网安联
Wang An Lian

誠天信威
iTrusChina

抗“疫”有情，网安联信创生态在线沙龙伴你行！

抗“疫”公益系列活动之十七（二）

天威诚信
统一密码服务平台建设方案

构建信任 · 传递信任

目录

CONTENTS

01

第一部分

应用背景

国家密码相关政策发展

2011年

国密局在《关于做好公钥密码算法升级工作的函》中要求2011 年7 月1 日以后建立并使用公钥密码的信息系统应使用SM2算法，已经建设2完成的系统，应尽快进行系统升级，使用SM2算法。

2015年

2014年底，国家密码管理局启动《重要信息系统密码应用推进总体研究课题》，确定十三五密码科技专项

2018年

等保2.0《信息安全技术 网络安全等 级保护基本要求》，适应新技术（安 全通用要求、物联网、云计算安全扩 展要求、移动互联安全扩展要求、物 联网安全扩展要求和工业控制系统安 全扩展要求）

2020年

2020年1月1日起施行《密码法》问责制：对有关国家机关、单位的密码工作进行指导和监督。密码管理部门依法履行监管职责，有关组织和个人应当配合。密码管理部门依法组织开展密码应用密码安全监督检查和执法，统一组织开展密码失泄密案件调查。

需求背景

市场需要标准规范化的统一密码管理手段

管理复杂

多厂商、多类型的密码设备，通常管理方式不尽相同，带来复杂的管理方式

密码资源使用率低

密码设备按应用系统去配备，应用系统独占其密码运算资源，容易造成设备利用率低、密码资源浪费等问题。

运维复杂

密码设备分散到各应用系统中使用，随着应用系统数量增多，设备数量增加，运维难度急剧提升。

安全性风险

缺乏统一的密码应用接口和管理标准，各应用系统开发人员安全专业程度不同，在使用密码设备时有安全性风险。

02

第二部分

解决方案

方案思路

- 统一商用密码服务平台的设计结合密码技术与“云”思维，通过对称密码算法、非对称密码算法、数字证书、电子签章、时间戳的综合应用，为业务系统统一提供身份认证、密钥管理、密码运算等密码服务，能够进一步有力支撑海量终端的接入与弹性安全边界的重构。

统一商用密码服务平台

1

拓展力强

利用“云”响应速度快、横向拓展力强、资源丰富的优势，构筑超高并发海量数据 的高速处理平台

2

动态伸缩架构

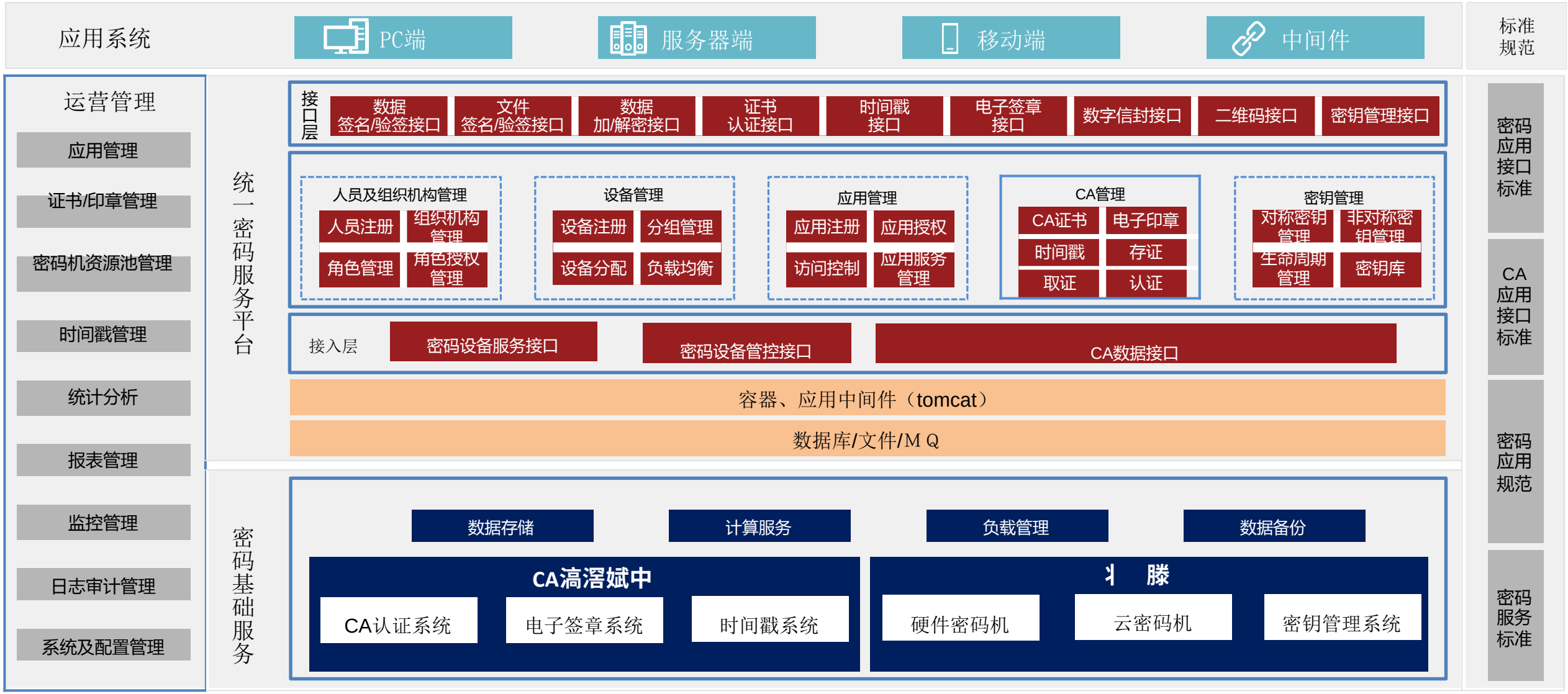
为实现密码资源根据 业务流量动态分配、 按需调整，以云部署 模式为基本框架，设 计了基于“容器”编 排的动态伸缩平台架 构。

3

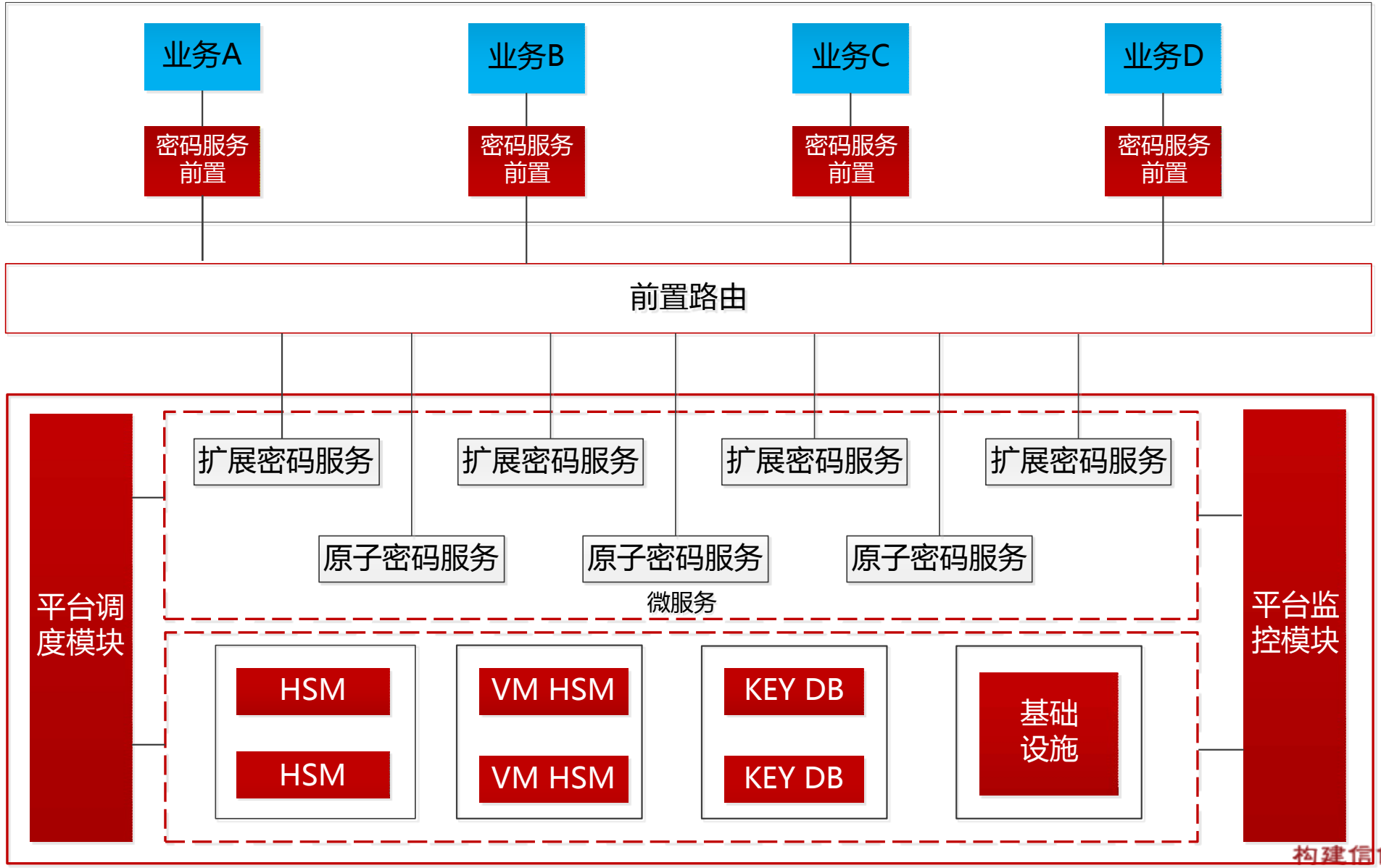
软硬协调

部署上充分利旧存量 硬件密码机， 设计软 硬协同调度策略。

系统总体架构


应用系统
PC端
服务器端
移动端
中间件
标准规范
运营管理
应用管理
证书/印章管理
密码机资源池管理
时间戳管理
统计分析
报表管理
监控管理
日志审计管理
系统及配置管理
统一密码服务平台
接口层
数据签名/验签接口
文件签名/验签接口
数据加/解密接口
证书认证接口
时间戳接口
电子签章接口
数字信封接口
二维码接口
密钥管理接口
人员及组织机构管理
人员注册
组织机构管理
角色管理
角色授权管理
设备管理
设备注册
分组管理
设备分配
负载均衡
应用管理
应用注册
应用授权
访问控制
应用服务管理
CA管理
CA证书
电子印章
时间戳
存证
取证
认证
密钥管理
对称密钥管理
非对称密钥管理
生命周期管理
密钥库
接入层
密码设备服务接口
密码设备管控接口
CA数据接口
容器、应用中间件（tomcat）
数据库/文件/M Q
密码基础服务
数据存储
计算服务
负载管理
数据备份
CA滴滔斌中
CA认证系统
电子签章系统
时间戳系统
滕
硬件密码机
云密码机
密钥管理系统
密码应用接口标准
CA应用接口标准
密码应用规范
密码服务标准

逻辑架构


业务A
业务B
业务C
业务D
密码服务前置
密码服务前置
密码服务前置
密码服务前置
前置路由
平台调度模块
扩展密码服务
扩展密码服务
扩展密码服务
扩展密码服务
原子密码服务
原子密码服务
原子密码服务
微服务
HSM
HSM
VM HSM
VM HSM
KEY DB
KEY DB
基础设施
平台监控模块

功能说明

运营管理	密码接口服务	密码服务应用	CA和密钥管理	运维监控管理

运营管理：

运营管理模块主要提供租户管理和平台配置管理功能。

租户管理包括：用户创建、密码资源分配及资源使用情况的统计分析功能。

配置管理包括：平台资源池配置、策略定义管理、服务管理。

- 用户管理
- 服务管理
- 密码机资源池管理
- CA资源
- 统计分析
- 报表管理
- 运营监控管理
- 日志审计
- 系统配置管理

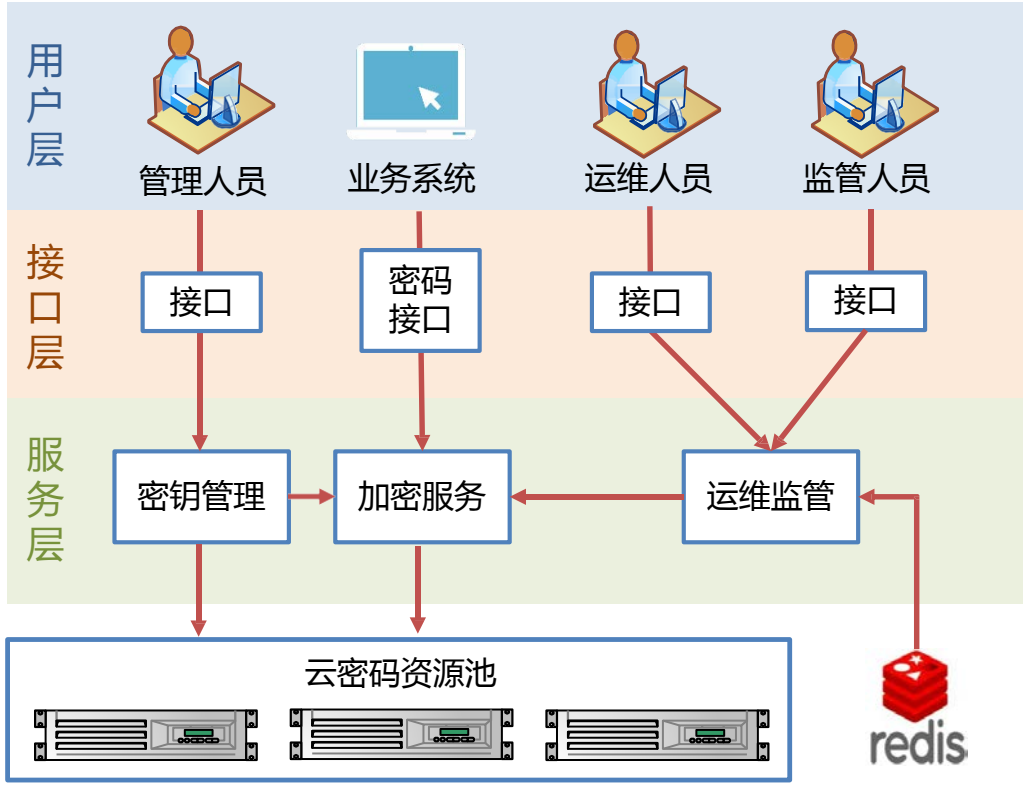
功能说明

运营管理	接口服务	应用管理	CA和密钥管理	运维监控管理

接口服务：

密码接口服务向授权的密码服务平台租户提供各类CA相关和应用密码运算服务，支持国密算法、国际算法。

- 数据签名验签接口
- 文件签名验签接口
- 数字信封接口
- 数据加解密接口
- 证书/签章接口
- 时间戳接口
- 文件完整性接口
- 二维码生成
- 二维码签名验签

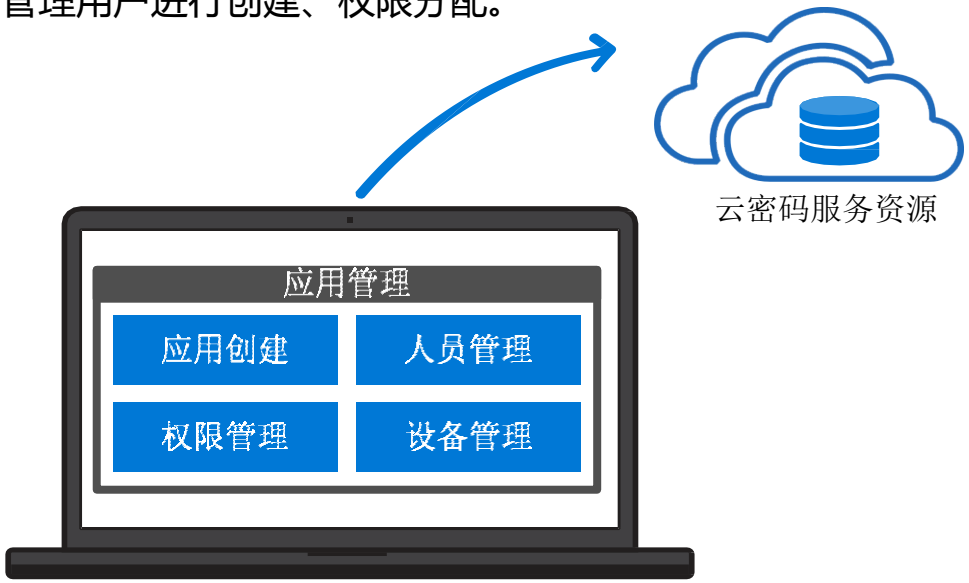


功能说明

运营管理	密码接口服务	**应用管理**	CA和密钥管理	运维监控管理

应用管理：

业务系统向密码安全管理子系统获得租户授权，完成该租户的应用创建、应用策略配置，并根据平台分配给租户的密码设备资源进行自行分配、配置管理。同时，针对该租户内的管理用户进行创建、权限分配。



- **应用创建**
- **人员管理**
- **权限管理**
- **设备管理**

密钥设备分配 + 应用策略配置 + 应用服务配置 = 业务调用

功能说明

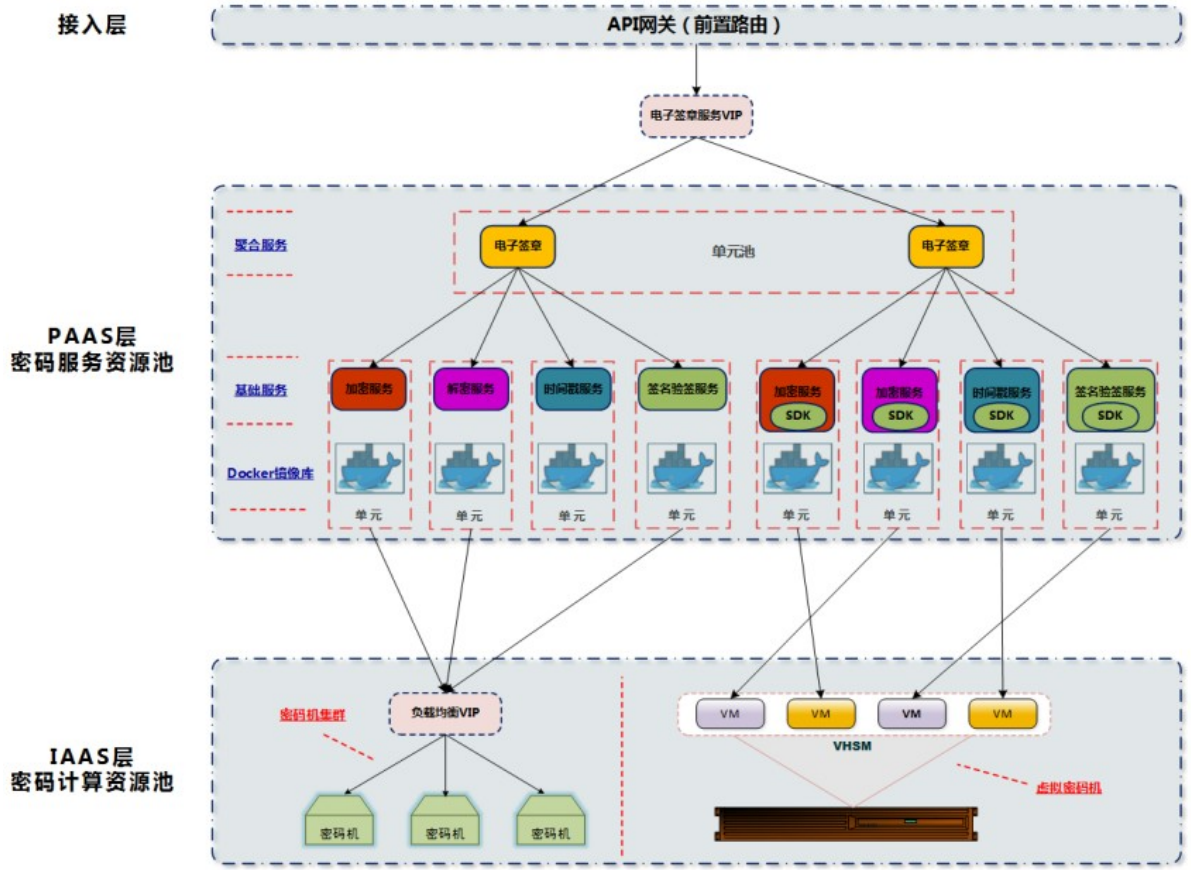
运营管理	密码接口服务	应用管理	CA和密钥管理	运维监控管理

密钥管理：

密钥管理支持包括对称密钥、非对称密钥、电子签章、数字签名、数字证书和认证令牌等多种加密对象的管理，参照密钥管理互操作协议（KM完成从密钥生成到密钥销毁的全生命周期管理，为用户提供一致性的密钥管理策略，易于配置和管理，减少密钥管理的维护成本，满足租户模式的密钥管理需求。

能力

- 适合云集中密钥管理特点
- 适合云的跨系统密钥交互
- 以应用场景为基础
- 密钥全生命周期管理
- 密钥使用策略管理
- 监控密钥使用过程
- 支持KMIP1.4协议



功能说明

运营管理	密码接口服务	应用管理	CA和密钥管理	运维监控管理

运维监控管理：

运维监控针对密码安全管理平台管理的密码资源池设备、应用密码接口服务、平台服务的使用情况、可用状态、故障信息进行实时监控，辅助平台管理员能够及时了解平台整体运行情况，以便进行系统运维、应急响应和资源扩容管理。

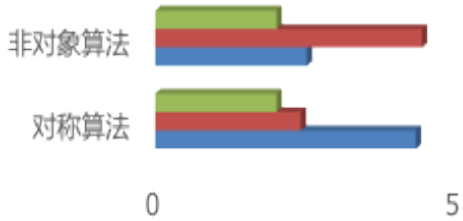
密码设备状态监控

服务状态监控

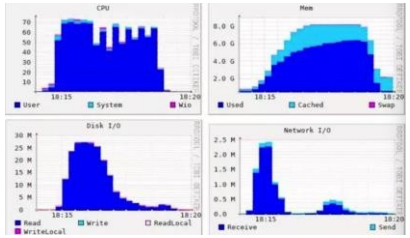
应用监控

故障告警

故障告警



密码运算资源



密码设备资源

服务特色

多种可信服务

企业只需部署一个平台即可享受全方位 一站式的密码服务体验。

双体系多算法

平台支持PKI以及多种国际算法和国密算法，支持RSA、DES、MD5、SHA1/256算法；支持SM2、SM3、SM4算法；

统一接口

平台建立统一的平台规范接口标准，通过统一的API对接， 企业系统可在统一的框架内按照数据标准对接平台。

统一密钥管理

平台统一管理密钥，规避密钥的生产、传输、存放、销毁等操作中存在的泄密风险

企业收益

开发成本低

由于平台接口标准统一，不需要企业的应用系统做太多改动，即可实现国密算法安全升级

成熟的运营模块

平台拥有成熟的运营模块，可支持多种营销模式，多维度的统计分析，辅助企业精细化管理

一站式服务

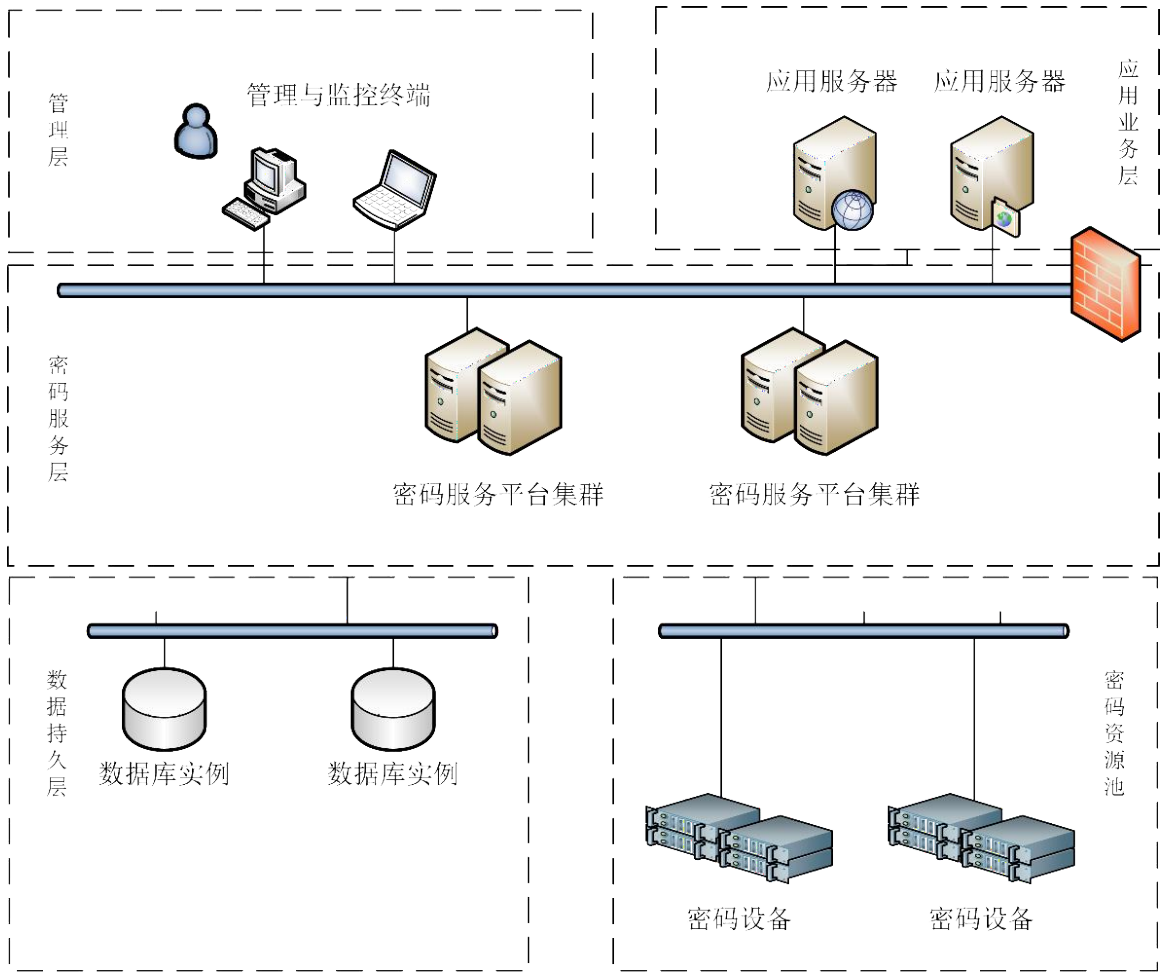
平台除提供基础密码算法以外，还集成了多种产品服务，企业可自由调用，省去企业切换多个系统的操作成本

避免重复投资

每个业务系统可能独自配备一套以上的密码设备，效能溢出，平台统一管理后配置密码能力可最大程度的分配密码运算能力，降低企业设备成本

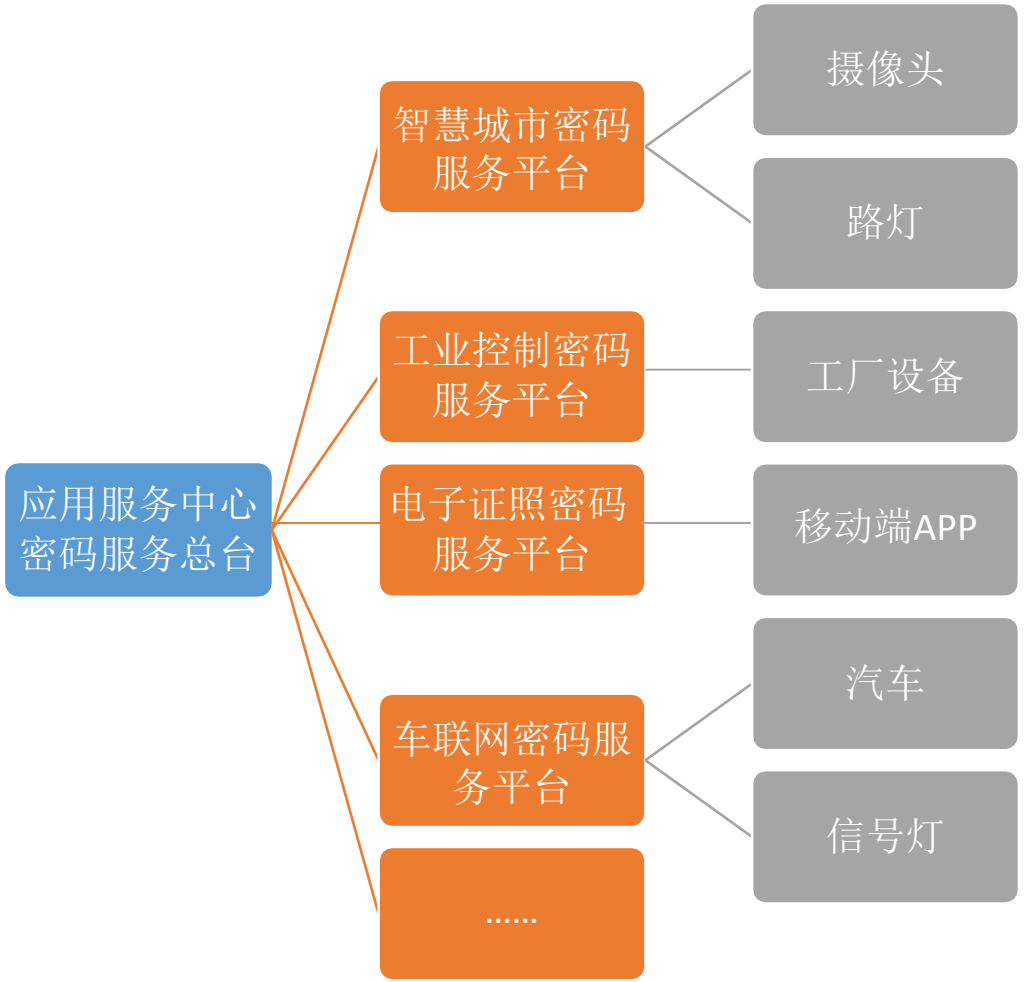
应用场景（业务系统国密升级）

- 密码服务平台向下控制硬件密码机，向上则为应用层提供标准的密码服务API，应用层不需要了解各类密码机的指令接口，也不用直接管理自身系统的密钥。
- 统一管理大量业务系统所需要密钥将极大简化应用层的开发和运维工作。
- 对未接入密码服务的系统来说，可最低开发成本的升级其安全等级，享受国密算法带来的安全服务。

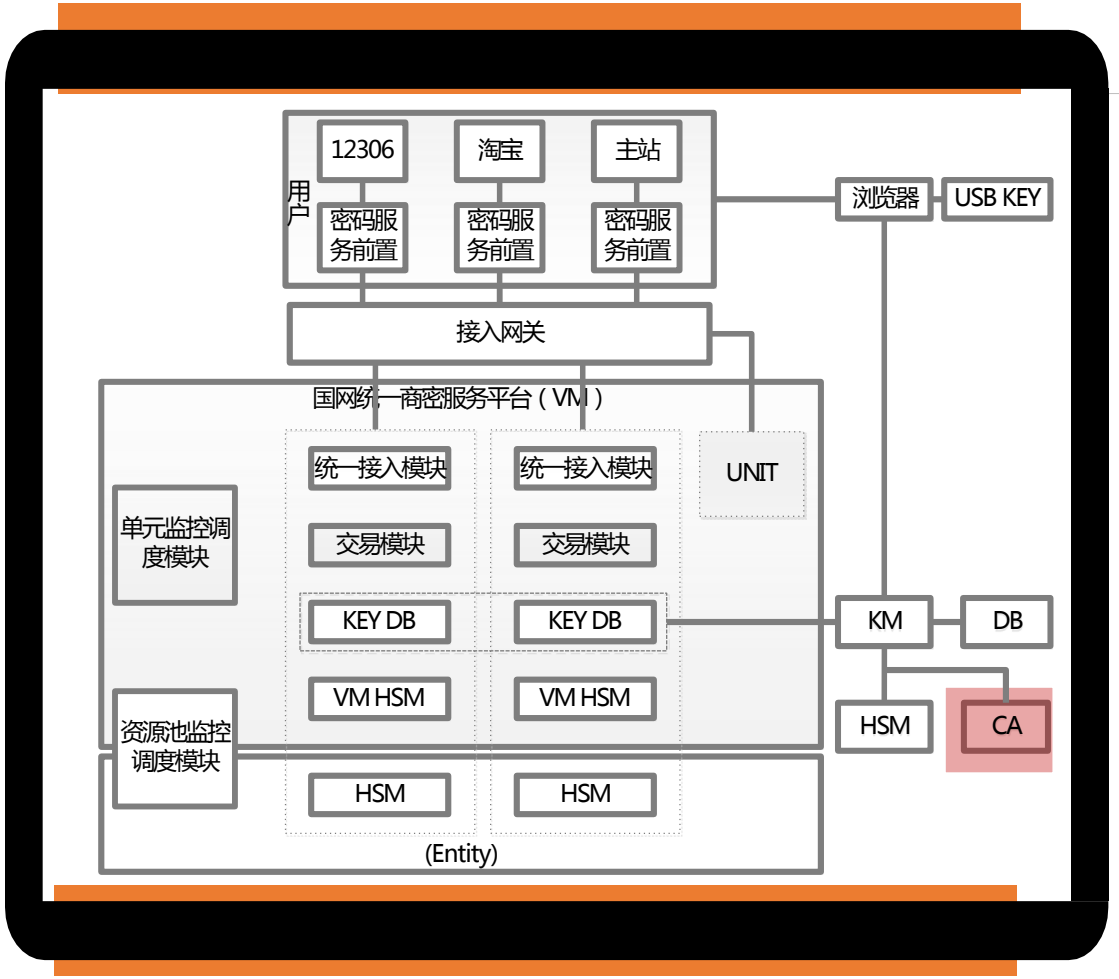


应用场景（万物互联，多级平台）

- 应用中心和各个分应用平台分别建立不同程度的密码服务平台，密码服务平台负担下属分应用平台的密钥产生，密码的运算以及对下属分应用平台的密码服务平台的统一监控
- 分应用平台的密码服务平台负责对接自身应用的实际应用端，例如APP，摄像头，汽车等等，负责应用产生的数据运营管理。
- 密钥由应用中心统一下发，统一运算，降低各个分应用平台运维人员工作量。
- 应用中心与分应用平台的多级密码服务平台通过安全的远程控制有机的成为一个整体。



国家电网成功案例



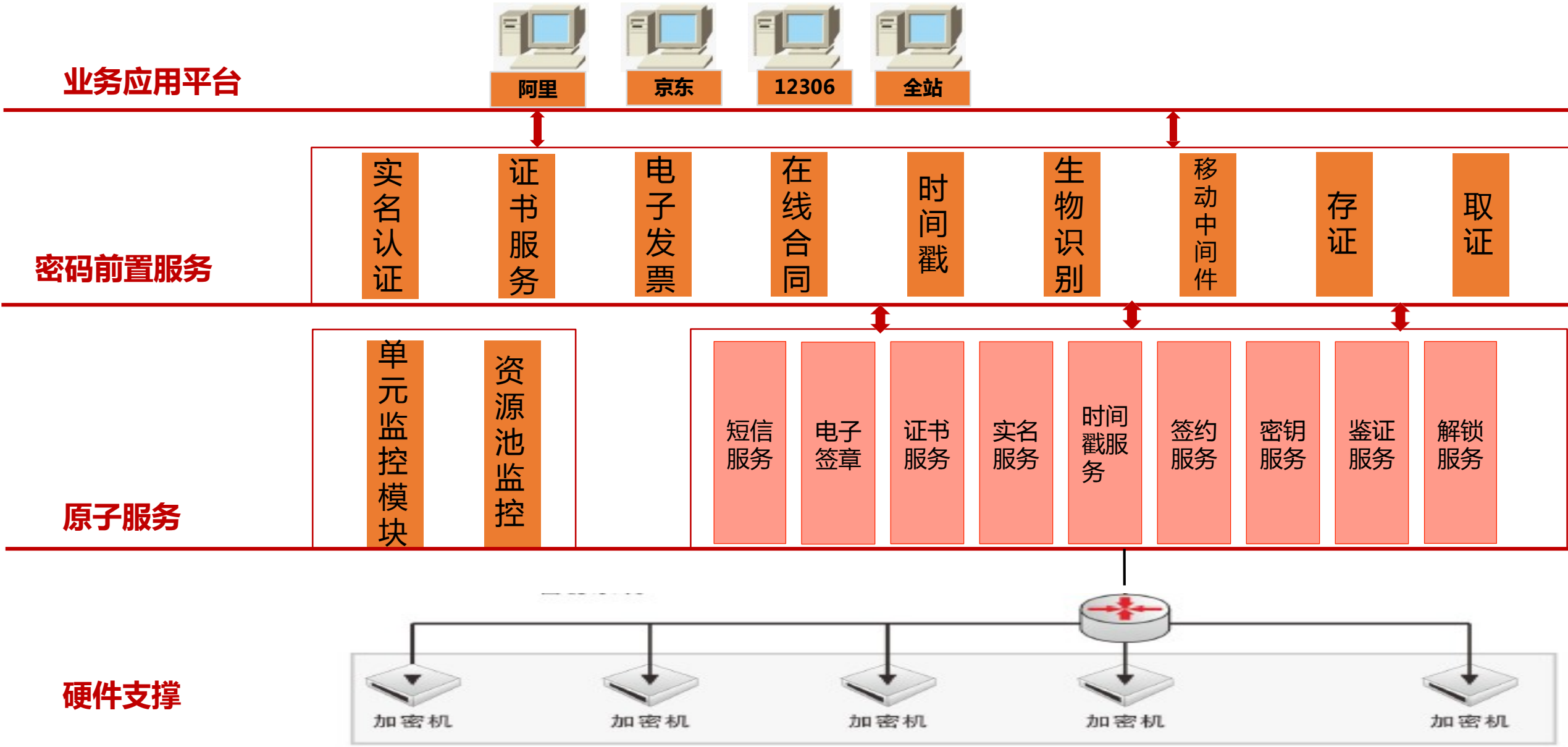
融合云计算技术，实现平台的动态伸缩。

平台模块化设计，实现平台的快速集成。

计算和业务处理分离，保障系统性能。

平台资源统一监控和调度，实现按需服务。

国网平台功能


业务应用平台
阿里
京东
12306
全站
密码前置服务
实名认证
证书服务
电子发票
在线合同
时间戳
生物识别
移动中间件
存证
取证
原子服务
单元监控模块
资源池监控
短信服务
电子签章
证书服务
实名服务
时间戳服务
签约服务
密钥服务
鉴证服务
解锁服务
硬件支撑
加密机
加密机
加密机
加密机
加密机

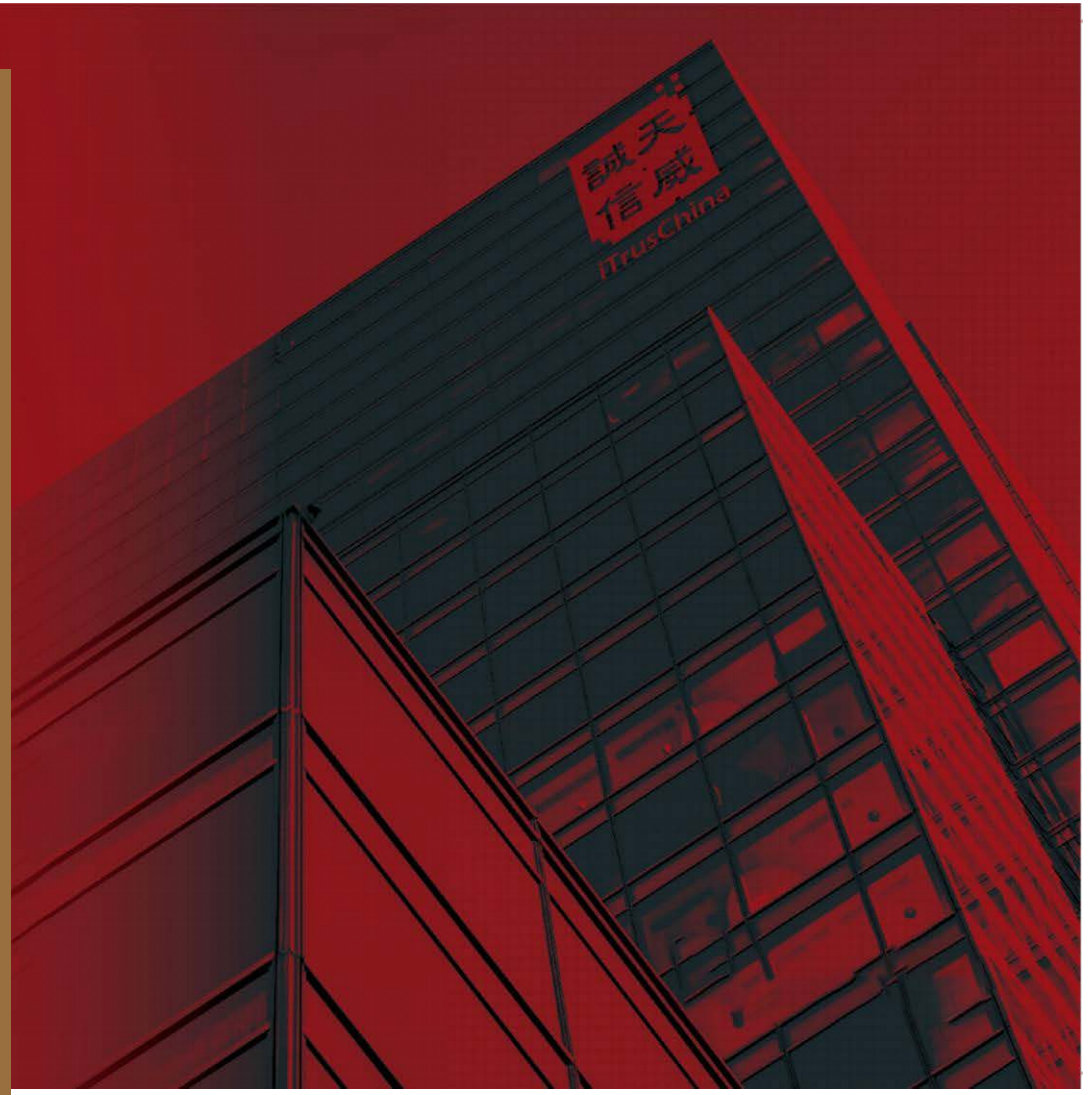
第三部分

公司介绍

关于天威诚信

天威诚信是依据《中华人民共和国电子签名法》，由工业和信息化部许可设立的电子认证服务机构，致力于提升网络空间的安全性和可信度，面向各类网络应用提供身份认证、行为认证，并对数据电文按照电子证据审查要求进行核验固化，以实现网络空间电子数据的安全、可信、可用、可追溯，促进数字经济的健康有序发展。

天威诚信已为近5亿用户提供电子认证服务，服务范围覆盖政务、银行、证券、保险、司法、招投标、互联网金融等领域。



公司发展历程

2000年

天威诚信成立；
经工业和信息化部许可成为全国PKI/CA企业，将Versign业务引入中国。

2002年

自主研发的证书认证系统（iTrusCA）通过公安部检测，获得《计算机信息系统安全专用产品销售许可证》；
获得《高新技术企业证书》。

2004年

参与《中华人民共和国电子签名法》和《电子认证服务管理办法》起草工作；
天威诚信CA处理中心获得中国信息安全产品测评认证中心颁发的国家信息安全认证产品型号证书。

2005年

获工业和信息化部《电子认证服务许可证》；
获得国家密码管理局颁发的《电子认证服务使用密码许可证》。

2007年

承担“十一五”国家科技支撑计划项目课题——《自主信息安全型服务集成运营技术研究开发》的研究。

2008年

获得“中国服务业科技创新奖”；
获得第29届北京奥运会及残奥会信息安全保驾护航奖。

2009年

取得《ISO9001质量管理体系认证证书》；
嵌入式统一身份认证管理系统（iTrusUTS）通过中华人民共和国国家版权局审核，首次发布。

2010年

成为北京电子商务服务平台重点企业；
iTrusESA、iTrusCA、iTrusUTS入选北京市自主创新产品目录；
承担国家发展和改革委员会信息安全专项——《基于电子签名的电子数据取证与证据管理系统研发和产业化项目》。

2012年

参与起草的《信息安全技术——电子认证服务机构运营管理规范》经全国信息安全标准化技术委员会批准正式发布；
获国家密码管理局授予《商用密码销售许可证》；
经全国信息安全标准化技术委员会秘书处批准，成为“网站可信国家标准项目组成员单位”。

2015年

天威诚信子公司天诚安信加入“中关村四方现代服务产业技术创新战略联盟”，开展中小微企业互联网金融服务和移动互联网+4.0试点研究；
天威诚信专利《降低主密钥破解和泄露危险的IBE数据加密系统及方法》获得授权；
获《信息系统集成及服务资质证书》。

2016年

成为中关村国家自主创新示范区标准化试点单位；
被国家知识产权局授予“国家知识产权优势企业”称号。

2017年

取得《ISO/IEC27001信息安全管理体系认证证书》；
获《电子政务电子认证服务许可》；
2017年，获得公安机关《信息系统安全等级保护备案证明（3级证书）》。

2018年

推出天威诚信电子认证云服务（PaaS)平台。

天威诚信产品体系

应用类产品

名鉴

电子合同（信任签）

平台

天威云-电子认证云服务平台+i信

法眼法律服务平台

服务类产品

认证类

- 证书服务
- 实名服务
- 人脸识别
- 动态口令
- 短信服务
- SSL证书
- CIM

签名类

- 签名服务
- 签约服务
- 时间戳服务

证据类

- 存证服务
- 取证服务

法律类

- 核验服务
- 固化服务
- 见证服务
- 取证服务
- 快速仲裁

平台运营管理

用户中心

- 客户管理
- 应用管理

费用中心

- 订单管理
- 消费账单
- 支付管理
- 发票管理
- 促销活动管理
- 服务计费

服务管理

- 服务管理
- 产品上架
- 服务商入驻
- 服务商产品上架

统计监控

- 统计报表
- 日志监控

客服

- 呼叫中心
- 在线支持
- 客服工单

技术类产品

CA类

- 数字证书认证系统
- 数字证书管理系统
- 密钥管理系统
- 在线证书状态查询

签名类

- 时间戳系统
- 移动数字证书应用系统
- 电子签名应用服务器
- 签名验签服务器
- 密码服务平台
- 手机盾（密钥分割）

认证类

- 多因素强身份认证
- 动态口令
- 认证宝

审计类

- 堡垒机
- 日志审计
- 数据库审计

存储类

- 安全存储

天威诚信典型合作伙伴一览

银行类

中国工商银行 INDUSTRIAL AND COMMERCIAL BANK OF CHINA
中国农业银行 AGRICULTURAL BANK OF CHINA
中国银行 BANK OF CHINA
中国建设银行 China Construction Bank
交通银行 BANK OF COMMUNICATIONS
中国邮政储蓄银行 POSTAL SAVINGS BANK OF CHINA
中信银行 CHINA CITIC BANK
兴业银行 INDUSTRIAL BANK CO.,LTD
浦发银行 SPD BANK
中国银联 China Unionpay
WeBank 微众银行
网商银行 MYbank

电子采购类

中粮 COFCO
国家电网公司 STATE GRID CORPORATION OF CHINA
HUAWEI
lenovo 联想
AIR CHINA 中国国际航空公司
方正集团 FOUNDER
中国电建 POWERCHINA
CEEC 中国能建
伊利
五粮液
本溪钢铁（集团）有限公司 BENXI IRON&STEEL(GROUP)CO.,LTD

企业电商类

淘宝网 Taobao.com
天猫 TMALL.COM
支付宝 ALIPAY
JD.COM 京东
良品铺子 BESTORE
国美电器
苏宁易购 suning.com
1号店
途牛
驴妈妈
大众点评 dianping.com
Ctrip 携程

互金类

京东金融 JD Finance
陆金所 Lufax.com
海尔金控 Haier Financial Holdings
鹏金所 Penging.com
人人贷 renrendai.com
钱包 QianBao.com
中邮消费金融 PSBC CONSUMER FINANCE
上海黄金交易所 SHANGHAI GOLD EXCHANEG
度小满金融
宜人贷 www.yirendai.com
易金所 一起玩转金融
中银消费金融 BOC CONSUMER FINANCE

证券、保险类

中国银河证券 CHINA GALAXY SECURITIES
华龙证券 CHINA DRAGON SECURITIES
国都证券 GUODU SECURITIES
广发证券 GF SECURITIES
方正证券 FOUNDER SECURITIES
国海证券
安信证券 ESSENCE SECURITIES
PICC 中国人民保险

政务类

SIPO 国家知识产权局
甘肃省公共资源交易局
甘肃省交通运输厅 www.gsjt.gov.cn
中华人民共和国生态环境部
临沂政务服务 公共资源交易
宁波市财政局 | 原宁波市地方税务局
福州市市民公共服务平台
德阳市政务网

信托类

渤海信托
华融信托
五矿信托 MINMETALS TRUST
西藏信托
云南国际信托有限公司 YUNNAN INTERNATIONAL TRUST CO.,LTD.
中海信托 ZHTC
中信信托 CITIC Trust
中原信托有限公司 ZHONGYUAN TRUST CO.,LTD.

云应用类

阿里云
腾讯云
用友 yonyou
京东云 预见无限可能
金山云 WWW.KSYUN.COM
HUAWEI
inspur 浪潮
有孚网络

构建信任·传递信任

iTrusChina

构建信任 · 传递信任

北京天威诚信电子商务服务有限公司
地址：北京市海淀区上地八街7号院4号楼401A
电话：010-50947500
E-mail：marketing@itrus.com.cn