级密钥只能在上级密钥使用规则规定的条件下进行解密，即下级密钥继承了上级密钥的密钥使用规则；每一个密钥又可能有多个密钥使用规则，密钥只能在满足其所有使用规则的前提下才能够被使用。

3.3.3 安全信任机制

版权保护系统的安全信任机制基于 PKI/CA 技术构建。系统中的服务端、客户端等都向认证中心申请获得一个数字证书，作为自己身份的凭证。

3.3.4 内容密钥管理及分发

密钥管理网关负责连通内容加密转码系统和许可证授权服务系统，接收内容加密转码系统推送过来的内容加密密钥，同时接收许可证授权系统对内容密钥的申请，并进行封装分发，确保内容密钥安全传输。

4. 方案特色

China 版权保护是"十三五"规划当中非常重要的一个方面，因为随着媒体融合的加速发展，内容的保护、内容创新将越来越重要。内容创新，除了技术、业务制作的创新以外，还有非常重要的一个机制的支撑是版权保护，如果版权得不到很好的保护，内容得不到很好的保护，就很难谈生态的创新、业务的创新、内容的创新。同时，在广电总局的指示精神的要求和指引下，国产密码算法在版权保护方面进行加强。

基于国产密码算法的版权保护应用技术方案是依据国家有关信息安全政策、法规，结合我国广电领域实际情况，在消化吸收国内外先进经验和技术基础上，立足国内自主研发，按照科学的管理思想进行设计。所设计的应急广播系统安全体系要求达到安全可靠、节俭实用、便于操作、易于维护和管理的要求。

同时版权保护系统还具备以下特色：

（1）遵循国家密码管理局有关技术标准；

（2）形成了具有国内推广价值的应用方案和产品；

（3）符合国际版权管理要求，适用于国内广电领域、互联网视频等方面；

5. 适用领域

结合国内视频产业的发展，基于国产密码算法的版权保护系统可以应用于各类电视台、互联网视频运营商、各地有线运营商等。

6. 企业分工

版权保护系统中主要采用的密码产品如下：

序号	产品名称	主要功能	产品型号	提供厂商
1	密钥管理系统	视频加解密密钥生成、管理、分发	SYT1401	北京江南天安科技有限公司
2	密钥管理网关	内容密钥管理、分发	SJJ1310	北京江南天安科技有限公司

3	许可证授权系统	内容许可证分发	SRJ1303	北京江南天安科技有限公司

7. 应用案例

广东南方新媒体股份有限公司是广东广播电视台通过整合旗下新媒体产业而成立的专业公司，具备国家广播电视总局颁发的互联网、移动互联网及专网视频业务的全部管理牌照。基于 ChinaDRM 的推广模式将建成首批 80 万终端用户的版权保护系统应用示范。

北京江南天安科技有限公司

联系人：朱家雄　　刘赛

电　话：13811190764　　13260283690

010-82326383　　010-82326383

数据全生命周期保护密码应用解决方案

1. 概述

云计算、大数据、人工智能和移动互联网的飞速发展，在带给社会便捷和智能的同时，也存在着数据泄露和滥用问题。2016 年 12 月，雅虎公司宣布其超过 10 亿的用户账号被黑客窃取。其中，敏感数据的安全保护当属人们最关心的问题之一。敏感数据作为组织（包括企业、政府等）的核心资产和个人的隐私信息，受到组织和个人的高度重视，通常包括核心代码、设计图纸、身份证号和健康信息等。

《中华人民共和国网络安全法》第十条明确要求建设、运营网络或者通过网络提供服务，应当维护网络数据的完整性、保密性和可用性；第二十一条：“采取数据分类、重要数据备份和加密等措施”；在法律层面，给予数据保护高度重视。刚刚发布的《信息安全技术网络安全等级保护基本要求》明确要求在三级及以上信息系统的安全通信网络和安全计算环境中使用密码技术。《信息系统密码应用基本要求》对等级保护不同级别的系统中密码技术的使用要求的更加细致。这些法律法规的出台无疑推动了密码技术在信息系统中的普及和应用。

2. 需求分析

数据的全生命周期通常包括使用、传输和存储三部分。在未经防护的情况下，数据的全生命周期都是以明文形式存在，一旦发生数据被盗，或者攻击者绕过权限非法访问，明文数据所承载的敏感信息的泄露势必会对相关组织和个人产生重大经济、名誉等损失。此外，数据全生命周期的防篡改意义重大，尤其在电子商务，网上银行等金融领域，数据的完整性是整个业务的基础支撑，很难想象一笔转账的金额被篡改后所造成的恶劣后果。云计算的弹性扩展和按需付费，使得大批企业纷纷上云，在享受云计算便捷的同时，数据的安全问题则变得更加棘手。由于其开放共享的特性，传统的物理边界消失，给数据的保护带来了新的挑战。

3. 方案架构

3.1 技术架构

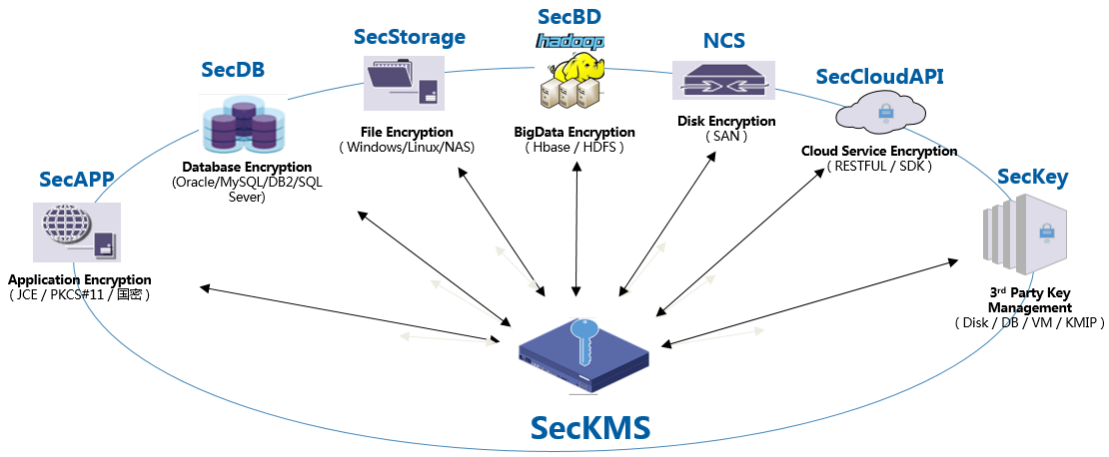


图 3-1 逻辑示意图

三未信安数据安全保护平台（以下简称“平台”），专门为保护敏感数据全生命周期的安全而设计，通过为用户提供功能丰富且易用的数据保护方案保证数据的保密性、完整性、真实性和可用性。平台以 SecKMS 密钥管理系统为核心提供不同层级的访问控制和数据加密产品，包括数据库加密（SecDB）、文件系统加密（SecStorage）、磁盘加密（NCS）、应用程序加密（SecApp）和大数据加密（SecBD）等。平台的应用场景广泛，包括数据中心，云环境以及它们的混合场景。

3.2 产品部署图

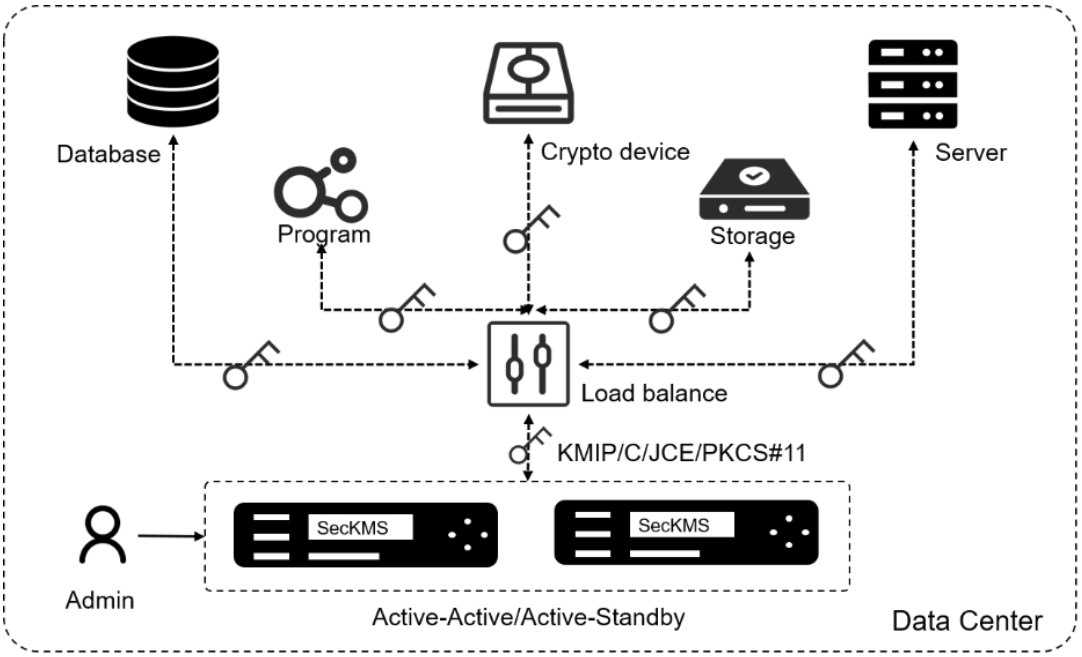


图 3-2 产品部署图

SecKMS 通过集群功能以双活，多活或者主备等方式为应用提供高可用的密钥管理服务。加密客户端部署在相应的服务器中，通过 TCP/IP 协议调用接口，实现数据的密码运算和密钥管理。管理员可以对 SecKMS 进行统一的管理和配置，包括密钥管理，系统管理以及人员权限分配等。当业务系统部署在云中时，SecKMS 通过云中 VPC 技术实现逻辑隔离，提供给 SecKMS 一个独立安全的运行环境。所有加密客户端通过 API 与 SecKMS 实现通信，以实现密钥的集中管理和密码运算。

3.3 主要功能

- 保证敏感数据机密性和完整性
- 保证数据在使用、传输和存储时的机密性和反篡改
- 集中的管理密钥和策略配置
- 采用企业级密钥管理系统实现所有加密客户端密钥统一管理和授权

3.4 主要技术指标

数据保护平台主要采用密码技术实现数据安全，相关的技术指标包括加解密，

密钥生成、获取等。具体参数如下：

SYT 1306 SecKMS 产品性能参数	
密钥容量	≥10000 万
KMIP 协议密钥容量	≥500 万
算法类型	SM1、SM2、SM3、SM4
性能指标	
KMIP 创建密钥	600Tps
KMIP 获取密钥	800Tps
SM2 生成	10800Tps
SM2 签名	30000Tps
SM2 验签	24000Tps
SM2 加密	6400Tps
SM2 解密	7200Tps
SM1 算法加解密	800Mbps
SM4 算法加解密	800Mbps

SecKMS 可支持 2000 个并发的业务系统，对存储到加密磁盘中的数据可达 750MBps。

4. 方案特色

- 数据保护类型丰富

平台可针对数据库、文件系统等实现结构化和非结构化数据的保护

- 密钥管理安全灵活

平台密钥管理采用合规的硬件密码模块保证密钥安全，并且使用灵活

5. 适用领域

北京三未信安 Sec 系列产品支持 KMIP（Key Management Interoperability Protocol）的标准协议，可广泛应用于金融领域、能源领域、水利/自然资源领域、国防和工业领域、公共通信领域、交通领域、公共服务领域、电子政务等领域。

SecDB、SecStorage、SecAPP、SecBD 等软件部署安装在不同行业和领域的业务系统中，通过 SSL 通道和 KMIP 协议与 SecKMS 连接。SecKMS 对各模块的密钥进行全生命周期管理，包括密钥生成、密钥分发、密钥归档、密钥轮换、

密钥备份、密钥删除、密钥销毁等操作。同时，SecKMS 可对业务系统中的用户进行权限策略配置，防止非授权用户访问业务系统和业务数据。

6. 企业分工

北京三未信安在实施过程中负责提供三未信安的安全产品、产品中的标准接口、合同规定的售后服务，必要时可提供产品的机房部署。

三未信安的产品清单包括：

序号	名称	
1	SecKMS	密钥管理系统，型号 SYT1306
2	SecDB	数据库加密软件
3	SecStorage	存储加密（文件加密、磁盘加密）软件
4	SecBD	大数据加密软件
5	SecAPP	应用加密软件

7. 应用案例

三未信安产品全面支持国密算法，其数据安全解决方案广泛应用于金融领域（客户有 Visa、戴姆勒金融、花旗银行等）、能源领域（客户有中石油、中石化、国网等）、水利/自然资源领域（客户有中国水利部）、国防和工业领域（客户有海关等）、公共通信领域（客户有华为等）、交通领域（客户有北汽等）、公共服务领域、电子政务（客户有北京 CA、上海 CA 等）。

案例 1 中石油和中石化的数据加密

中国石油和中国石化使用三未信安的密码机产品，对业务系统和数据进行加密存储，并通过密钥生命周期的管理，达到数据安全保护的目的。

案例 2 华为云专属加密

基于三未信安为华为华北区（北京）提供加密实例的专属加密服务，基于国密算法，提供多种权限认证并支持加解密、签名、验签、产生密钥和密钥安全管理等服务。

北京三未信安科技发展有限公司

联系人：鹿淑煜

电　话：18678882580

0531-88988936

透明文件加密应用解决方案

1. 概述

我们当前已经从 IT 时代走向了 DT 时代。IT 时代是信息技术的时代，DT 时代是数据时代。企业日常经营涉及大量数据共享和流转。2017 年国数经济规模达 27.2 万亿，占国内生产总值（GDP）比重达到 32.9％ 。数字化同时带来机遇和挑战，用户需要共享与安全兼得。但是数据泄露事件日趋频繁、触目惊心。

来自企业内部的数据安全威胁客观存在，好人坏人难辨的情况下仍需要共享和使用数据，所以必须推动以数据为中心、以密码为主动防御手段的企业安全建设。

由于国防军工、金融、交通、政务等关键行业敏感信息的泄露对社会危害巨大，国家也正在积极不断推进保护数据安全相关的法律法规建设。2018 年 7 月两办联合发布《密码工作规划》表示，密码防护数据安全是的工作重心，需要在关键信息基础设施、重要领域应用密码产品，实现数据全生命周期的防护。2018 年 7 月网信办《关键信息基础设施安全保护条例(征求意见稿)》第五十三条，关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。

目前，现有信息系统中广泛缺失密码能力，而且国外密码算法(如 AES、RSA、SHA256)占据大部分市场份额，国外密码从供应链安全角度存在安全风险，密码作为战略性资源和重要核心技术，不能受制于人，必须发展自主密码国产。早在 2018 年 3 月《密码法》进入人大年度立法计划。

商用密码的在数据安全领域的推广应用具有重大意义，首先、密码保障国防军工、金融、交通、政务等重要领域数据安全；其次、有力支撑信息领域核心技术突破；最后，切实维护国家安全、促进经济社会发展、保护人民群众利益。

2. 需求分析

数字化的发展，加速了数据的共享和流转，推动了企业业务效率快速提升，

为企业带来了巨大利益，而高价值的非结构化的文档类数据成为更加明确的攻击目标，重要的文档数据是企业核心业务风险。

企业文档数据安全风险主要来自，外部的攻击者通过各种手段和技术突破防线来窃取数据；内部的恶意人员通过隐藏方式，将有价值的数据盗取来获取利益。

企业敏感的文档数据的全生命周期，包括数据采集、数据加工、数据存储、数据使用、数据分发、数据销毁几个环节均存在被泄密的风险，其中数据存储、数据使用、数据分发是重点。

企业文档数据泄密风险防护的主动防御重要手段是加密，并考虑与网络安全被动防御管理的联动，例如边界防护的防火墙、统一审计的日志管理、第三方的身份认证等的联动，可以构建多维度多层次的数据安全防护体系。

3. 方案架构

炼石透明文件加密方案（简称 TFE）可以实现逐文件逐密钥的静态数据加密，通过在应用系统文件加密驱动层做配置升级，应用免开发改造实现存盘文件密文存储。

3.1 产品部署图

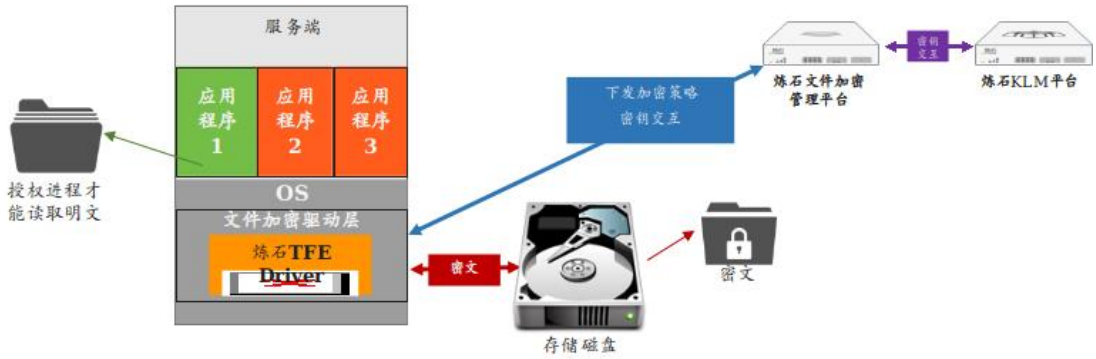


图 3-1 产品部署图

炼石透明文件加密管理平台，提供策略下发、密钥全生命周期管理、审计等功能。

透明文件加密插件通过对应的组件模块客户端来对这些组件模块进行访问。文件存储时，经由透明文件加密插件后被加密，再存储到磁盘上；文件读取时，

经由透明文件加密插件后按照规则被解密。

炼石透明文件加密管理平台，负责定义、调整策略平台规则，如黑白名单等，以及保存审计记录。

密钥全生命周期管理平台（简称 KLM）统一进行加解密所使用密钥的管理工作：文件加密管理平台与密钥生命周期管理平台进行交互，获取加解密所使用的密钥。

在目标服务器上运行一个进程，对炼石透明文件加密插件生成的日志文件进行扫描处理，将内容发送到炼石透明文件加密插件审计组件/炼石文件加密管理平台，保存。

3.2 主要功能

支持主流操作系统环境：支持 Windows 以及 Linux 环境。

非结构化数据加密：可以对任何类型的非结构化数据加解密处理，如：各种格式的图片、微软 MS-office 文档等等。

指定文件加密：可指定要加密的文件夹，该文件夹（及其子文件夹）的文件在保存时被加密。

可识别应用：选择要授权的应用，通过白名单机制使应用正常访问；未授权应用或者直接拷贝文件，只能读取密文文件。

对应用透明：加密插件对应用是透明，不改变之前的运行机制，写入加密，读取解密。

细粒度的访问控制：提供主体到人、客体到文件级别的控制。

数据审计：记录识别到的主客体信息，提供对加密文件的审计日志功能，并且防篡改。

满足合规要求：硬件产生真随机数，加密算法支持国密 SM2、SM3、SM4，具有商用密码产品型号证书。

支持高可用：支持 HA 高可用方式部署，支持主、从互备，防止主机故障、网络故障、程序故障引起的业务损失。

支持大规模部署统一管控：面对企业信息系统多、数据库多的情况，可部署统一数据库加密管理平台和密钥生命周期管理平台，集中管理。

3.3 主要技术指标

炼石透明文件加密平台上线后，原有业务系统存储、读取文件的速度下降不高于 10%。

涉及的密码算法性能指标：

密码算法	执行操作	性能（单线程）
SM2	签名	每秒 2.7 万次
	验签	每秒 1.5 万次
SM3	哈希	2.4 Gbps
SM4	加解密	Gbps

注：以上性能测试结果均基于 Intel i7 处理器

4. 方案特色

细粒度的访问控制：提供主体到人、客体到文件级别的控制。

满足合规要求：加密算法支持国密 SM2、SM3、SM4，具有商用密码产品型号证书。

高质量密码能力：加解密速度快，基于 Intel i9 处理器,多线程模式，单颗 CPU 加解密速度达到 130Gbps。

5. 适用领域

重点行业有：航天、军工、高端制造、金融、交通、政务等等。

业务场景主要有：PLM 系统的数模文件、CAD 系统的设计图纸、保险公司的保单电子原件、电子政务的红头文件。

6. 企业分工

主要实施步骤：需求分析、数据文件分级、方案设计、验证测试、切换上线、运行维护。均由北京炼石网络技术公司负责实施完成。

主要产品清单如下：

炼石 CipherGateway 业务应用安全网关（型号：SJJ1717）；

炼石 CipherSuite 密码软件（型号：SJM1808）。

7. 应用案例

7.1 中电 53 所 PLM 设计文档安全

西门子 TeamCenter 应用软件完全无改造；

实现针对特权账户的约束管理；

实现应用用户超时登出；

实现基于国密算法的文件透明加密存储。

7.2 九天微星文档系统业务安全

与炼石文档管理系统无缝适配集成，业务系统无需改造；

结构化数据与非结构化数据，统一平台策略加密存储；

平台高可用，支持双机热备。

北京炼石网络技术有限公司

联系人：钱晶

电　话：15201490479

010-88459460

隐私数据保护密码应用解决方案

1. 概述

随着我国社会网络化、数据化和智能化的加速推进，数据成为社会经济发展的驱动力。如何在维护隐私和数据安全利益的前提下，促进数据的开放、共享和流通利用，成为推动数据经济发展的关键所在。在网络普遍应用之后，内部泄露、非法窃取、买卖公民个人信息等成为社会公害，不仅危害个人隐私，而且是数据正当使用的“拦路虎”。《网络安全法》、《个人信息安全规范》、《等保 2.0》、《通用数据保护条例》等国内国际政策法规格要求企业强化信息安全建设，进行信息安全保护；基于商用密码，实现对隐私数据的保护，既有利于保护公民的信息安全，也能有效的保障企业健康发展。

2. 需求分析

隐私数据往往以多种形式多种状态存在于企业的系统中，如数据库（关系型数据库、非关系型数据库）、文件(存在于系统中或磁盘中)等。安全风险存在于如下：

自外部黑客常见的攻击手段和漏洞包括：SQL 注入、缓冲区溢出、拒绝服务、提权等，也有利用未及时安装补丁、缺省安装漏洞、程序后门和危险代码破坏权限体系，导致数据库服务终止和敏感数据泄密。内部运维人员和 DBA：明文存储的安全威胁，使得数据文件、备份文件被拷贝后，可以轻易恢复。DBA 等高权限用户可以随时任意地访问敏感数据；弱口令的存在，使得容易被人暴力破解或尝试成功，访问敏感数据导致泄密和篡改；内部人员、第三方维护人员的误操作、维护操作、越权操作和恶意操作。总之隐私数据存在批量脱库或文件导出等风险，使得数据安全处于严重安全威胁中。

隐私数据保护需要能够提供综合的面向数据库、文件、磁盘、传输等各种形式的各种状态的系统数据加密保护手段，保障数据全生命周期，全业务流程的安

全性。

3. 方案架构

北京江南天安科技有限公司通过对隐私数据泄密的综合分析，打造企业级密钥管理系统，对企业的用户隐私数据进行全流程加密保护。

3.1 技术架构

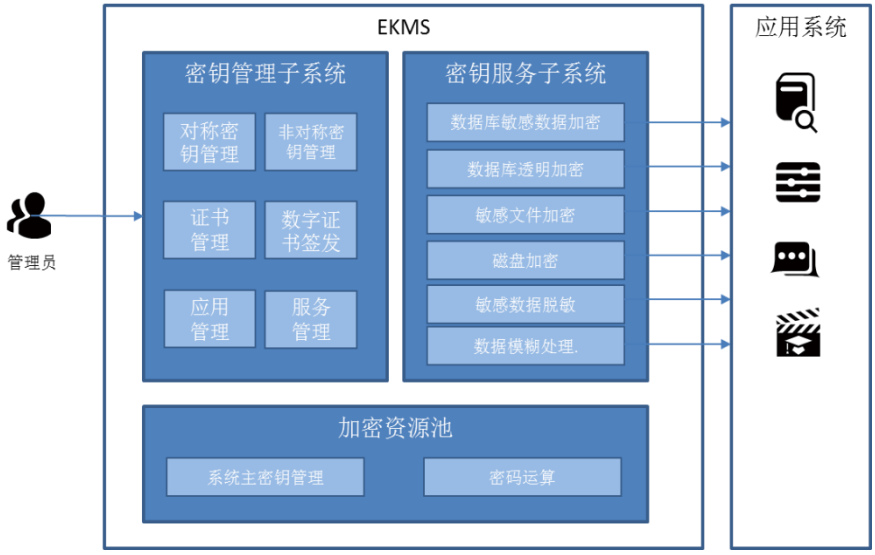


图 3-1 技术架构图

企业级密钥管理系统基于商用密码机提供安全合规的密码计算服务能力，通过统一的密钥管理，对应用于各系统的密钥进行统一的密钥生成、派发、备份、恢复、更新、归档、销毁、查询等生命周期管理，结合严格的密钥使用授权，密码服务功能可对数据库、文件系统、业务系统等提供各类隐私数据保护方案。结合云加密资源池的服务能力，使得系统可支持上层各种业务应用。

3.2 产品部署图

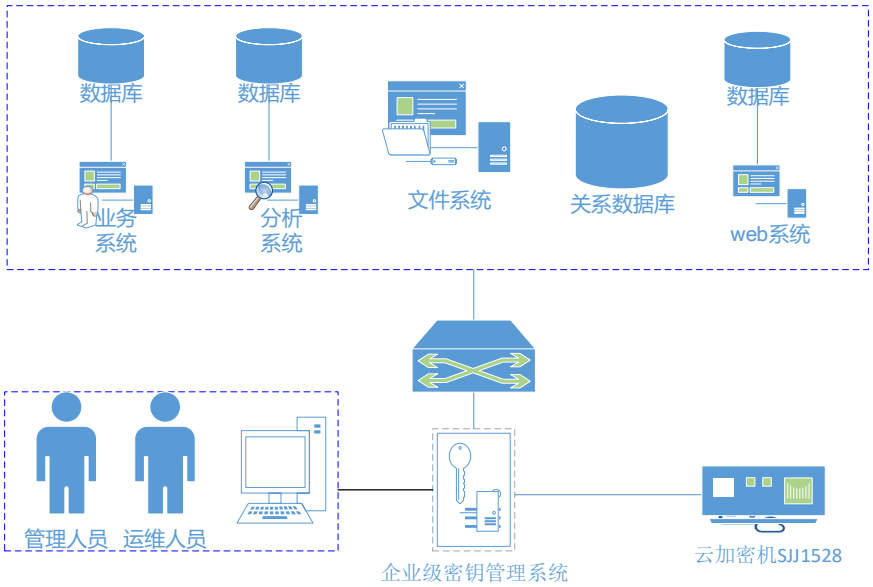


图 3-2 产品部署图

3.3 主要功能

本方案可以通过密钥管理系统面向隐私数据提供如下保护功能：

敏感数据加密功能：提供面向关系型数据库、非关系型数据的敏感数据加密，并解决因数据加密而造成对数据特征的破坏问题，提供数据密文模糊检索功能。

数据库透明加密：针对大规模存量系统无法进行改造时，提供数据库透明加密功能，在不改造现有系统功能前提下，实现对落盘数据密文化处理，增强安全保护。

敏感文件加密：针对系统中存在的大量包含有隐私敏感数据的文件，提供文件加密功能，实现文件流转、存储过程中加密。特敏感数据可以实现文件不出系统，本机实现密文化。针对大文件提供优化处理方案，实现快速高效密文化。

磁盘加密：通过文件系统的加密配置，实现文件在磁盘中存储时以密文形式存在，磁盘丢失不会造成信息泄密，同时操作系统层面对用户透明，无感知。

数据脱敏：屏蔽敏感信息并使屏蔽的信息保留其原始数据格式和属性，以使得应用程序可在使用脱敏数据的开发、测试、或数据分析过程中正常运行，发挥

数据属性价值，但同时对数据进行保护。

面向切面加密编程：提供基于加密标识的引擎，使得开发者无需关心安全方案处理逻辑以及处理过程，通过配置化手段即可实现系统开发过程与加密的关联。

3.4 主要技术指标

平台支持集群化部署。

单平台加密吞吐量不小于 10W TPS。

数据增、删、改、查操作不超过 5ms。

对原系统的性能损耗不超 10%。

4. 方案特色

本方案具有如下优势：

多场景支持：针对隐私数据保护，深入隐私数据存在的每个环节、每种形式、每种状态均可以提供加密方案，而不针对特定的场景，使得数据的全生命周期安全可靠。

密钥统一管理：不同于其他方案，引入加密时，使得密钥分散于各类系统中，密钥的管理难度大。统一密钥管理使得各类业务系统引入加密方案，其密钥具备统一的管理，间接也保障的加密信息安全性。

密码资源动态扩展：结合江南天安云密码资源池技术，使得密码资源可以弹性分配，动态扩展，实现密码资源高效应用，降低运维人员操作风险。

高效性：高性能的密码服务结合各场景下性能优化方案，使得数据引入加密处理同时，对原系统的性能损耗均可控。

安全性：使用国家密码管理局批准型号的硬件加密机，对密钥的生成、存储、分发、备份等，有严格的安全防护措施，符合相关部门政策性要求。

5. 适用领域

本方案可广泛适用于金融、交通、医疗、能源、教育、住建、社保、民生、保险、证券、基金、电信、公安、互联网等领域，实现对系统中的隐私数据进行

安全保护。

6. 企业分工

主要采用的密码产品如下：

序号	产品名称	主要功能	产品型号	提供厂商
1	云服务器密码机	数据加密密钥生命周期管理，数据加解密服务	SJJ1528	北京江南天安科技有限公司
2	企业级密钥管理系统	实现各种对称和非对称密钥生命周期管理，提供各种层次的加密服务。	EKMS	北京江南天安科技有限公司

7. 应用案例

该方案成功助力国内多家大型快递公司实现业务系统敏感数据的加密保护改造。使得涉及敏感隐私数据的众多系统实现了统一的密钥管理、统一的密钥服务、统一的隐私数据加密处理。充分保障快递公司超数亿用户的隐私信息。

其他客户包括：考试中心、某招聘公司、某证券公司等。

北京江南天安科技有限公司

联系人：朱家雄　　刘赛

电　话：13811190764　　13260283690

010-82326383　　010-82326383

通用密码方案

安全门禁系统密码应用解决方案

1. 概述

天地融 SRT1801 安全门禁系统以国家密码管理局颁布的 GM/T 0036 -2014《采用非接触卡的门禁系统密码应用技术指南》为依据，基于银行核心系统的对账平衡原理，采用国家密码管理局颁布的 SM2、SM3、SM4 算法对用户进行身份认证以及数据的全链路加密，实现了用户的安全授权、身份认证、区域出入权限安全管控以及日志记录的安全审计，满足 GM/T 0054-2018《信息系统密码应用基本要求》规范中对门禁系统的相关要求。

2. 需求分析

当前市场上主流门禁系统的安全设计集中在卡和读卡器部分，对于整个门禁系统中用户的授权安全管理、数据传输安全、白名单安全、日志安全等方面保护不足，主要体现在：

- 读卡器与控制器之间采用开放式韦根协议，传输信号很容易被截取分析攻击，伪造信号进行开门控制，造成风险漏洞。
- 开门权限白名单在线路上明文传输，控制器上明文存储，存在被篡改的风险。
- 管理员可以随时对个人进行授权，并且可以修改记录数据，存在职权乱用的风险。

为了解决这些安全问题，采用密码技术对整个门禁系统的前端与后台的功能和数据传输全面加固，采用双向安全通信协议、数据全链路加密、分级授权审批等方式，实现了整个门禁系统的全方位安全。

3. 方案架构

3.1 技术架构

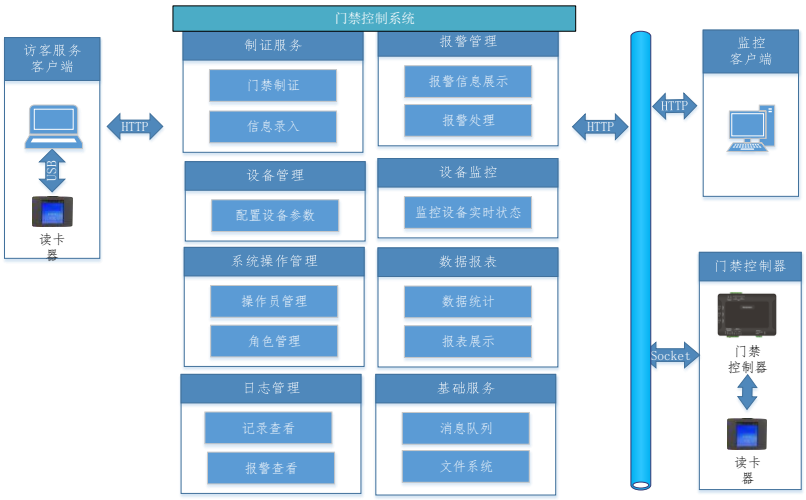


图 3-1 安全门禁系统技术架构

SRT1801 安全门禁系统分为前端设备和后台服务两大部分。前端设备包括部署在各个点位的设备，包括门禁卡、读卡器、控制器等。后台功能包括用户管理、设备管理、运维管理、制证等各类服务。

3.2 产品部署图

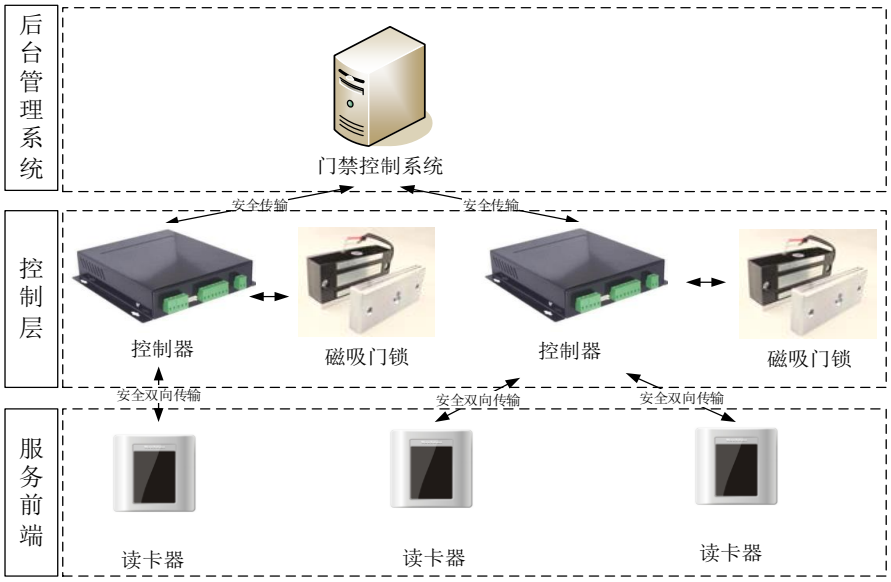


图 3-2 安全门禁系统部署

门禁读卡器和门禁控制器部署在各应用场景，采用基于 PKI 体系的身份认

证，保证人员出入安全运行；后台控制系统集中部署在机房，便于统一管理与维护。

3.3 主要功能

数据全链路加密

设备上电时进行互相间的身份认证与密钥协商，且会话密钥定期更新，对传输数据进行全链路安全保护。系统下发的白名单等数据，以及控制器上传的读卡器刷卡日志等信息，都是经过加密的，避免明文传输，保证运行数据安全，有效防止数据被篡改以及设备被替换。

系统用户权限管理

门禁系统支持根据业务创建不同的管理角色，每个角色可以定义不同的权限，实现业务上的灵活控制。典型角色包括管理人员、操作人员、授权人员、审核人员等，实现了权限多级管控。

制证开卡审计

制证开卡会产生一条系统审核信息推至“提交审核”人员，审核人员可在登录系统后的待办事件模块查看处理该条审核记录，能够有效避免传统管理员的无限制开卡。

3.4 主要技术指标

- 白名单生效时间<1 秒，可以实时生效；
- 控制器支持 10 万条脱机工作记录加密存储；
- 系统支持终端设备数量>10 万，用户数>1000 万；
- 支持 SM2、SM3、SM4 密码算法；
- 遵循 GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》。

4. 方案特色

系统安全逻辑闭环

与普通的门禁系统只能在后台查看刷卡数据相比，天地融的门禁系统通过登

录、授权、制卡、刷卡、认证、审计，多个功能点完成闭环认证，保证每条数据都是卡片刷卡产生，且记录不可删除，有效防止数据的篡改。

门禁卡片防复制

普通门禁卡以可读的 UID 值或简单的软件加密作为身份凭证，可被复制到另外一张门禁卡内，复制的卡同样可作为出入证使用。天地融安全门禁系统的门禁卡基于国密安全芯片研制，密钥由安全芯片随机生成、加密存储、不可读出，可以有效的防止复制。

协议安全高效

市场上通用的控制器通讯协议为摩托罗拉在上世纪设计的韦根协议，缺乏有效的安全架构。天地融自主设计的高速安全传输协议，能够在不改动原门禁线路的基础上，只需更换读卡器和控制器，即可通过复用的线路实现全面支持安全门禁系统的双向安全数据传输。

5. 适用领域

天地融公司自主研发设计的安全门禁系统是高性能、高安全的区域访问管控系统，通过部署在各个出入口的门禁读卡器提供身份认证服务，可广泛应用于居民住宅、企业办公、公共服务机构的人员管控等访问保护场景，例如园区、建筑、办公室等出入口人员权限管控，并支持闸机、中距离读卡器、身份证刷卡、人脸识别等多种场景的扩展。

6. 企业分工

天地融安全门禁相关配套设备为天地融自主研发设计实施，用户可根据需求选择定制，门禁后台服务器支持多种国产型号，灵活可控。天地融提供全套的门禁卡、读卡器、控制器及管理后台，并负责施工实施或配合需求方要求。

7. 应用案例

天地融安全门禁系统可以应用于居民住宅、商业、企业等有访问控制需求的

领域，另一方面，对于原有的安全性不高的门禁系统，比如基于 Mifare1 卡或 ID 卡的门禁系统，可以进行安全替换升级。目前，已在多个重要场景部署，成功实现了人员出入的安全管控。

天地融科技股份有限公司

联系人：程璐

电　话：18610599339

010-56675666

安全键盘密码应用解决方案

1. 概述

随着无纸化办公的日益普及，在开放的互联网安全漏洞层出不穷的大背景下，保证信息的输入安全以及系统准入安全认证等具有广阔的应用空间。

天地融安全键盘高效地实现智能化安全办公。键盘操作简单，灵活可控，通过与安全芯片以及安全摄像头等设备高度集成，无需复杂繁琐的周边硬件，即可实现系统用户本人安全登录、键值记录、人脸定时识别及办公考勤等功能，是理想的一体化办公安全解决方案。

天地融安全键盘支持 SM1、SM2、SM3、SM4 等密码算法，遵循国家密码管理局颁布的 GM/T 0028-2014《密码模块安全技术要求》中密码模块安全二级相关要求，符合国家密码管理局相关要求和规范。

2. 需求分析

当前大部分使用 ID 与密码甚至是智能密码钥匙作为身份认证的系统无法保证是用户本人登录，进一步的，登录信息及输入内容可能被木马劫持，这在一定程度上造成了信息泄露的敞口风险。

天地融安全密码键盘专注于简单高效地实现智能化办公安全。键盘内置高安全芯片，通过 USB 接口与 PC、笔记本连接，通过安全芯片的安全保护功能，以及摄像头的人脸识别与活体检测，可方便快捷的实现信息安全输入、应用安全登录认证、安全电子邮件加密与认证、数据传输加密保护等多种功能。

3. 方案架构

3.1 技术架构

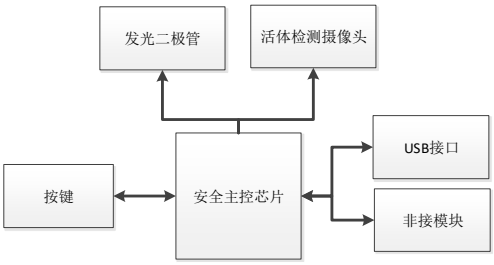


图 3-1 技术架构图

硬件上采用安全芯片作为主控芯片，提供信息加解密、文件数字签名与验证等功能，充分保证信息安全。摄像头带活体检测的人脸识别功能，能够保证是用户本人使用计算机。非接模块和 USB 模块支持各类身份认证卡、智能密码钥匙等外部设备。

3.2 产品部署图

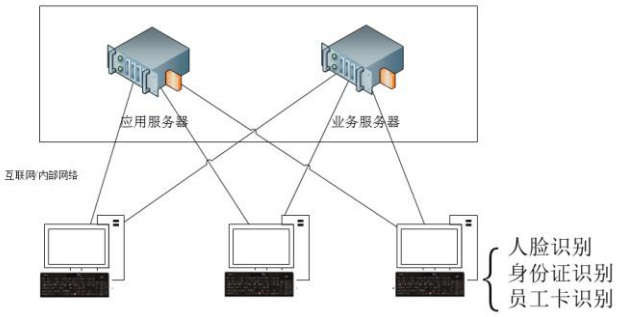


图 3-2 产品部署图

通过前端统一的设备部署，安全密码键盘可以对多个不同的业务提供支持，比如安全电子邮件系统、OA 系统登录、安全公文传递系统等。

3.3 主要功能

安全输入

自带安全芯片，可对按键输入进行加密保护，保障信息加密传输。

授权认证

安全键盘自带读卡器，可支持非接卡及身份证的认证和授权。

键值记录

可实现对键盘键值的记录、人脸照片的定时识别抓取比对与记录，保障办公角色与权限的安全性。

人脸识别

内置小型摄像头，基于云台自动追踪人脸，可抓取识别办公电脑使用人员照片，进行人脸识别登陆电脑系统，支持定时识别办公人员人脸，保证是用户本人操作。

3.4 主要技术指标

项目	指标
尺寸	458(L) x 165(W) x 39.5(H) mm
键盘	104 键
显示屏	0.96’ OLED 显示屏
电源	从 PC USB 供电, DC5V 辅助电源供电
读卡标准	支持 14443-Type A 二代身份证
摄像头	200W 像素，最低光照度：0.5Lux 镜头视角: 120, 支持补光灯
工作温度/湿度	0°C~ 55°C , 0 ~95%（非冷凝）
工作电流	< 220mA (MAX) @12V

4. 方案特色

高兼容性

支持 14443 Type A 、 二代身份证、智能密码钥匙的读取来授权使用设备及权限管理。

安全认证

支持身份证授权认证和人脸识别授权认证登陆电脑系统。

智能办公

安全键盘输入；键值实时记录、人脸定时识别；人脸、身份证验证登陆系统；刷卡考勤等功能。

5. 适用领域

产品以及解决方案通过功能模块高度集成的键盘设备，无需复杂繁琐的周边硬件，即可实现安全输入、安全登录认证、安全文件加密等功能，键盘通过 USB 接口与 PC、笔记本连接，部署方便，操作简单，可广泛应用于政府机关、企事业单位的办公环境中，特别适用于需要对信息安全保护、人员身份强认证的领域。

6. 企业分工

天地融安全键盘相关配套设备为天地融自主研发设计实施，功能实现方案可根据用户需求选择定制，后台服务器支持多种国产型号，灵活可控。天地融公司提供全套的安全键盘及管理后台，并负责施工实施或与总体单位配合。

7. 应用案例

天地融安全键盘专注于简单高效地实现智能化办公安全，打造桌面安全办公环境，是一体化的办公安全解决方案。产品支持输入键值加密、登录认证、安全记录、人脸识别等多项安全功能，为信息系统、办公环境提供安全保护。产品已在多个重要场景部署，成功实现了使用人员的身份管控以及系统信息安全保护。

天地融科技股份有限公司

联系人：程璐

电　话：18610599339

010-56675666

安全视频监控系统密码应用解决方案

1. 概述

“黑天鹅”、“棱镜门”等事件给我国公共视频监控系统的安全应用敲响了警钟。报告显示，全球 228 个国家和地区，8063 个城市，2635 万个摄像头暴露在公网，一旦被黑客成功控制将对公共安全造成巨大威胁。

GB35114-2017《公共安全视频监控联网信息安全技术要求》作为我国首个关于视频监控联网信息安全方面的技术标准，首次对公共安全视频监控的信息安全提出明确规范要求，是全面加强公共安全视频监控领域信息安全的技术依据。

兴唐通信科技有限公司积极响应国家政策，提出视频监控系统密码安全防护解决方案。通过新增安全视频监控前端设备结合对已建系统进行安全加固的方式，实现“身份可信、设备可控、数据可靠”的目标。

2. 需求分析

在物联网、大数据融合应用的推动下，IP 网络摄像头被规模性使用。但随着视频监控建设应用不断深入，也面临着诸多挑战。首先，从前端设备到监控中心，视频数据在采集、传输、存储、调阅过程中处于“裸露”状态，信息安全防护弱，数据与敏感信息存在失控泄漏风险。其次，海量终端接入存在身份认证与大规模管理难问题，海量数据预测预警安全防范处理能力尚不足。另外，当前的视频监控系统接入能力单一，安全产品应用及发挥安全功能效能不到位。

通过上述安全风险分析，梳理出如下安全需求。1）基于国密算法的设备身份认证；2）信令和数据的真实性、完整性、可追溯；3）基于视频帧的端到端视频加密保护，确保视频数据的机密性；4）需基于数字证书用户认证管理，确保合法用户授权访问。

3. 方案架构

3.1 技术架构

以安全传输网络为安全载体，构建从安全前端，到安全中心，再到安全用户的全方位安全框架。配合视频安全密钥服务系统、智能监控子系统等平台支撑，实现设备间双向身份认证、用户身份认证、视频签名应用、视频加密应用。

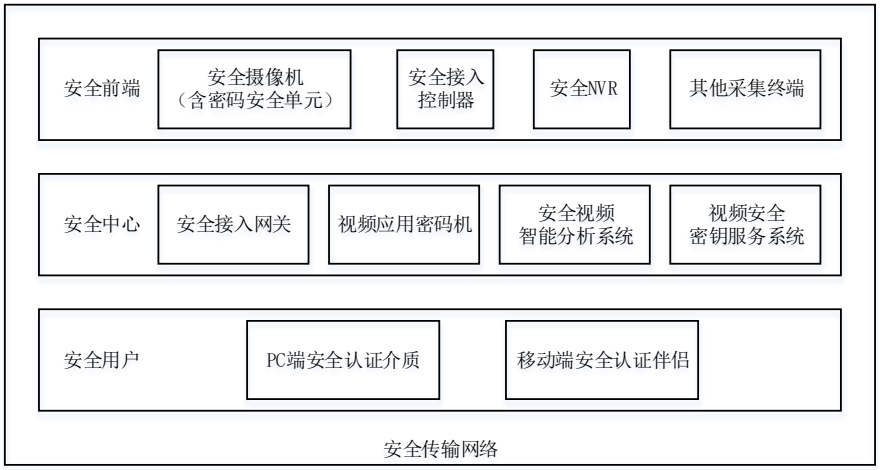


图 3-1 技术架构图

3.2 产品部署图

安全设备部署方式如下图所示：

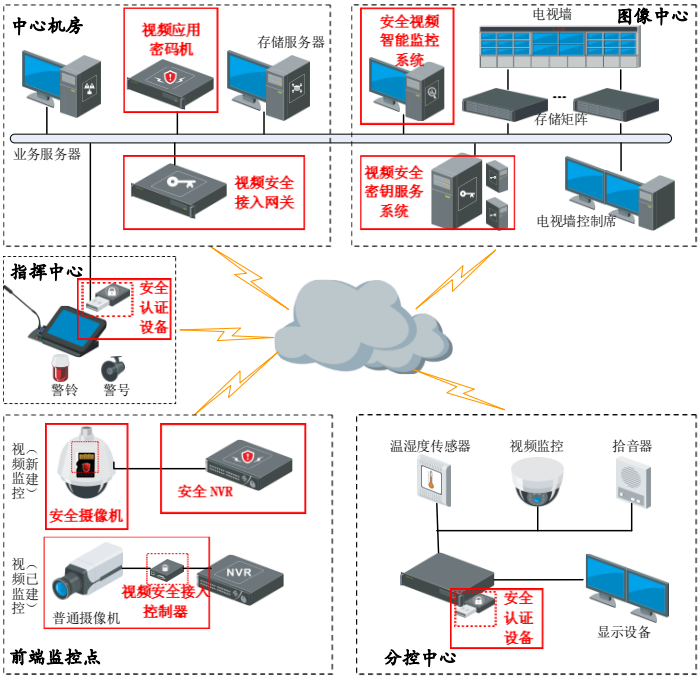


图 3-2 产品部署图

3.3 主要功能

（1）前端设备安全防护。为前端摄像机提供加密存储服务，同时实现身份认证和隧道加密功能。

（2）网络安全防护。对前端安全监控设备视频数据进行机密性防护，对视频流进行加解密转发；完成两侧系统的数据隔离和安全交换。

（3）中心监控平台安全防护。实现后端平台用户身份认证，根据用户权限实施访问控制策略；对视频进行数据解密、正确性验证、安全管控。

（4）用户终端接入管控。针对 PC/平板/手机等不同终端形态采用内嵌安全模块和外接 U-Key 等安全防护设备，实现用户身份认证、视频解密浏览等功能。

（5）视频安全密钥管理。提供证书查询和验证服务、对称密钥管理等功能，支持国家密码标准算法，为视频监控系统后端管理平台提供证书查询和验证等服务。

3.4 主要技术指标

支持 SM1/SM2/SM3/SM4 等国密算法；

前端安全摄像机支持大容量加密存储，加密速率≥30Mbps，存储容量支持

16G/32G/64G/128G；

中心设备支持 300～800 路视频接入，加解密速率≥1600Mbps，签名速率≥3000 次/秒,验签速率≥1500 次/秒。

4. 方案特色

系统设计基于纵深防御理念，采用身份认证、数字证书、网络防护等技术构建密码安全防护体系，为视频监控系统提供全面的安全保障，可解决用户及设备身份认证、信令和数据完整性、视频数据来源可追溯性和机密性防护等实际需求。

系统的前端设备采用多种密码安全单元，提供一体式、分体式等多种安全防护手段，分别适用于新建安全视频监控系统需求和已建视频监控系统的安全加固升级需求，适应性较强，自由度较高。

5. 适用领域

该系统可为政府机构、军事军工、武警边防、司法监所、城管交通、生态环保、能源电力、金融等领域提供“身份可信、设备可控、数据可靠”的安全视频监控服务。与智能分析、态势感知、指挥调度等多种业务整合的能力已得到既有项目有效验证，可为视频监控系统实际应用提供无感密码安全防护。

6. 企业分工

解决方案中涉及产品均可由兴唐通信科技有限公司提供；同时，系统已基本遍历适配主流视频监控厂家产品。欢迎与更多视频监控厂家、安全厂家的多种形式合作。

7. 应用案例

遵循 GB35114 要求，为某省司法监所建设安全视频监控系统。该系统经数月正常运行无故障后，顺利通过了工信部信息产业数据通信产品质量监督检验中心的信息安全功能及性能测试。随后邀请相关单位领导和专家对该系统部署运行

情况进行参观和评估，到场领导和专家认为该系统符合 GB 35114-2017 相关要求，能够在不影响业务系统正常运行的前提下满足用户及设备身份可信认证、信令和数据完整性防护、视频数据来源可追溯性和机密性防护等实际应用需求，可用于指导安全视频监控系统广泛部署和建设。

兴唐通信科技有限公司

联系人：王健安　　胡伟

电　话：13699262399　　13466362701

010-62301206　　010-62302004

安全 USB 摄像头国密改造应用解决方案

1. 概述

现在各大银行的业务处理窗口，外设部分已经大部分完成了国密化改造，但是采集图像信息的摄像头还没有进行国密改造，存在巨大的隐患。

2. 需求分析

摄像头采集个人的头像信息，并进行消息的传递。在传递过程中存在数据泄露或者被截取的风险。目前各大银行的图像采集系统都还在使用老式的普通摄像头，随着金融行业日益增长的外设的安全性需求，有大批的摄像头需要更换更安全的基于国密算法加密的摄像头，或者对现有的摄像头进行改造。本解决方案适用于需要此类需求的项目。

3. 方案架构

本方案通过我司自主设计的基于 ARM SC000 内核的安全国密芯片，通过芯片内部的 USB OTG 连接通用的摄像头模组，并将采集到的数据信息进行加密，通过通用的 USB Device 和主机 PC 相连，将加密后的图形信息传输给银行的 PC 终端。

本方案可以在通用摄像模组的基础上，通过增加一个芯片，实现将通用 USB 摄像头转换为国密加密的安全摄像头。可以支持 SM2,SM3,SM4 等国密算法，性能可以高达 1Mbps.满足银行系统对于信号采集速度的需求。

3.1 技术架构

整体技术架构说明：

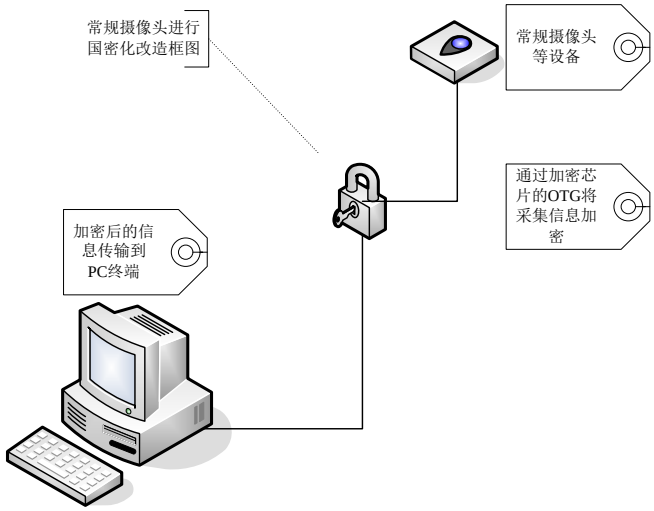


图 3-1 技术架构图

3.2 产品部署图

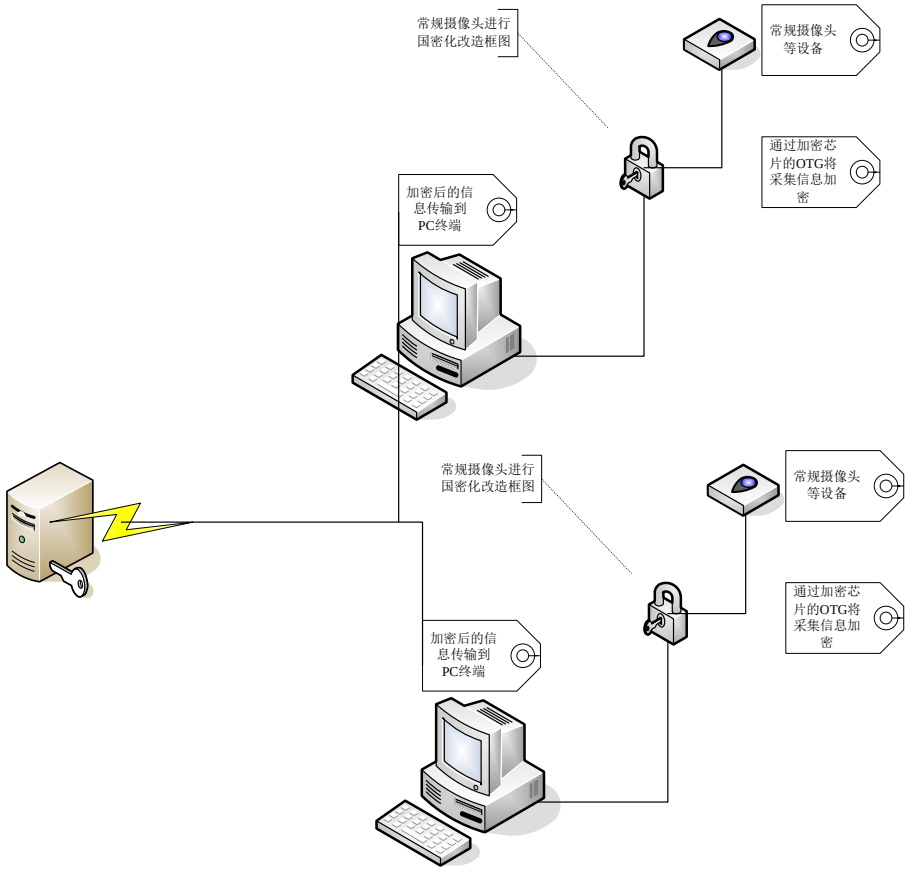


图 3-2 产品部署图

3.3 主要功能

我司拥有自主知识产权的 SSX1616 芯片，具有二级国密认证资质。支持 USB OTG 和 USB Device 双接口。可以在一颗芯片上进行业务功能 1 和业务功能 2。通过 USB OTG 获取摄像头采集到的图形信息，然后使用指定的国密加密标准加密后，主机端（通常是柜员的 PC）通过 USB Device 接口将加密后的图形数据获取。完成摄像头信息的加密采集流程。

业务功能 1:SSX1616 芯片通过 OTG 接口采集 USB 摄像头的数据。

业务功能 2:主控端(通常是 PC)通过 USB 主接口获取 SSX1616 芯片获取到并加密的图形数据。

3.4 主要技术指标

传输速度：1Mbit/s

支持算法：SM2,SM3,SM4

图像传输：可以传输 352*288 分辨率图像 10 张/s

认证资质：国密二级

4. 方案特色

可以在现有 USB 方案的基础上以嵌套的方式加入。

传输速度快。

支持算法全。

使用我司拥有自主支持产权的 SSX1616 国密二级认证安全芯片。

升级维护方便，符合企业需求。

5. 适用领域

适用于银行柜台外设 USB 摄像头的国密化改造项目。

适用于需要将数据信息进行加密传输的 USB 外设类项目。

6. 企业分工

芯片企业：提供芯片和相应的技术方案。

设备集成商：将经过加密后的 USB 设备加入银行系统。

7. 应用案例

某国资密码设备单位使用我司 SSX1616 国密二级认证安全芯片对银行的现有 USB 摄像头进行国密化改造，加强了摄像头采集图像信息的安全性，取得良好的成果。赢得客户好评。

北京华大信安科技有限公司

联系人：樊剑平

电　话：13611288138

安全中间件（SAP）密码应用解决方案

1. 概述

为全面贯彻落实网络安全法、关键基础设施保护条例，加强网络安全和自主可控，进一步提升国外商业软件 SAP 的安全防护水平，保障各领域 ERP 系统的安全自主可控,针对现有 SAP 系统设计了支持国密算法的 SAP 密码中间件功能，旨在推广国产密码算法与安全产品，解决现有 SAP 系统产品的安全隐患和使用问题，提升 ERP 大集中系统的安全防护水平和稳定运行能力。

2. 需求分析

SAP 被誉为“世界 500 强背后的管理大师”，随着 SAP 在中国的应用范围的不断扩大，然而 SAP 服务器在缺省配置下是不安全的，这主要表现在以下两个方面：

- SAP 客户端（SAP GUI）和 SAP 服务器之间的数据通信，包括用户名和口令等重要数据仅仅是压缩传输，未进行加密，由于压缩算法是公开的，所以其安全强度相当于明文传输，安全性较低；
- SAP 服务器本身没有提供原生的数据加密、电子签名等功能，这使得企业的诸如财务这样的核心系统的业务数据在传输过程中存在失窃的可能。而且，尤其是电子签名法出台后，电子签名在企业 OA 尤其是财务系统中的应用需求也日益突出；

3. 方案架构

3.1 技术架构

SAP 密码中间件系统以 Secure Network Communications（下文中简称“SNC”）和 Secure Store &Forward（下文中简称“SSF”）中间件为依托，以 AS 管理为核心，将安全认证、数据加密、数据认证融入到 SAP 业务中，将 PKI 体系与 SAP

业务过程融合，为 SAP 业务中间过程服务。

系统逻辑结构如下所示：

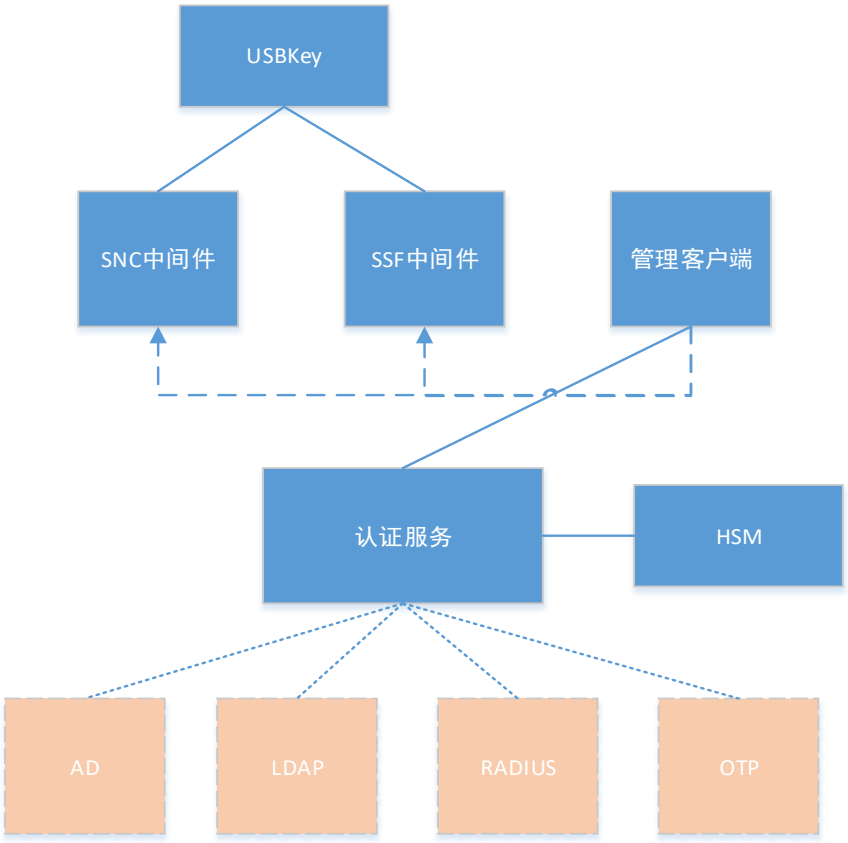


图 3-1 技术架构图

3.2 产品部署图

SAP 密码中间件分为客户端和服务端两个部分，客户端部署在用户办公 PC 端，与用户 USBKey 协同工作；服务端部署在 SAP 业务服务器，与密码机协同工作，如下图所示：

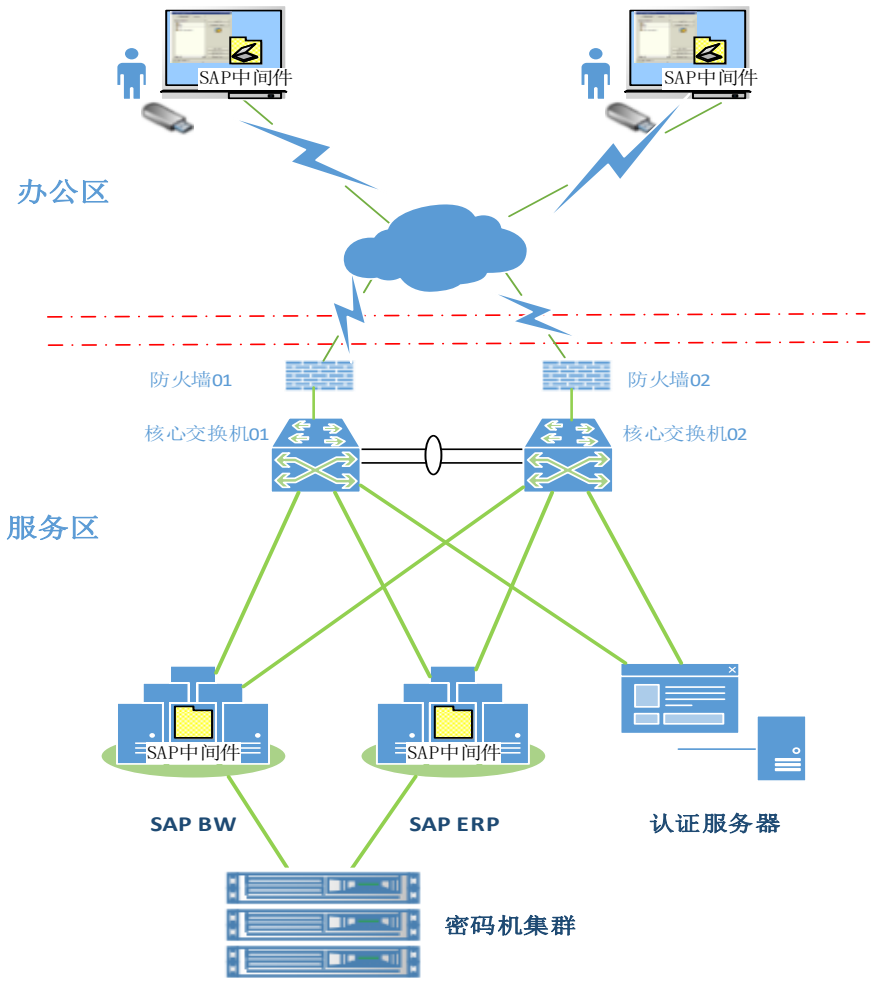


图 3-2 产品部署图

3.3 主要功能

- SNC 安全登录及数据加解密

SAP 密码中间件采用基于 x509 数字证书和数字签名的双向认证方式，在成熟的体系架构上实现用户登录，替代传统的用户名+密码的方式。同时，SAP 密码中间件在 SNC 登录过程中协商会话过程数据加密密钥，在后续的交互过程中对业务数据进行加解密。

- 数据安全存储及转发

SAP 密码中间件采用 PKCS#7 作为安全包的封装格式，实现 SAP 业务流程中数据在业务实体存储及传递的安全功能。SAP 业务系统（如 HR、FI 等）某一个业务流程需要进行数字签名，则调用 SAP 密码中间件软件的 SSF ABAP 应用语言接口实现签名功能进行签名。

3.4 主要技术指标

SNC 登录不大于 0.5 秒；

SNC 数据传输延时不超过 0.04 秒；

SSF 性能不低于 10Mbps；

4. 方案特色

合规密码算法

SAP 密码中间件系统采用 SM1、SM2、SM3、SM4 密码算法，为 SAP 密码中间件系统提供更高的算法强度，更高的计算性能及安全性。

高效信息安全通道

SNC 通道的建立协议由认证协议和通信协议两部分组成。其中认证协议用于完成终端与服务器的身份认证。通信协议用于完成应用数据的加密传输，保证数据传输的高效和安全。

无缝对接

SAP 密码中间件系统依据 GSSAPI 和 SAP 的 SSF 中间件规范进行设计，可与 SAP 系统实现配置化无缝对接。同时，SAP 密码中间件可定制支持 AD、LDAP、RADIUS 和 OTP 等多种第三方认证源。

5. 适用领域

作为世界第一大 ERP 软件厂商 SAP，世界 500 强中有 85%的公司使用了 SAP 的 ERP。同样，在中国很多的大型央企、国企也都使用了 SAP，在信息安全上升到国家战略高度的大背景下，SAP 本地化的安全解决方案必定有广阔的应用空间。

6. 企业分工

下表列出方案实施过程中所涉及的产品信息：

编号	产品清单	用途	提供者	备注

1	SAP 密码安全中间件	实现SAP系统应用安全	北京三未信安科技发展有限公司	
2	SJJ1012-A 服务器密码机	提供密钥保护及密码运算	北京三未信安科技发展有限公司	支持用户已采购的其他厂商密码机
3	SJK1864-G 智能密码钥匙	终端密码运算与证书介质	北京三未信安科技发展有限公司	支持已采购友商智能密码钥匙

7. 应用案例

国内某能源企业为了进一步提升 SAP 的安全防护水平，保障其 ERP 系统的安全自主可控，该企业在“重要信息系统安全提升项目”中，特别提出使用 SAP 安全中间件产品。在本次应用中，SAP 密码中间件覆盖 ERP 大集中系统五大核心板块共计 8000 用户，客户端统一使用 USBKey+中间件实现 SAP 安全登录，后台采用密码机+中间件实现对客户端登录验证和数据传输的加解密功能。

北京三未信安科技发展有限公司

联系人：张玉涛

电　话：15315551558

010-59785977

身份证云认证密码应用解决方案

1. 概述

为满足越来越多移动场景中的身份证实名制认证需求，天地融基于互联网云技术，遵循国家密码管理局颁布的《GM/T0003-2012 SM2 椭圆曲线公钥密码算法》等密码行业标准，自主设计了一款基于 PKI 密钥体系和国产安全芯片的 SRT1608 互联网身份证云认证平台，在联网的读卡终端（SRJ1605、SRJ1710 等）配合下，可以进行安全的身份证核验操作，能够满足安全检查、共享租赁等多种场景中实名制身份认证的需求，支持 SM1、SM2、SM3、SM4 密码算法。

2. 需求分析

当前越来越多的场景要求出示身份证进行实名制验证，包括快递收揽的实名制查验、乘客的身份抽查、单位上的访客登记等。与业务系统联通的居民身份证核验机具一旦遗失，可能会成为攻击者侵入业务系统的起点，为此，多个行业分别制定了自己的机具使用规定，将设备管理提升到了非常重要高度。

天地融设计的互联网身份证云认证系统，通过读卡器中的安全芯片与云认证平台间建立的安全管道对传输内容进行加密保护，不仅能够保证传输信息安全，而且可以保证接入服务的管控，在对身份证信息安全保护的同时实现了对业务系统的安全保护，能够对系统接入进行安全管控，有效防止各类攻击。

3. 方案架构

3.1 技术架构

图 3-1 身份证云认证系统架构示意图

互联网身份证云认证系统主要由身份证核验终端和云服务平台两部分组成，一个云服务平台可以支持多个身份证核验终端的互联网接入。身份证核验终端负责业务一线的身份证读取核验，获取相关信息通过安全管道上送云服务平台。云服务对身份证信息进行业务处理，比如实名取票时的票务对应性核验等。

3.2 产品部署图

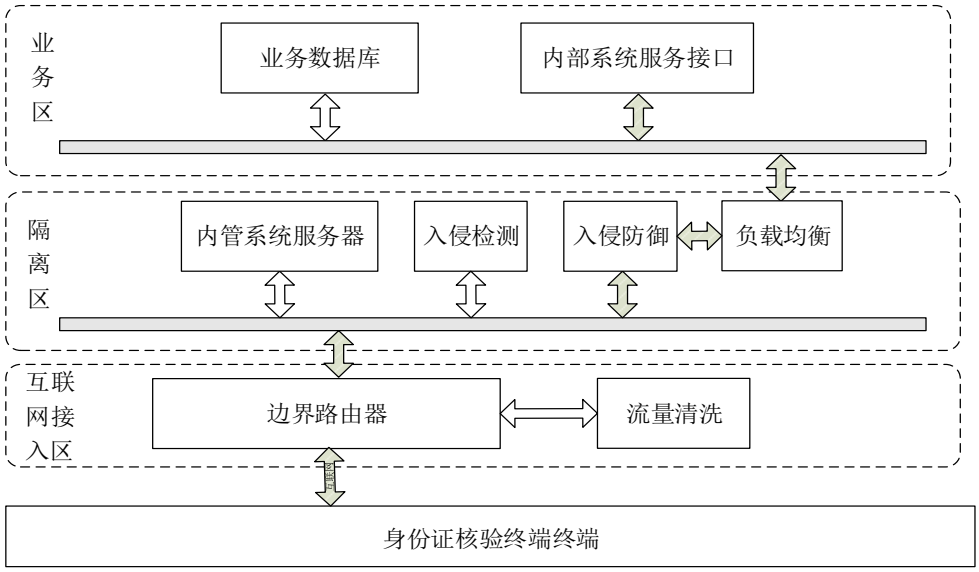


图 3-2 身份证云认证系统部署示意图

身份证核验终端既可以是一个独立设备，也可以与其他业务终端集成，形成业务场景灵活部署。后台数据库、内部系统服务接口等重要数据和接口受到统一的安全分层保护，保证业务的安全运行。

3.3 主要功能

居民身份证核验

支持二代居民身份证核验，可广泛用于快递实名、银行开户、访客登记、地铁安检等领域。进一步的，通过人脸识别功能，将身份证的照片与现场实时采集照片的比对，可以实现证件与人的一致性核验，避免身份证冒用的情况。

数据后台统一处理

业务上使用的身份证数据由云认证平台统一提供。在实现公民信息保护的同时，有利于业务的统一规划、大数据分析、风险控制等实施，包括黑名单人员提示、关注人员实时上报等。

身份证核验服务集成

主要业务服务接口集中部署在云认证平台，由云认证平台统一对外提供身份证信息服务。

3.4 主要技术指标

序号	项目	指标
1	并发服务数量	支持百万级
2	系统管理	支持不同角色权限配置
3	服务管理	不同场景差异化返回信息
4	系统服务对接	向其他系统提供对接服务
5	信息安全	敏感信息加密

4. 方案特色

规范合法

身份证云认证方案是以第二代居民身份证的认证体系作为信任基础，通过对第二代居民身份证内信息的读取、认证，完成实名认证。

保护隐私

采用国密算法和通过国家主管部门审核的高安全的安全方案，对用户个人的隐私信息进行加密保护，确保不会泄露，让用户使用起来更加放心。

操作规范

操作简便，对终端设备要求低，易推广和监管，便于规范市场实名认证操作。

便携高效

身份认云认证方案的系统架构，减轻了前端用户设备安全管控的负担，并结合“互联网+”，实现了高效身份证核验。

5. 适用领域

面向各类基于居民身份证的实名核验场景，适合身份证核验终端大规模批量部署，以及身份证核验终端与各类设备集成，如快递实名、公共交通安全检查及。

6. 企业分工

天地融身份证云认证平台为天地融自主研发设计实施。天地融提供全套的身份证核验终端和云服务平台，并提供完整的业务解决方案定制服务。云认证平台支持多种国产服务器上的部署，实现安全可控。

7. 应用案例

身份证云认证系统已在多个重要场景中完成应用部署，举例如下：

公共交通实名核查

北京市公安局公共交通安全保卫总队使用身份证云认证身份核验解决方案，为执勤民警和协警配备了人手一个的身份证核验终端，在保障十九大期间的公共安全以及日常公共交通安全的同时，充分缓解了传统身份证信息核验造成的乘客流量压力。

快递实名核验

天地融身份证云认证技术协助珠海市公安局对快件寄递实名核验要求进行落地部署。用户在寄送快件时核验身份证进行身份信息确认，从源头上杜绝违规物品的寄递，信息不在终端留存，最大限度的保护了用户的身份信息安全。

天地融科技股份有限公司

联系人：程璐

电　话：18610599339

010-56675666

密码服务资源池密码应用解决方案

1. 概述

近年来，网络安全已上升到国家战略高度，密码技术作为网络安全重要的主动防护技术，在国家信息化进程中也得到了更多的应用和发展。随着应用业务的多样化以及基于云计算的基础设施建设不断完善，对密码技术的应用方式也提出了更多的要求，传统的直接集成密码设备的方式也面临着各种问题。

2. 需求分析

传统的基于各种密码设备的集成方式，在应用业务多样化的环境下，很难灵活的适应业务需求变化带来的密码应用新需求，同时传统的硬件密码设备在云环境中部署具有一定障碍，很难满足云计算环境下弹性部署、动态调配密码资源的需求。并且传统密码设备集成中，应用开发商专业程度不同，应用密钥管理和使用分散，导致应用集成密码开发及用户的运维成本急剧上升，更增加了系统安全风险，亟需为用户整合密码资源，提供统一的密码资源管理与统一的密码服务接入规范，为应用业务提供更规范、更专业、更高效的密码技术支撑。

3. 方案架构

密码服务资源池的设计与开发遵循了国家商用密码相关标准及规范，支持SM1、SM2、SM3、SM4 等国密算法，同时也应用了虚拟化、Docker 等成熟技术来组织密码资源，满足弹性部署需求。

3.1 技术架构

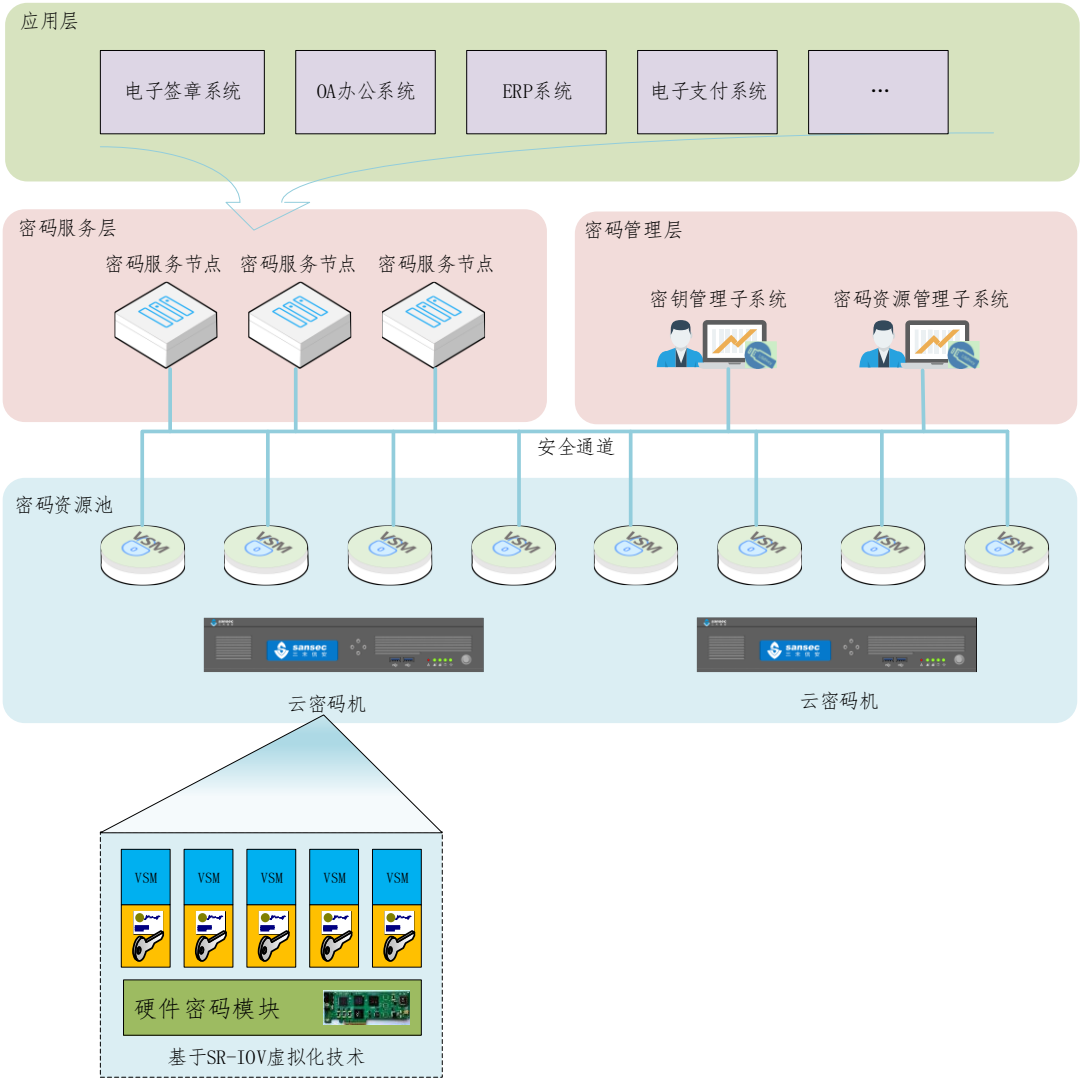


图 3-1 产品架构图

密码资源池属于密码基础设施，是利用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同时降低总体成本及提高服务资源利用率的目的。密码管理层是密码服务资源池的支撑与运维平台，其中密钥管理子系统为密码服务资源池提供密钥与证书的管理服务支撑，密码资源管理子系统负责密码服务资源池的运维保障。密码服务层是由密码服务 API 及密码应用代理等组成的密码服务资源池，可以基于密码资源为应用层提供丰富的密码服务功能。

3.2 产品部署图

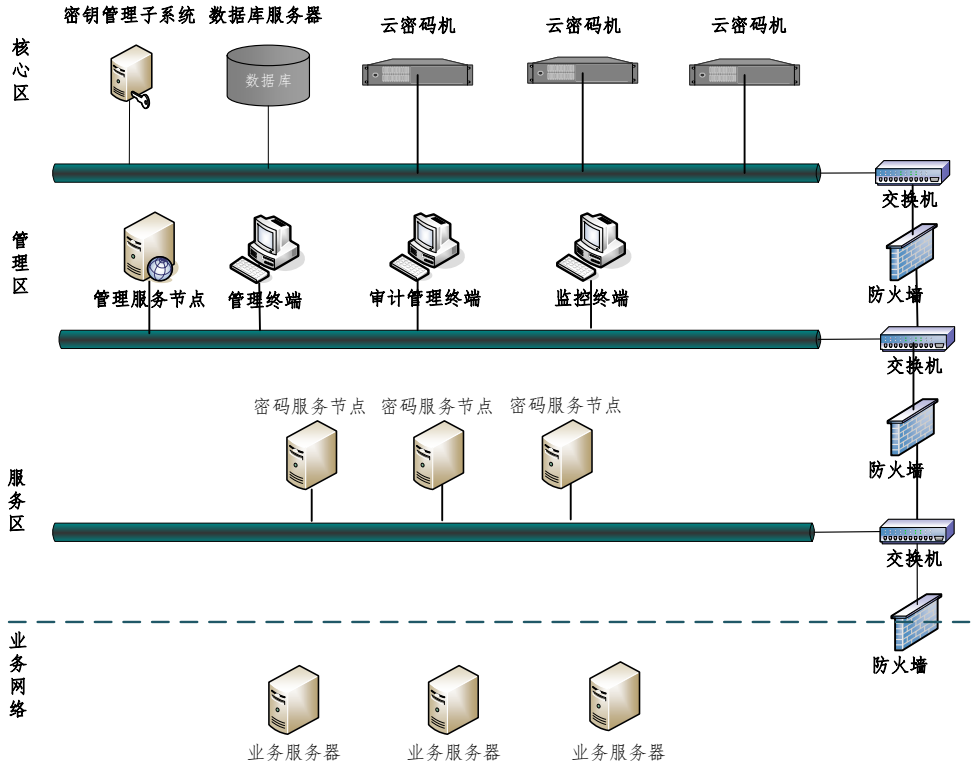


图 3-2 产品部署图

云密码机作为密码资源池载体与密钥管理子系统部署在核心区，密码资源管理子系统部署在管理区，服务节点部署在服务区，为业务网络的业务服务器提供密码服务。各区域之间采用 TLS 安全协议互联，保证通信的安全性。

密码服务节点服务接口在《GM/T0018-2014 密码设备应用接口规范》以及《GMT 0019-2012 通用密码服务接口规范》的基础上以 RPC 调用的形式进行了扩展和进一步的封装，在保证性能的前提下保证了对业务和监控的支撑能力。

用户业务访问密码资源池采用符合国密标准的 TLS 安全协议来保护通信的安全。业务请求在资源池内部处理时，密码服务节点会根据密钥属性配置和请求信息来判定对密钥的请求是否满足密钥权限，并拒绝非法请求。

3.3 主要功能

- 密码服务资源管理：将密码硬件资源虚拟化、池化，进行统一的管理与监控，降低运维成本。
- 密钥管理：提供集中密钥管理服务，为应用系统及密码资源提供密钥全生命

周期管理。

- 密码服务管理：为业务系统提供统一、规范的密码服务功能，降低应用开发成本，规范应用系统使用密码的安全性。
- 业务应用规划：系统可进行业务应用的规划，根据业务需要分配其所需的密码资源，支持应用认证策略和访问策略配置。
- 集中监控：系统支持对密码资源状态、密码服务状态进行实时监控，发现异常时可通过短信邮件等方式发送告警信息。

3.4 主要技术指标

密码服务节点在推荐配置（CPU: Intel Xeon E5-2670v3，内存：16G）上运行时，单节点最大并发数不低于 20000，服务热备切换时间小于 1s，平均业务转发延迟小于 15ms。具体密码运算指标如下：

- SM2 签名: 120,000 TPS
- SM2 验签：110,000 TPS
- SM1 加解密: 10Gbps
- SM3 加解密：14Gbps
- SM4 加解密：15Gbps

4. 方案特色

- 密码资源弹性调度：借鉴云计算基础设施的弹性计算概念，实现了密码资源的动态调度算法，密码资源分配自动可伸缩，保障业务系统可靠性的同时也实现了密码资源的优化分配。
- 以应用业务为核心进行密码资源的分配与管理：系统以用户业务为核心来组织自身的各项管理功能，可助力用户快速实现业务应用的密码集成规划部署。
- 智能化的统计分析机制：系统支持运行数据的智能统计分析功能，为智能运维提供数据支撑。

5. 适用领域

密码服务资源池方案是依据应用功能和业务场景云化应运而生的新型密码技术方案，可适用于任何使用传统密码设备的场景，特别适用于密码设备繁多、应用系统多样的传统业务场景，以及运行在云中的应用场景。

6. 企业分工

编号	产品清单	用途	提供者
1	SJJ1601 云服务器密码机	密码硬件资源载体	北京三未信安科技发展有限公司
2	密码服务资源池系统	实现密码资源池的统一管理和服务调度	北京三未信安科技发展有限公司

7. 应用案例

国内某政府行业用户已建设了密码服务资源池系统，密码服务资源池主要为用户提供了数据加解密服务、数据签名验证服务、密钥管理服务等功能，其中重点实现关键业务系统中敏感数据的加密保护，涉及数十个业务系统，数据规模约几千万条。密码服务资源池系统为该用户提供了高效的密码资源调度及密码计算功能，为用户各个应用系统的信息安全建设保驾护航。

北京三未信安科技发展有限公司

联系人：许永欣

电　话：18660805090

0531-88988936

基于“垂直认证”技术的保密通讯系统
密码应用解决方案

1. 概述

国际上所有保密手机，都是采用手机里内置加密芯片实现的，亦即：手机与加密芯片一起卖。即使用户已经有手机了，用户若想使用语音加密通话，必须再购买一部保密手机。另外，警察执法需要对执法现场的视频实时加密传输给指挥部，必须购买专门的警务手机。

现在的加密技术通常采用公钥基础设施(PKI)，它可以保障数据交换过程的安全，但是设置与管理 PKI 都很费时费力。手机网络电话需要针对移动终端的运行环境，进行保密通讯协议设计。本解决方案有效的解决了 PKI 构架中的问题，通过在移动通信终端中使用对称加密方式和拥有专利的密钥一次一变技术，不需要非对称加密方式和证书文件，有效提高了加解密速度，同时避免了公钥的存储、管理等问题，也不会发生证书被窃取和篡改的危险。

2. 需求分析

2013 年斯诺登事件引起国内外重大关注。曾经在国家安全局办公室工作的爱德华·斯诺登将一些文件复制后交给媒体将文件公开。国家安全局在 PRISM 计划中可以获得的数据电子邮件、视频和语音交谈、影片、照片、VoIP 交谈内容、档案传输、登入通知，以及社交网络细节。

美国情报机构直接进入美国网际网路公司的中心服务器里挖掘数据、收集情报，从音频、视频、图片、邮件、文档以及连接信息中分析个人的联系方式与行动，包括微软、雅虎、谷歌、苹果等在内的 9 家国际网络巨头皆参与其中。美国惊人规模的海外监听计划覆盖范围广，从欧洲到拉美，从传统盟友到合作伙伴，从国家元首通话到日常会议记录，引发美国外交地震。

手机作为个人日常使用的通信终端，其安全性的重要程度不言而喻，针对前文提到的信息泄露和窃取，更需要做好防护。保密通信系统正是为解决电话、邮

件信息等安全传输防护问题而设计的安全系统。

3. 方案架构

采用对称密码算法建立认证架构，以及网络身份认证、数字签名和数据加密协议，认证架构简单。采用对称密码算法（如：SM1、SM4），可完成身份认证、数字签名、密钥交换和数据加密等 4 种功能；“垂直认证”技术是采用组合密钥生成算法（CSK，companed single key），解决对称密码算法密钥管理的难题，可实现认证密钥、签名密钥、加密密钥和交换密码的密钥等 4 种密钥都一次一变。对比国际上现有 PKI 技术有安全性高、速度快、管理用户量大、建设和维护成本低等 5 大优势。在手机里部署一块加密芯片和一个 APP，在加密芯片里，写入语音加密协议，一部手机就可以变成一部保密手机。

《保密通讯系统》是基于对称密码算法、组合密钥生成算法和安全芯片技术的移动安全产品，用于双方用户之间通话的语音数据加密，保证网络 IP 电话语音数据的加密传输。

3.1 技术架构

《保密通讯系统》由用户端安全系统和服务器端安全系统两部分组成，如图所示。

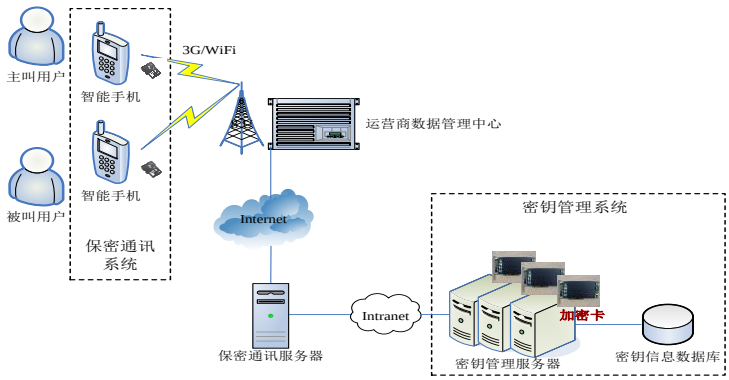


图 3-1 技术架构图

3.2 产品部署图

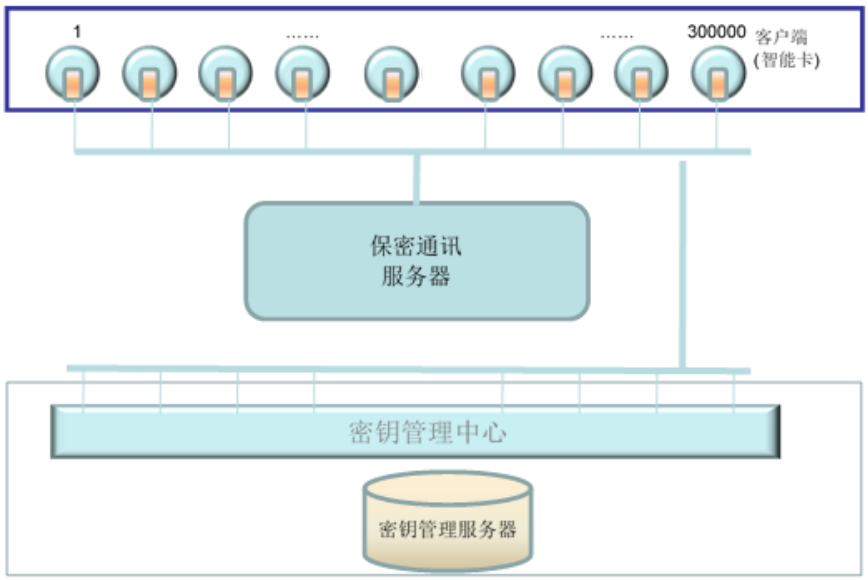


图 3-2 产品部署示意图

移动用户的智能卡分配给每个保密通讯用户，智能卡芯片中灌有用户密钥种子。通过客户端连接智能卡调用安全协议来实现保密通讯操作，实现保密通讯过程密钥生成、加解密和语音数据加解密功能。

保密通讯服务器是保密通讯主叫用户和被叫用户之间沟通的桥梁，负责在主叫用户和被叫用户之间将保密通讯用户的保密通讯过程密钥密文和语音数据密文进行转发，从而实现保密通讯。

密钥管理服务器端配备加密卡硬件设备，在密钥初始化、密钥分发和保密通讯过程密钥交换阶段对保密通讯用户的密钥进行分发管理和保密通讯过程密钥交换，用于实现对用户密钥种子的生成、加密存储、分发和保密通讯过程密钥交换。

3.3 主要功能

《保密通讯系统》主要功能是加密通话双方用户的语音数据，保证语音数据在传输过程中的保密性，由保密通讯用户端模块、保密通讯服务器端模块以及密钥管理服务器端三部分组成。

其中密钥管理服务器配备加密卡。移动终端的智能卡插入移动终端卡槽中，

保密通讯用户在进行保密通讯时，需要生成过程密钥和加密密钥，保护语音数据和过程密钥的安全性。

3.4 主要技术指标

我们的“垂直认证”技术产品，经过第三方权威部门的检测报告：可管理用户规模达 3 亿，并发认证：1228.50 次/秒，并发签验：823.93 次/秒。“垂直认证”技术的技术性能，远远超过 2020 年国家该领域的技术指标，并发认证对比国家 2020 年科研重大项目指标，快千倍。

过程密钥和交换过程密钥的用户密钥等 2 种密钥都一次一变。密钥交换速度超快达到 0.03 秒，同时，不影响手机（明文）网络电话的正常通话体验。

4. 方案特色

1、架构和协议安全性高，垂直认证技术是认证/签名和加密协议在芯片里运行，认证/签名和加密密钥一次一变。

2、运行速度超快，采用单钥（对称）密码算法建立认证/签名和加密协议。

3、认证中心管理用户量大，采用少量标识和密钥种子，建立的（单一）认证中心管理用户量大（单座认证中心做过 3 亿用户的检测，这是国际上首例）。

4、认证中心的建设和维护成本低。对比第三方认证技术，如：PKI 或 IBE，可降低建设成本 85%。减少维护人员 85%以上。

5、产品获得了业内顶尖专家的支持和书面推荐，认证和签名技术已经获得国家密码管理局颁发的商用密码产品证书。

5. 适用领域

保密通讯系统的应用，可以保障手机网络电话通讯过程中语音信息的保密性，避免保密信息或敏感信息泄露，保护用户隐私。本产品适用于需要保护客户隐私和秘密的行业，可供需要加强通讯信息保护的企业用户或个人用户使用，潜在市场空间大，预期经济效益显著

6. 企业分工

北京金奥博数码信息技术有限责任公司负责全部系统建设工作。

产品为“SJT1601 加密通话系统”

7. 应用案例

与手机厂商合作，推广我们的“垂直认证”芯片、认证/签名一体机和密钥管理机设备，以及软件安全系统：⑴用于保密通信系统，⑵用于高端移动支付系统。

北京金奥博数码信息技术有限责任公司

联系人：郭建伟

电　话：13910317685

数据中心高速加密交换系统应用方案

1. 概述

本项目采用 GDOI 协议实现组密钥管理，研发高性能加密模组，在用户原有核心交换机产品基础上实现国密算法加密交换功能，满足企业用户应用环境、技术特点及安全需求，实现自主可控

2. 需求分析

大型企业核心网络以核心、汇聚、接入三层结构为主，在数据传输环节，从接入层到汇聚层到核心层之间虽采用了专线连接，但由于数据以明文方式传输，网络安全威胁来源广泛、形式复杂，一旦恶意人员能够访问到专线链路，数据可以被任意的截取、重组，还原出原始的数据信息，给企业构成严重威胁，危害国家关键基础设施安全。

- 根据国家等级保护及行业安全政策的合规性要求，需要采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性以及数据的完整性；
- 采用密码技术对通信双方进行身份认证，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；
- 采用密钥管理系统实现对密钥的生成、存储、分发、导入、导出、使用、备份 、恢复、归档 、销毁等环节的集中管理和密钥策略制定，通过以上安全防护措施保障数据安全性。

3. 方案架构

该项目核心加密组件由高速加密模块及 GDOI 密钥管理系统组成，主要采用国密标准的 SM2、SM3 以及 SM4 算法作为加密套件，高速加密模块采用可编程逻辑部件技术实现，双向加解密性高达 40Gbps；GDOI 密钥管理系统采用 GDOI

协议创建分组密钥管理模型，将业务加密密钥及加密策略采用集中分发模式进行管理。

3.1 技术架构

3.1.1 加密模块

整个加密模块分左右两个独立的通道，每个通道可以处理 20Gbps 的业务数据。每个通道提供独立的业务接口、管理接口和认证接口；同时两个通道共用一个配置接口。加密模块实物图如下：

加密模块的物理接口包括：业务物理接口、管理物理接口、用户身份认证 USB 接口、配置物理接口、数据处理单元、以太网 PHY、数据缓存 SRAM、安全芯片、扩展模块等接口，硬件接口设计如下图所示：

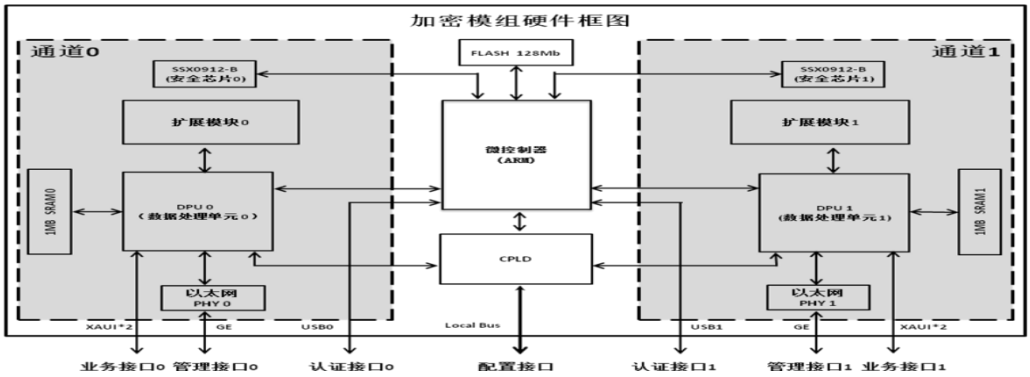


图 3-1 技术架构图

3.1.2 GDOI 密钥管理系统

GDOI 密钥管理系统基于 RFC6407 标准架构（管理和控制）和 IPSec ESP 标准封装（数据转发），采用组加密技术，通过简单高效的组秘钥管理机制支持任意节点间的加密通讯，具有大规模可扩展性，降低运维成本，不依赖隧道的加密技术，仅对报文内容加密，对加密节点之外的网络透明，不改变网络架构，适应已有拓扑。在标准框架内用国密算法替换通用加密算法，满足更高安全需求。

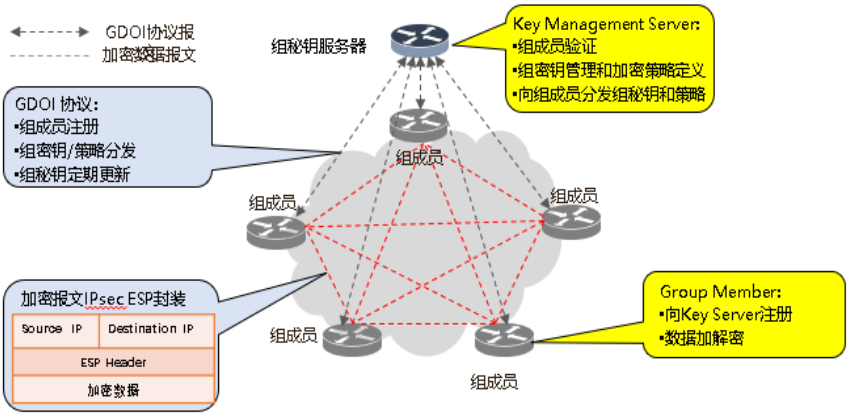


图 3-2 框架图

3.2 产品部署图

数据中心高速加密交换系统由配置在网管中心的 GDOI 密钥管理系统和配置在广域网网关位置的加密交换机组成。其中，GDOI 密钥管理系统为密钥管理系统和策略管理中心。加密交换机主要加解密数据，完成与 GDOI 密钥管理系统的身份认证、密钥协商、策略下发、密钥下发以及数据的协议解析、策略查询等功能。部署逻辑如下：

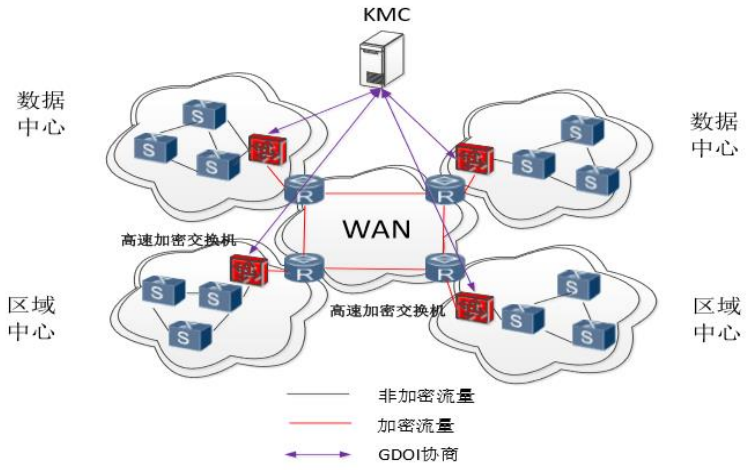


图 3-3 产品部署

3.3 主要功能

高速加密计算功能、用户访问权限控制、密钥管理功能、组策略处理、GDOI 协议处理、日志采集与状态检测。

3.4 主要技术指标

3.4.1 数据中心高速加密交换系统（整体）

- 支持算法。国密标准算法 SM2、SM3、SM4；业务数据加密算法 SM4，ESP 隧道模式实现；存储保护加密算法 SM4；密钥分发加密算法 SM2、SM3 和 SM4。身份认证加密算法：SM2 和 SM3。
- 性能。SM4 加解密速率≤40Gbps；数据转发速率为 16-64Gbps；SM2 密钥对生成：≤59 对/秒；SM3 杂凑算法：≤40Gbps。
- 接口。XAUI 数据通道：4 个，其中 2 个为加密通道、2 个为解密通道，4 个 XAUI 通道之间相互独立。每个 XAUI 接口总线带宽为 12.5Gbps，可以提供 10Gbps 业务数据的传输。GE 接口：2 个，提供对加密模块的控制，例如下发 TEK 密钥，进行对称密钥数据计算等。USB 口：2 个，实现密钥注入功能。LBUS 接口：1 组，加密模块初始化阶段，对模组内 FPGA、CPU 等硬件大包进行加载。
- 设备管理接口。千兆网口，用于交换机配置、网管接口、密管接口；串口，用于命令行 Console 接口、Console 接口。
- 组策略数：≥10000 条，每个组的成员数： ≥1000 个；密码设备数：≥256 个；KMC 生产存储保护密钥时间≤2，KMC 生产公私钥对时间≤2ms。

3.4.2 GDOI 密钥管理系统

- 产品规格指标。支持接入设备最大数量 2048 台；支持最大分组数量 1024 个；单个分组最大支持 1024 个组成员；最大策略条数 10240 条；最大注册并发数 200 条；每秒新建连接数 64 条；密钥更新周期最小 30 分钟，最大 24 小时；支持 SM2、SM3 及 SM4 算法。
- 工作条件。组策略数≥10000 条，每个组的成员数≥1000 个密码设备数≥256 个，MC 生产存储保护密钥时间≤2，KMC 生产公私钥对时间≤2ms。
- 工作环境。额定工作电压：220V±15% 50~60HZ；工作环境温度：0-40℃；工作环境相对湿度：10-95% 非凝结；存储环境温度：-10-40℃；存储环境相对湿度：10-95% 非凝结。

- 可靠性指标：平均无故障时间：≥20000 小时。

3.4.3 高速加密模组技术规格指标。

外形尺寸：240x167x20（长 x 宽 x 高）mm；性能指标：SM3，SM4 运算速度 40Gbps；签名 150 次/秒（256bit）；总线形式：XAUI，GE，Local Bus，USB；工作电源：+12V；工作温度：0－45 摄氏度；湿度：<90％。

4. 方案特色

- 应用理念创新设计。将交换设备与加密模块跨界融合，在用户原有核心交换机产品上实现基于国密算法的加解密功能。
- 超高性能算法实现。高性能可编程逻辑器件（FPGA）实现了自主知识产权的高效加解密，双向加解密性能高达 40Gbps。
- 密码算法等效替换。实现 GDOI 协议国产化，国密算法替换原有国际算法，实现了商用密码在核心技术上的等效替换、平滑过渡。
- 全新信任组成员密钥管理机制。采用高效的 GDOI 组密钥管理机制支持任意节点间的加密通讯，具有大规模可扩展性。
- 现有网络平滑接入。实现与现网设备的平滑接入，对原有的系统使用模式、组网方式不需做任何改变，保护已有投资，加密策略灵活定制，满足不同业务系统数据加密需求。

5. 适用领域

- 数据机密性及完整性保护要求较高的场景；
- 多个数据中心、数据中心内部不同机房之间的数据安全交换；
- 其它有高速交换和加密交换需求的场合；
- 高速加密模组原生支持华为的业务主板。
- 定制主板，高速加密模组可定制应用。

6. 应用案例

该方案目前已在某能源集团公司部署应用，在其信息系统中，一套有保障的网络基础设施是所有信息系统运行的基础。

目前本项目包括的高速加密模组、GDOI 密钥管理系统等产品已在该能源集团公司广域网，即 4 个集团级数据中心、区域中心和部分二级单位的主干网络中部署，共涉及 158 个节点实施部署，包括其下属局级单位，高速加密模组直接插入现有核心交换设备中，无需网络结构变化，通过 5 元组的加密策略灵活适用各种业务应用，有力的保证骨干网络节点之间的数据传输加密，为该能源公司网络基础设施建立安全保障，发挥国产密码在保护能源行业网络与信息安全中的重要支撑作用，切实增强自主可控能力。

北京数盾信息科技有限公司

联系人：姜沛君　　卢效伟

电　话：15901299719　13601194778

010-66008006　010-66008006

移动智能终端密码应用解决方案

1. 概述

移动智能终端在高安全、大额度的交易应用需求中，必须采用数字签名、加密等措施，保护交易的安全性。一般性应用中，最低应该采用密码模块（提供数字签名、加密等功能）方式，目前密码模块遵循的主要标准是《密码模块技术要求》和《密码模块检测要求》，这两个标准是为硬件密码模块（加密卡、USBKEY）量身打造的。

2. 需求分析

移动互联网发展越来越快，人们对于手机软件的认知和使用已经成熟，越来越多的人每天都在过着以手机为中心的生活，智能手机早已取代电脑，成为人们日常使用频率最高的产品。

在移动端，蓝牙盾、音频盾等硬件密码模块能够为用户交易提供安全保护，但是也存在携带不方便的问题。基于手机 TEE 和 SE 的移动终端密码解决方案-手机盾产品采用国产密码算法，在移动智能终端上利用 TEE 和 SE 进行“空中下证”，部署环境，完成移动互联网安全认证，而且携带方便、安装快捷、使用简单。可应用于金融交易、电子商务、电子政务、企业信息化、网游、网上报税、网上招投标等领域。

3. 设计方案

移动终端密码解决方案-手机盾产品由运行在开放操作系统（Android）中的客户端 SDK 与运行在可信执行环境（TEE）中的可信应用（TA）、安全芯片（SE）中 Applet 和后台系统组成。如下图所示：

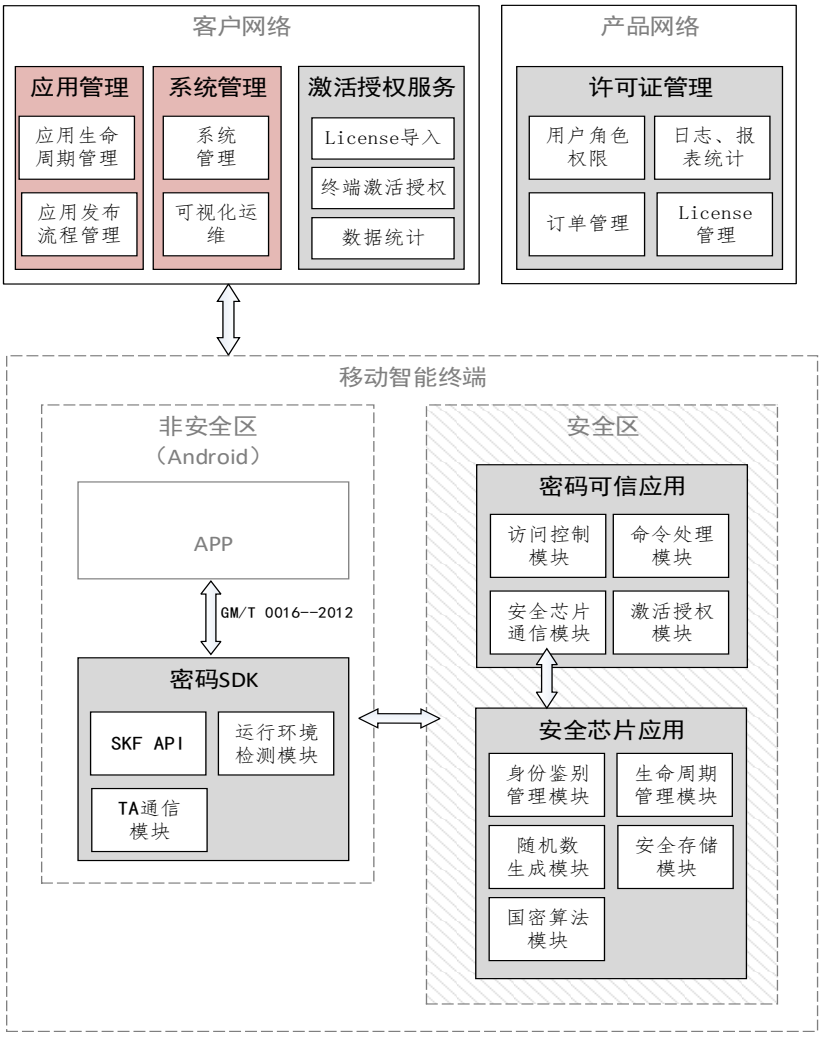


图 3-1 架构图

客户端应用（Client App）

客户端应用运行在开放操作系统 Android 上，通过调用密码模块的客户端 SDK 提供的 APDU API，向密码模块发送 GM/T 0017—2012《智能密码钥匙密码应用接口数据格式规范》中规定的命令 APDU 和接收响应 APDU，以执行核准的密码功能。

客户端 SDK

客户端 SDK 运行在开放操作系统 Android 上，通过调用 GP TEE 规范中的 TEE Client API 与 TEE 环境中的 TA 进行指令和数据交互。

可信执行环境（TEE）

TEE 是驻留在移动智能终端的主处理器上的安全区域，提供与设备上的 Rich OS（例如 Android）并存的运行环境，并且向 Rich OS 提供例如敏感数据的安全存储、核准的密码算法、可信用户界面等安全服务。TEE 为 TA（Trusted Application 可信应用）提供

了安全执行环境：它同时提供保密性和数据完整性保护，对 TA 访问资源和数据提供访问权限控制，隔离多个 TA 之间的运行环境和敏感数据。为保证 TEE 有可信的信任根，在安全启动过程中，TEE 首先被鉴权，然后从 Rich OS 中隔离出来。

可信应用（TA）

密码模块 TA 运行在 TEE 可信执行环境中，TA 通过 GP TEE 规范中的 TEE Internal API 来获取安全资源和安全服务的访问权限。TA 接收来自客户端应用的命令 APDU，并按照 GM/T 0017—2012 中规定的 APDU 功能执行核准的密码功能，并返回响应 APDU。

安全芯片（SE）

TA 涉及密钥相关功能均在 SE 中实现，主要功能模块包括指令处理模块、角色鉴别模块、安全存储模块、随机数生成模块和国密算法模块。

后台服务

后台系统实现对安全芯片中应用进行管理，提供计费及计费统计功能，可以对系统运行情况进行记录、统计，并可以实现可视化运维。

4. 方案特色

采用国密算法

实现了 SM2 非对称密码算法，SM3 密码杂凑算法，SM4 对称密码算法。

遵循国密规范标准接口

在移动智能终端上实现了 GM/T 0016—2012《智能密码钥匙密码应用接口规范》、GM/T 0017—2012《智能密码钥匙密码应用接口数据格式规范》。

TEE TA 保证用户输入输出信息安全

TEE 为 TA（Trusted Application 可信应用）提供了安全执行环境：它同时提供保密性和数据完整性保护，对 TA 访问资源和数据提供访问权限控制，隔离多个 TA 之间的运行环境和敏感数据。为保证 TEE 有可信的信任根，在安全启动过程中，TEE 首先被鉴权，然后从 Rich OS 中隔离出来。

SE 存储和管理密钥和敏感信息

在 SE 中部署 Applet 应用，实现密钥生命周期管理，包括密钥的产生、使用以及销

毁，同时，可以对敏感数据进行存储。

降低成本

用户手机为认证载体，降低客户成本，空中制证，减少客户工作量，减少用户排队时间成本和交通成本。

5. 相关产品

手机盾 WatchKeyOCL_MTS:应用于金融领域

警务通手机盾：应用于公安领域

性能参数：

编号	功能模块	说明
1	安装 applet	安装 applet 平均时间小于 10s
2	下载证书	下载证书平均时间小于 5s
3	生成密钥对（SM2）	小于 200ms
4	签名 1k	签名次数大于 8 次/秒
5	签名 10k	签名次数大于 6 次/秒
6	报文最大长度	512K

6. 应用案例

金融：

建设银行手机盾项目

中国银行手机盾项目

政企：

新疆公安厅警务通空中下证项目

江西公安厅警务通空中下证项目

公安一所警务通空中下证项目

公安三所警务通空中下证项目

北京握奇智能科技有限公司

联系人：鲁洪成

电　话：18001226283

010-64722288