

**Aisino** 航天信息



# 航天信息 密码系列产品

AISINO CRYPTOGRAPHIC  
SERIES PRODUCTS



## 公司简介

### COMPANY PROFILE

航天信息股份有限公司是中国航天科工集团有限公司控股的国有科技型上市公司，于2000年11月1日成立，2003年7月11日在A股市场成功挂牌上市（SHA:600271），是中国IT行业最具影响力的上市公司之一。

依托航天的技术优势、人才优势和组织大型工程的丰富经验，航天信息以信息安全为核心，重点发展金税、金融科技服务、智慧、网信产业并积极拓展国际市场，面向政府（行业）、企业信息化市场，提供信息技术服务和一体化解决方案，服务2000万企业用户和政府客户。在全国31个省、市、自治区和5个计划单列市、2个特别行政区，建立了近200家分子公司、1100余家基层业务单位。拥有信息安全、人工智能、大数据、区块链等关键核心技术，承担了“金税工程”、“金卡工程”、“金盾工程”等国家重点工程，是国家大型信息化工程和电子政务领域的主要参与者。

“ 成为国际一流的信息产业集团，致力于信息更安全、更增值，社会更智慧、更诚信 ”



## VPN 综合安全网关

航天信息VPN综合安全网关内置经国家密码管理局鉴定并批准的高速密码模块,全面支持SM系列密码算法,所有密码运算均由内置高速密码模块实现,完全释放主机CPU性能,产品支持国密标准的IPSec与SSL安全传输协议,为客户提供安全、高效的可信认证、加密传输等服务。



### 产品功能

#### PRODUCT FUNCTION



#### 可信身份认证

支持国密标准规定的数字证书+口令的“双因子”认证机制,确保登录用户的身份安全可靠。



#### 信息加密传输

采用国密标准要求的隧道模式进行安全报文的加密传输,保障信息传输安全。



#### 多信任链支持

支持多个信任根和多条信任证书链,符合X.509格式的CA机构均可纳入安全网关的信任域体系。



#### 权限控制

基于X.509数字证书目录结构树的授权控制,可以授权特定目录节点下的用户对特定资源的访问权限。



#### 单点登陆

系统具有单点登录功能,可以实现一次登录,全网通行。



#### 日志追踪

通过系统日志可对用户行为进行追踪,方便查找可疑或不规范的用户操作行为。

### 产品特点

#### PRODUCT FEATURES



#### 可靠性

基于国密SM系列算法,采用IPSec、SSL协议实现可信身份认证、数据传输安全。



#### 易用性

客户端和管理端均采用图形化界面进行用户操作,使用简单,配置便捷。



#### 稳定性

支持断线重连、负载均衡等功能,保证服务稳定运行。



#### 兼容性

全面支持中标麒麟、银河麒麟等操作系统终端环境的接入认证与访问控制,同时兼容Windows、Linux操作系统以及Android等移动平台的安全接入需求。



#### 多接口组合

支持千兆电、千兆光、万兆光等多种网络接口,满足用户不同应用需求。

# 设备参数

## EQUIPMENT PARAMETERS

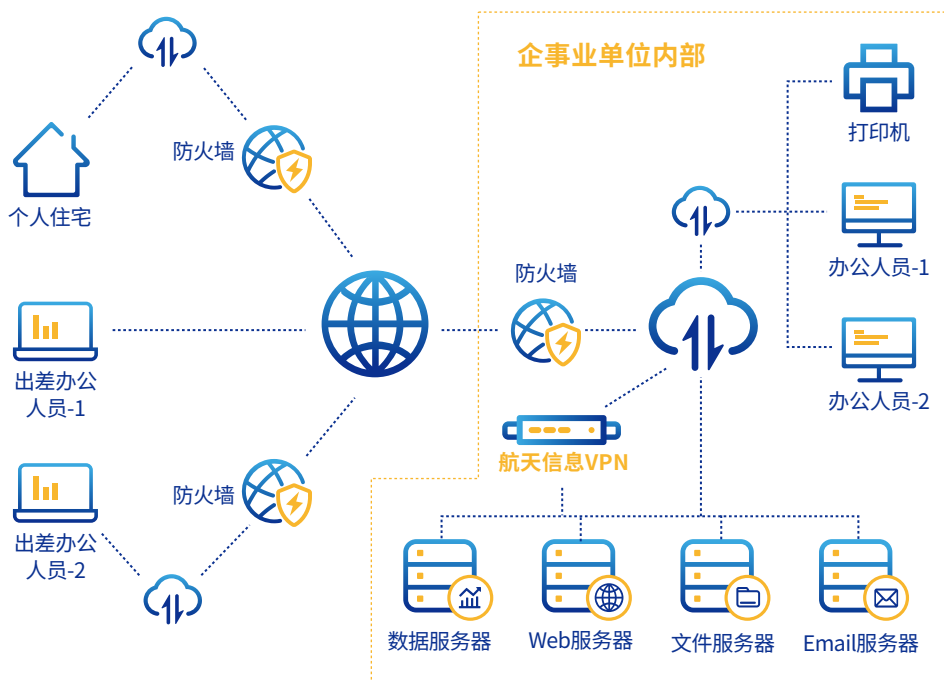
规格		参数
SSL 性能	算法套件	ECC (SM2)-SM4-SM3 ECC (SM2)-SM1-SM3
	每秒新建用户数	≥2000
	最大并发连接数	≥100000
	最大用户数	≥10000
	密文吞吐率	≥800Mbps

规格		参数
IPSec 性能	算法套件	SM2+SM1+SM3+ESP SM2+SM4+SM3+ESP
	工作模式	隧道模式
	密文吞吐率	≥500Mbps
	隧道数	≥20000

## 典型应用

### TYPICAL APPLICATIONS

在企事业单位内网服务器前端部署一台航天信息VPN综合安全网关,为远程办公用户提供基于“数字证书+口令”的“双因子”身份鉴别机制,确保登录用户的身份合法性。用户通过存储在USBKey中的数字证书登陆VPN综合安全网关进行身份认证和会话协商,协商通过后与VPN综合安全网关之间建立SSL隧道,实现交互数据的加密传输。



VPN综合安全网关典型应用示意图

## 主要客户

### MAJOR CUSTOMERS



湖北省粮食局



河南省应急管理厅



招商局集团

## 产品资质

### PRODUCT QUALIFICATION



## 签名验签 服务器

航天信息签名验签服务器是面向各类电子数据提供基于数字证书的签名和加解密服务的专用密码设备。产品遵循国密系列标准,提供符合国家标准接口规范的数据接口,支持国密SM系列算法和国际通用算法,为应用系统提供身份真实性、数据保密性、数据完整性和操作行为不可抵赖等安全保障服务。



### 产品功能

#### PRODUCT FUNCTION



#### 数字签名

支持PKCS#1格式的数字签名和PKCS#7格式的Attach、Detach数字签名。



#### 数字信封

支持PKCS#7格式的数字信封加解密。



#### 密钥管理

提供SM2/RSA密钥生成、存储、导入、导出、备份、恢复到销毁的全生命周期密钥管理功能。



#### 证书管理

支持SM2/RSA证书请求、导入、导出、解析,提供CA信任链、CRL、OCSP等多种方式的证书有效性验证,支持证书历史数据库。



#### 信任链管理

多CA信任链和多级CA信任链管理。



#### 系统管理

实现三元权限管理,支持密码服务节点管理、权限用户管理等,提供数据的密文备份/恢复功能。

### 产品特点

#### PRODUCT FEATURES



#### 标准化

遵循国密系列标准,符合《GM/T 0020-2012证书应用综合服务接口规范》标准接口规范。



#### 国产化

支持SM2/3/4算法和国密证书,支持信创硬件设备和软件操作系统。



#### 安全性

密码运算和密钥存储基于硬件密码设备,采用分级权限用户管理系统。



#### 兼容性

支持多CA证书链,提供Win/Linux/信创环境下C/Java等多种形式的签名服务调用接口。



#### 高可用性

支持双机热备和集群部署,实现负载均衡调度。

# 设备参数

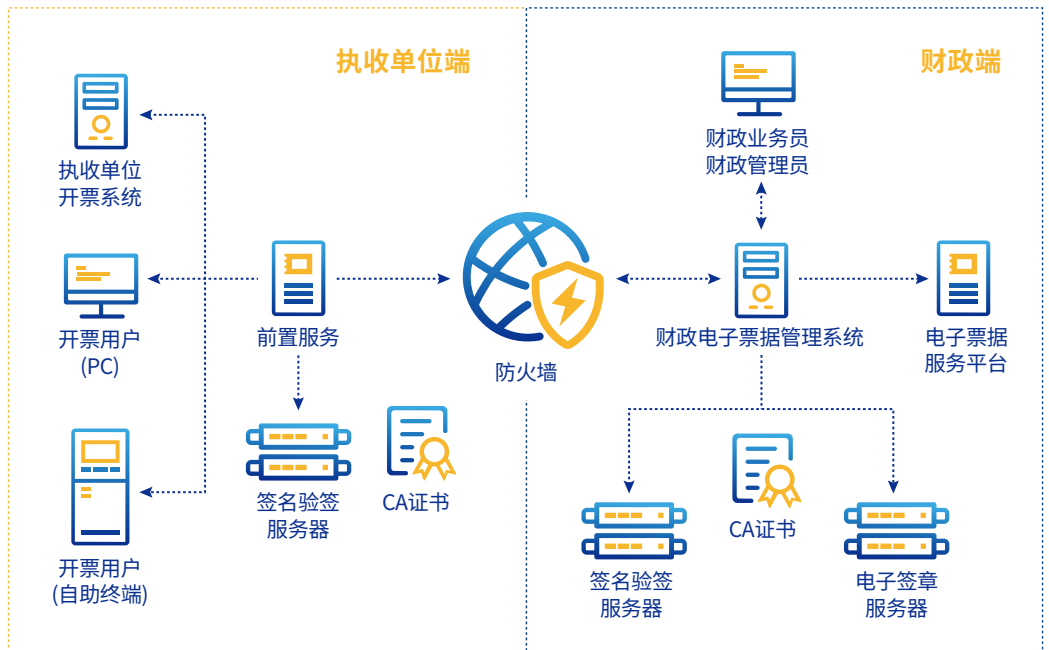
## EQUIPMENT PARAMETERS

规格	参数
SM2签名/验签	80000/60000 tps
SM2生成密钥	15000 对/秒
RSA2048签名/验签	4500/100000 tps
RSA2048生成密钥	34 对/秒

## 典型应用

### TYPICAL APPLICATIONS

财政电子票据业务需要各执收单位与财政部门进行数据交互, 为了保障电子票据业务数据的安全性, 根据财政部《关于财政非税电子票据业务中密码设备应用有关事宜的通知》(财信[2019] 25号) 有关要求, 需要在执收单位和财政部门分别部署签名验签服务器, 来保障电子票据数据传输过程中的保密性、完整性。



财政电子票据系统签名验签方案

## 主要客户

### MAJOR CUSTOMERS



宁夏财政厅



温州卫健委



浙江省肿瘤医院、银川市贺兰县人民医院、  
固原市原州区人民医院等

## 产品资质

### PRODUCT QUALIFICATION





## 时间戳服务器



航天信息时间戳服务器依据国密标准，采用精准时间源、高强度安全保障机制，为用户提供精准可信且不可抵赖的时间戳服务。可以满足应用系统签发时间戳、验证时间戳、同步可信时间的需求，同时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。

### 产品功能

#### PRODUCT FUNCTION



#### 可信时间源同步

可与国家授时中心进行时间源同步，同时支持北斗、GPS、CDMA三合一时间源，确保签发时间戳权威性。



#### 时间戳签发验证

签发可信时间戳、验证时间戳有效性。



#### 系统备份及恢复

支持系统信息的备份及恢复，确保系统数据的安全可靠。



#### 支持连接白名单

通过连接白名单，实现时间戳服务器对应用服务器的授权认证。

### 产品特点

#### PRODUCT FEATURES



#### 合法合规

符合《中华人民共和国电子签名法》，采用权威第三方认证机构颁发的时间戳服务器证书，具备法律效力。



#### 权威可信

采用先进精准的可信时间源设备和时间同步技术保证时间的真实可靠。



#### 管理便捷

包含时间同步管理、时间戳证书管理、密钥和证书管理等。



#### 冗余热备

支持多台时间戳服务器的并行，实现设备冗余热备和负载均衡。



#### 安全可靠

基于高强度的双向身份认证，确保管理者的合法身份。

## 设备参数

### EQUIPMENT PARAMETERS

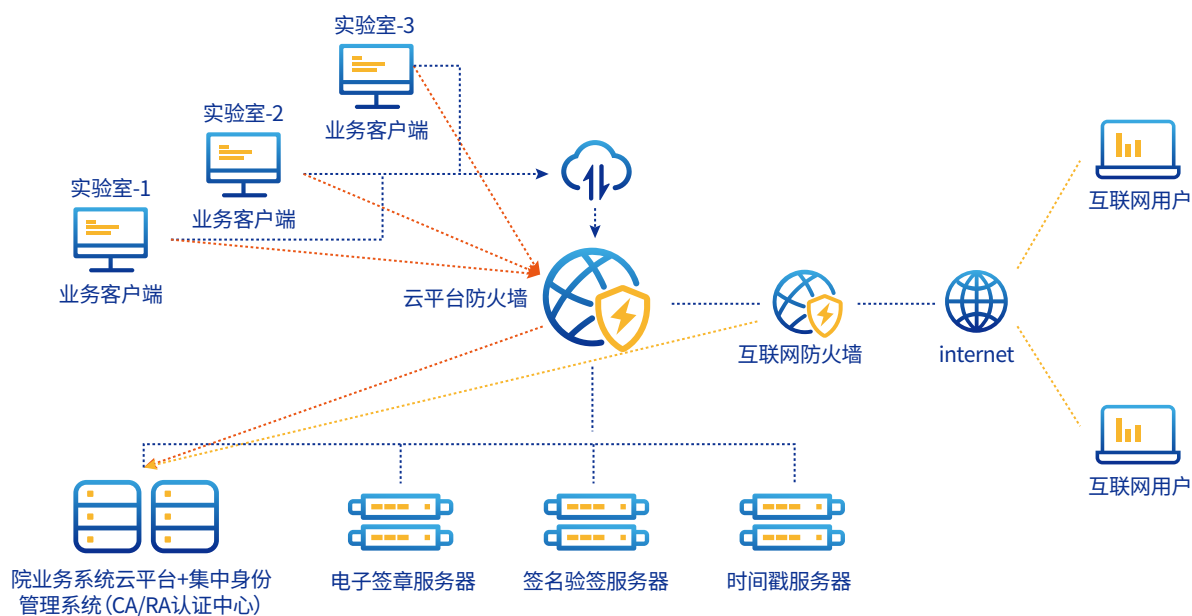
规格	参数
SM2签发效率	40000 次/秒
SM2验证效率	24000 次/秒
RSA 2048签发效率	2800 次/秒
RSA 2048验证效率	50000 次/秒
授时精度	0.5-3ms

规格	参数
守时精度	<1ms (72h)
时间源信号模块	支持北斗、GPS、CDMA三合一时间源
时间同步协议	NTP、SNTP
支持应用接口	Java、C、COM
MTBF	50000h

## 典型应用

### TYPICAL APPLICATIONS

根据食品药品检验研究院业务需求,部署包含时间戳的签章服务,主要为“食品LIMS系统、药品LIMS系统、OA系统”提供包含高精度时间戳的签章服务。



时间戳服务器典型应用示意图

## 主要客户

### MAJOR CUSTOMERS



温州康宁医院集团



广西省税务局



陕西省食品药品监督检验研究院



## 服务器密码机

航天信息服务器密码机是由航天信息自主研发的高性能密码设备，产品可为多任务并行的业务系统提供高强度、高效率的数据加解密、签名验签等服务，同时提供安全、完善的密钥管理机制，可广泛应用于政务、电子商务、银行、等行业的业务系统中。



### 产品功能

#### PRODUCT FUNCTION



#### 数据加解密

支持SM4/AES/3DES算法的ECB和CBC模式的数据加密和解密功能。



#### 密钥管理

支持密钥安全产生、分发、更换、备份、恢复、存储、销毁等管理功能。



#### 密码算法支持

支持SM系列国密算法，RSA等国际标准算法。



#### 真随机数

采用国家密码局审批的WNG-8随机数发生器产生的真随机数，确保密钥的质量。



#### 权限管理

采用分级权限管理，分为管理员和操作员权限，确保严格的权限控制。



#### 标准API接口

支持PKCS#11、MS-CSP等国际标准接口，并可根据用户需求定制接口。

### 产品特点

#### PRODUCT FEATURES



#### 高可靠性

支持多机并行、双机热备、断链修复等功能，提供强大的容错能力，保障业务运算的连续性。



#### 高稳定性

服务器密码机的平均无故障工作时间（MTBF）大于50,000小时。



#### 高安全性

采用三层密钥体系结构，并将密钥加密存储，受到非法入侵时自动销毁。



#### 兼容性

支持X86环境和信创环境下的各类处理器、操作系统、数据库、中间件等。



#### 易用性

通过可视化配置管理工具，方便对服务器密码机进行配置和管理操作。

## 设备参数

### EQUIPMENT PARAMETERS

规格	参数	规格	参数
SM2签名/加密密钥对存储能力	≥500对	RSA (2048) 签名速度	≥1200 次/秒
SM2签名速度	≥51200次/秒	RSA (2048) 验证速度	≥44500 次/秒
SM2验签速度	≥39400 次/秒	SM4算法加解密速度	≥5500Mbps
RSA (2048) 密钥对生成速度	≥39对/秒	SM3杂凑算法	≥3000Mbps

## 典型应用

### TYPICAL APPLICATIONS

在电子公文应用中,在不同业务服务端部署服务器密码机,对传输的数据进行加密保护,对于解密后的接收数据,通过业务系统调用服务器密码机对数据进行加密存储,从而杜绝明文数据泄露和被篡改的隐患,同时防止未经授权的用户查看和利用数据。



## 主要客户

### MAJOR CUSTOMERS



天津市公安局



国资委



招商局集团



南京信息技术研究院

## 产品资质

### PRODUCT QUALIFICATION



## 电子签章系统

航天信息电子签章系统是将传统的印章模式与数字签名技术完美结合的应用软件系统,可灵活应用于电子发票、电子票据、电子病历、电子证照、各党政机关和企事业单位的电子公文、电子合同、OA管理等业务系统中,为其提供电子印章制作、管理、盖章、验章等服务。



### 产品功能

#### PRODUCT FUNCTION



#### 签章验章

支持以可视化软件/插件/SDK接口形式对OFD、PDF、WORD、EXCEL、WPS、HTML等格式的数据文件进行签章验章。



#### 印模管理

提供印模图片的管理,印模文件支持PNG、JPG、BMP、GIF多种格式。



#### 系统管理

实现组织机构管理、密码服务节点管理、权限用户管理,支持数据备份/恢复功能。



#### 用户管理

支持多级组织架构的用户管理。



#### 印章管理

提供印章申请、印章制作、印章冻结、解冻、注销管理。



#### 印章委托

支持用户印章委托管理。

### 产品特点

#### PRODUCT FEATURES

#### 标准化

遵循国密系列标准规范,符合国家政务服务平台对接标准。

#### 国产化

支持信创环境、国密算法和国密证书,提供OFD版式文件的签章验章。

#### 安全性

支持基于证书的用户权限认证登录和接口调用,密码运算和密钥存储基于硬件密码设备,采用分级权限用户管理系统,提供密码服务授权管理。

#### 高可用性

支持双机热备和集群部署,实现负载均衡调度,支持千万级用户。

#### 扩展性

支持分级节点管理,制章点和用章点可统一部署和分布式部署,提供网络盖章和本地盖章。

#### 兼容性

支持多CA证书链,提供Windows/Linux/信创环境下C/Java等多种形式的签章服务调用接口。

# 设备参数

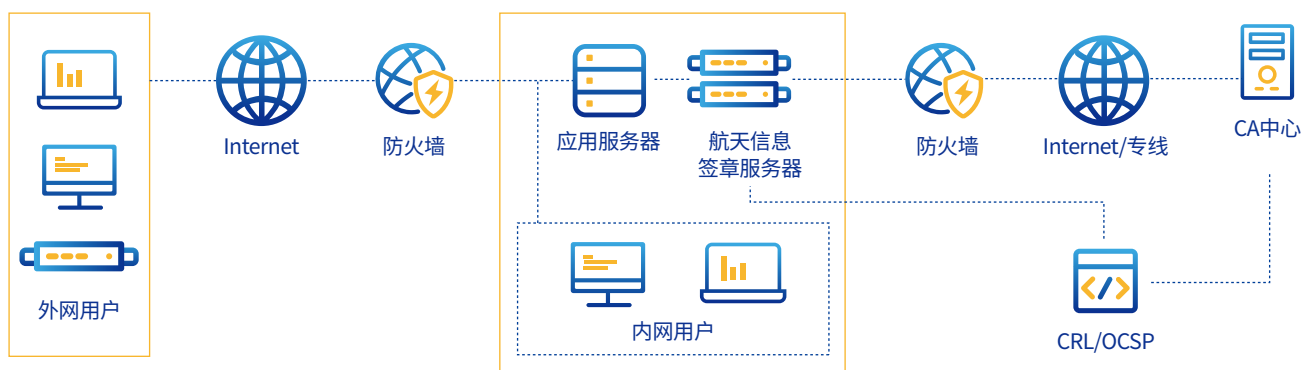
## EQUIPMENT PARAMETERS

规格	参数
SM2签章	8000 tps
SM2验章	4000 tps
RSA 2048签章	4100 tps
RSA 2048验章	7000 tps
文档格式	OFD、PDF、WORD、EXCEL、WPS、HTML

# 典型应用

## TYPICAL APPLICATIONS

51发票平台使用航天信息电子签章系统，采用分布式部署方式，在电子发票业务中应用电子印章制作、盖章、验章等服务。平台建成以来，为数百万用户、数十亿份发票提供稳定的电子签章服务，促进了平台用户（企业、社会公众）制章及电子发票盖章全程线上化，节省了发票成本，提高了发票处理效率。



航天信息电子签章系统典型应用示意图

## 主要客户

### MAJOR CUSTOMERS

宁夏自治区

吴忠市政府

天津公安

辽宁公安

国资委协会办

中国记者协会

宁夏国税局

山西国税局

江西国税局

京东

中国移动

麦当劳

国美

## 产品资质

### PRODUCT QUALIFICATION





## 密钥管理系统

航天信息密钥管理系统可实现对密钥的全生命周期集中管理,包括密钥生成、存储、备份、归档、恢复、更新,满足第三方业务系统对于对称密码体制和非对称密码体制的密钥服务需求,支持认证中心和司法取证的需要。系统使用经国家密码管理局批准的密码设备,支持符合PKCS#11标准的加密设备和国密SM系列算法。

### 产品功能

#### PRODUCT FUNCTION



#### 密钥生成

采用由国家密码管理局批准使用的双物理噪声源生成随机数,可生成各类对称密钥和非对称密钥。



#### 标准化密码接口

提供符合《GM/T 0018-2012 密码设备应用接口规范》的标准化接口。



#### 密钥安全存储

设备内部支持多种密钥的安全存储。



#### 密码算法支持

支持SM系列国密算法,以及国际算法。



#### 密钥备份与恢复

可通过页面灵活备份密钥,保障备份数据的安全性。

### 产品特点

#### PRODUCT FEATURES



#### 高兼容性

支持多款密码设备,兼容通用Linux、中标麒麟、银河麒麟操作系统,支持Oracle、达梦等数据库。



#### 安全性高

密钥产生后加密存储,传输使用数字信封形式,确保密钥管理及存储安全性。



#### 方便集成

提供多个密钥管理接口,覆盖功能范围广,第三方业务系统接入灵活。



#### 管理服务分离

拆分密码管理和服务功能,实现系统灵活部署、便于管理人员日常运维。



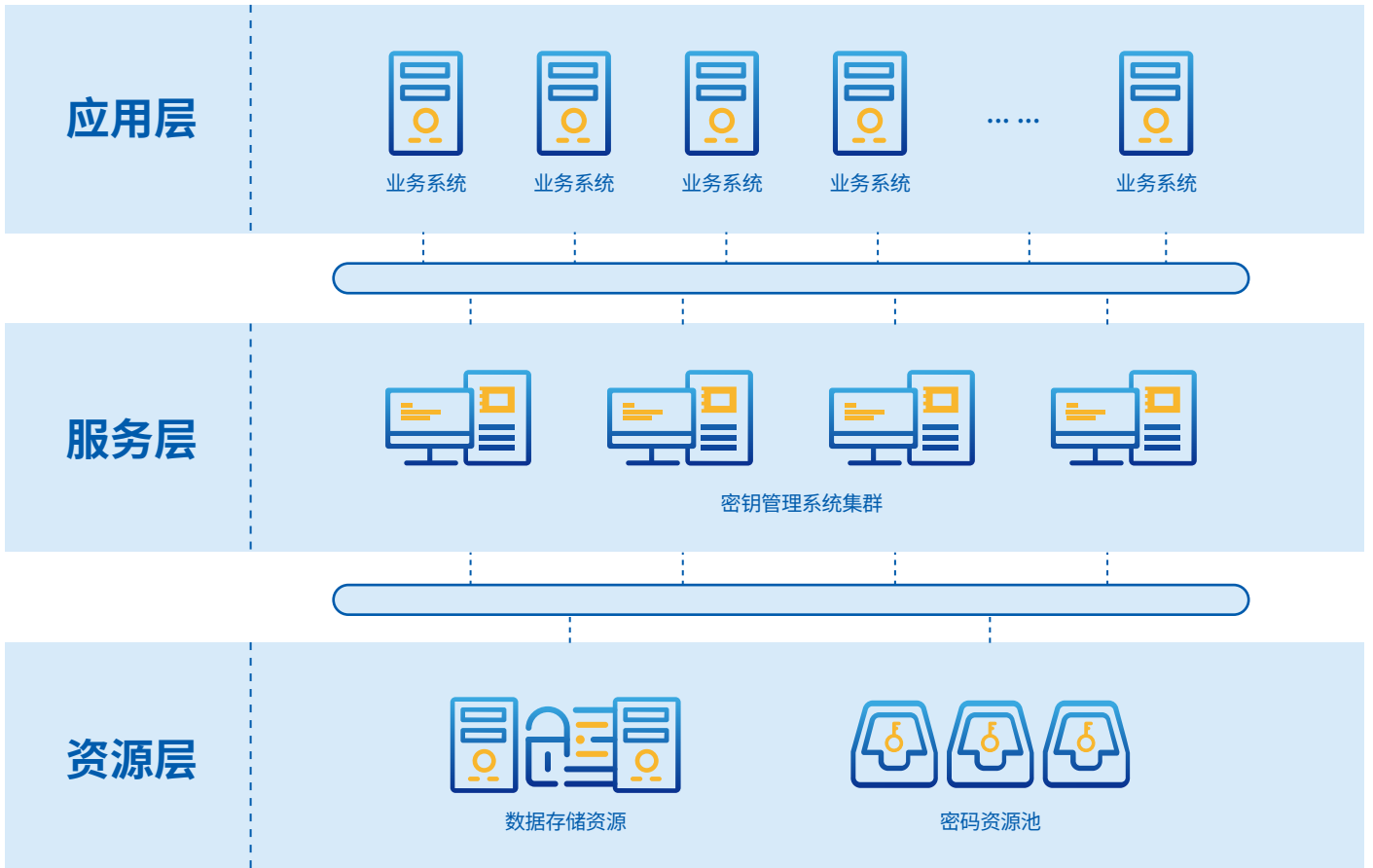
#### 密钥预生成

密钥生成机制灵活,可通过定时任务预先生成非对称密钥对,提高系统非对称密钥生成效率。

# 典型应用

## TYPICAL APPLICATIONS

航天信息密钥管理系统广泛应用于电子政务、电子商务、金融、医疗、社保、公共资源等业务系统中,为第三方应用系统提供安全、完善的密钥管理服务。



密钥管理系统典型应用示意图

### 主要客户

MAJOR CUSTOMERS



重庆市公安局



国资委



西藏CA



中国外运股份有限公司

### 产品资质

PRODUCT QUALIFICATION



## 数字证书认证系统

航天信息数字证书认证系统，遵循国家密码管理局颁布的《证书认证系统密码及其相关安全技术规范》等标准，支持SM2、SM3、SM4等密码算法，可用于数字证书的申请、审核、签发、注销、更新、查询等业务，系统包括证书签发、用户注册管理、证书/CRL发布和证书状态在线查询等子系统。

### 产品功能

#### PRODUCT FUNCTION

#### 证书管理

提供证书签发、注销、恢复、冻结解冻功能，提供证书全生命周期状态管理。

#### 证书发布

签发证书发布至LDAP，提供证书下载功能。

#### 证书状态在线查询

提供OCSP服务，支持证书状态的在线查验。

#### CRL签发

支持定期签发或手动签发CRL文件，并发布至LDAP供用户下载验证。

#### 证书查询统计

可按照多个维度对已签发证书进行查询统计，生成统计报表。

#### RA管理

管理下级RA节点，对节点进行注册、授权、冻结解冻等管理。

#### 子CA管理

支持设置子CA，可签发子CA根证书，并对子CA进行统一管理。

#### 证书模板管理

可自定义证书模板，用户可灵活配置证书自定义扩展项。

### 产品特点

#### PRODUCT FEATURES

#### 易用性

内置签名证书、加密证书、SSL站点证书等多种数字证书模板，并支持自定义。

#### 兼容性

支持多种目录服务器、数据库和操作系统，适配多厂家多型号的加密机、智能卡。

#### 适用性

支持页面发证和接口调用发证模式，提供对代理机构(LRA)的多级发证管理功能，适用不同发证场景。

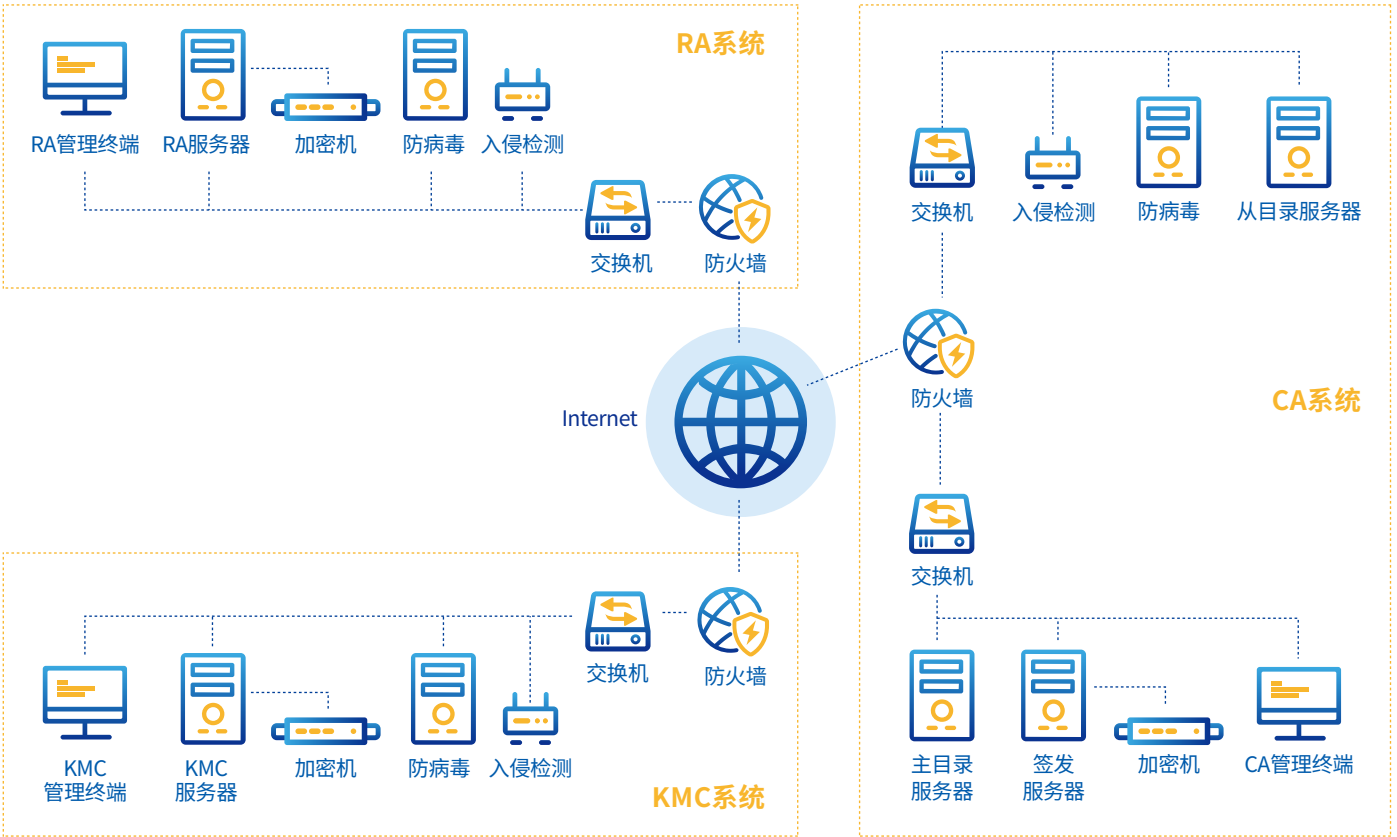
#### 稳定性

在税务领域、多个省级公共资源交易平台广泛应用，发证量巨大，运行稳定。

# 典型应用

## TYPICAL APPLICATIONS

航天科工集团部署了一套航天信息数字证书认证系统,该系统全面采用国产密码算法及集群部署,为全体系员工签发数字证书,实现集团内部应用的多因子身份认证。该系统制作的数字证书全面支持X86终端及国产终端,为科工集团应用提供了强有力的安全保障。



航天信息数字认证系统典型应用示意图

## 主要客户

MAJOR CUSTOMERS



西部CA



国资委



西藏CA



中国外运股份有限公司

## 产品资质

PRODUCT QUALIFICATION





## 统一密码服务平台

航天信息统一密码服务平台以密码运算为基础、密码设备为支撑、密码服务为思想、资源集中化管理为手段，屏蔽后台密码设备的多样性、指令的复杂性，实现业务系统的统一调用，为业务系统提供统一、安全、可扩展的密码服务，为密码设备提供集中化的管理与维护，是密码应用的核心产品。



### 产品功能

#### PRODUCT FUNCTION

##### 密码应用服务



提供透明数据库加密、文件加解密、安全代理通信、电子签章、手机盾、时间戳、身份认证等多种密码应用服务，方便业务系统快速实现密码应用改造。

##### 密码运算服务



提供加解密、签名验签、HASH、MAC等多种基础密码运算服务。

##### 密钥管理



提供海量用户的密钥安全管理，支持密钥生成、备份、恢复、导入、导出、销毁等全生命周期管理。

##### 密码资源管理



根据不同应用对密码资源的需求，基于虚拟化方式按需分配资源，有效利用密码资源。

##### 统一设备管理



适配多厂家、多类型密码设备，支持多种设备动态接入，对密码设备集中分配，实现资源池动态调度。

##### 密码态势感知



实时采集分析密码应用数据，以驾驶舱的形式多维度展示密码应用整体态势。

##### 云化技术支撑



提供高可用、动态扩展、负载均衡、流量控制、虚拟化等云化技术支撑。

##### 运营管理



面向多样化的客户及应用，提供统一、集中、可视化的运营管理。

### 产品特点

#### PRODUCT FEATURES

##### 运行机制可靠

采用动态扩展、负载均衡、流量控制、微服务等云化技术支撑，支持容器化、分布式部署，平台具备高可扩展、高可用、高稳定性。

##### 平台运行高安全

提供统一安全身份认证服务，确保接入用户、系统、资源的安全可信，通过密钥安全、通信安全、授权访问等机制保障平台服务安全。

##### 灵活可靠的密码资源池

支持服务器密码机/云密码机/签名验签服务器等多种类型的密码设备，无感动态调配应用的密码资源。

##### 实施建设低冗余

高度整合已有、新采密码设备，统一管理密码资源，有效避免密码运算资源浪费。

##### 全方位状态监控

对密码资源、服务、应用进行全方位监控，具备强大的数据分析能力。

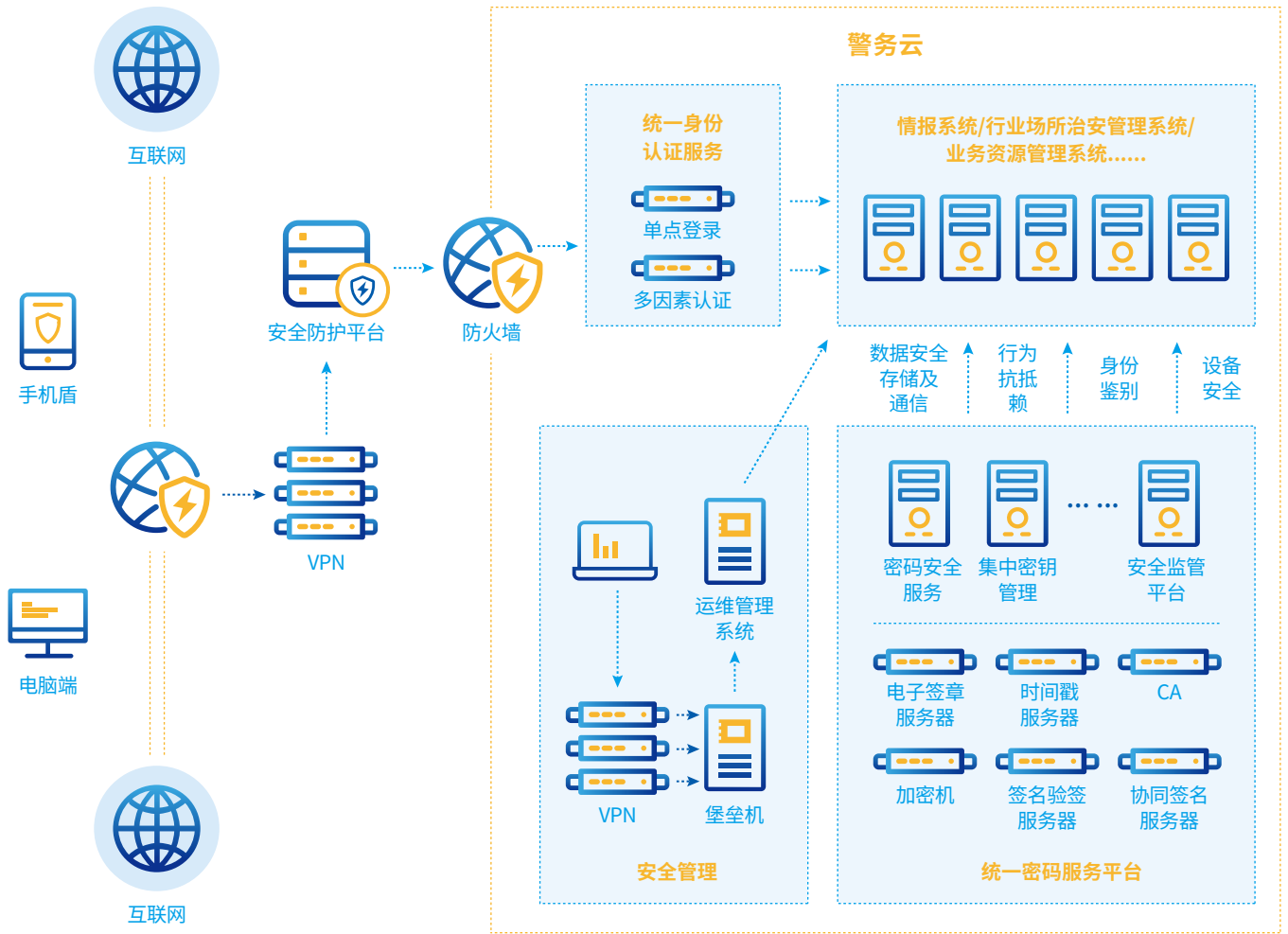
##### 透明化的密码服务

具备多种透明密码应用服务，应用系统可通过平台服务降低密码改造难度。

# 典型应用

## TYPICAL APPLICATIONS

统一密码服务平台为警务云平台提供身份认证、通信加密、数据加密、文件加密、签名验签等密码服务。



XX公安厅警务云平台

### 应用领域

#### APPLICATION FIELD

统一密码服务平台统筹管理接入,为大规模数量信息系统提供密码运算服务,主要包括:

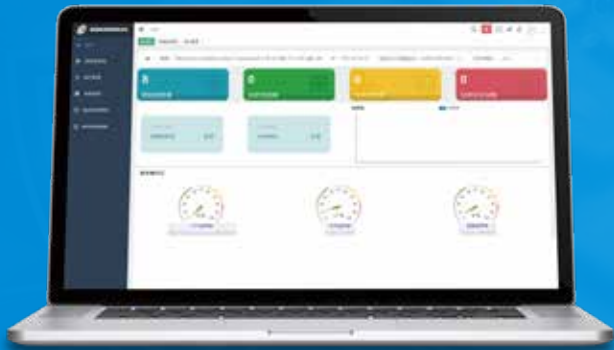
- 1 为省市级电子政务云平台提供密码服务,特点是拥有大量信息系统且安全要求高。
- 2 为大型央企提供密码服务,特点是拥有信息系统数量大、管理复杂、信息安全要求高。
- 3 为部委及行业提供密码服务,特点是企业和行业拥有大量下级单位且安全要求高。

### 产品荣誉

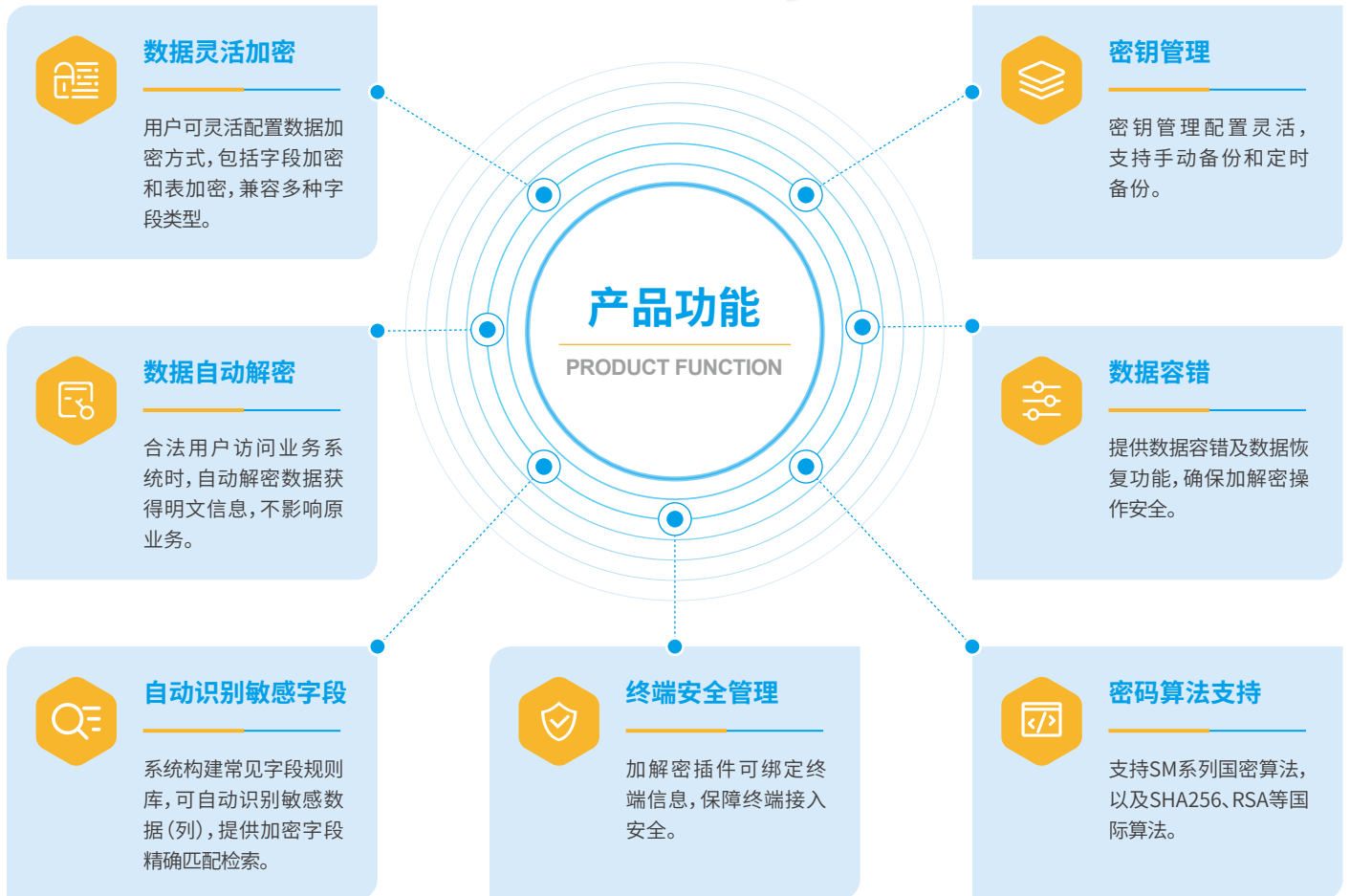
#### PRODUCTS HONOR



## 数据库透明加密系统



航天信息数据库透明加密系统针对敏感数据保护的政策要求和企业应用的需求,提供应用免改造、灵活部署、安全性能高的透明化数据加解密服务,解决数据库敏感数据面临的被窃取、篡改、泄露等安全问题,实现了数据库中加密字段精确检索和加密存储,保证数据全生命周期的安全。



# 产品特点

## PRODUCT FEATURES



### 高兼容性

支持MySQL、Oracle、PostgreSQL、MariaDB、SQLserver、达梦、金仓等多种关系型数据库。



### 应用免改造

业务系统无需修改源码，即可将应用数据的敏感字段按需配置，自动加密存储。



### 性能影响小

数据加解密过程几乎不影响原有业务性能。



### 集中管控

大规模部署统一管控，集中管理多套、多种类数据库。



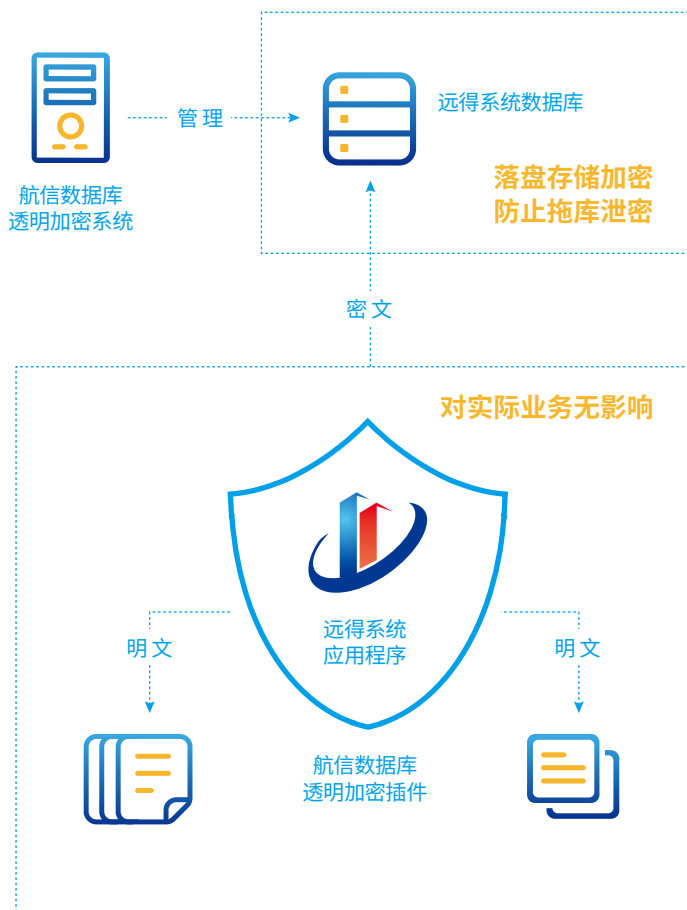
### 部署灵活

采用旁路部署方式，不影响原有业务，无需调整网络结构。

# 典型应用

## TYPICAL APPLICATIONS

远得销项发票智税管理系统采用SpringMVC+MySQL开发，在应用服务器端集成插件后，进行简单配置修改，即可对企业税号、银行信息、销项进项信息等敏感数据明文进行加密，保证数据安全。



id	address	clientbank
1620724346409118	地址118	IONJUCMOsO4/...
1620724346409146	地址146	IONJUCOLQvYA...
1620724346409153	地址153	IONJUCO4P5T4...

数据库直接读取、非法读取：  
保密字段clientbank为密文

id	address	clientbank
1620724346409118	地址118	银行卡账户118
1620724346409146	地址146	银行卡账户146
1620724346409153	地址153	银行卡账户153

有权限的内部数据读取：  
明文clientbank不影响系统业务

## 远得销项发票智税管理系统



## 统一身份认证系统

航天信息统一身份认证系统将业务系统中共性的用户登录功能抽象整合，基于密码安全技术形成集中式用户登录认证系统，实现“一次认证、多业务通行”的效果。系统支持口令、短信认证、生物特征识别、数字证书等多种安全认证机制，可为各信息化业务系统提供高性能的用户管理、统一接入、统一授权、统一认证、安全审计等服务。



## 产品特点

### PRODUCT FEATURES



#### 高安全性

敏感信息采用通信信道、数据双加密,短时效令牌一次一密,支持国密算法。



#### 兼容性强

兼容OAuth2.0、CAS等多种标准认证协议,支持linux、国产操作系统部署集成。



#### 高易用性

只需通过简单集成对接,低代码量的改造(10行左右),即可集成。



#### 适应性强

提供多种语言SDK包、API接口,以适应业务应用的认证需求。



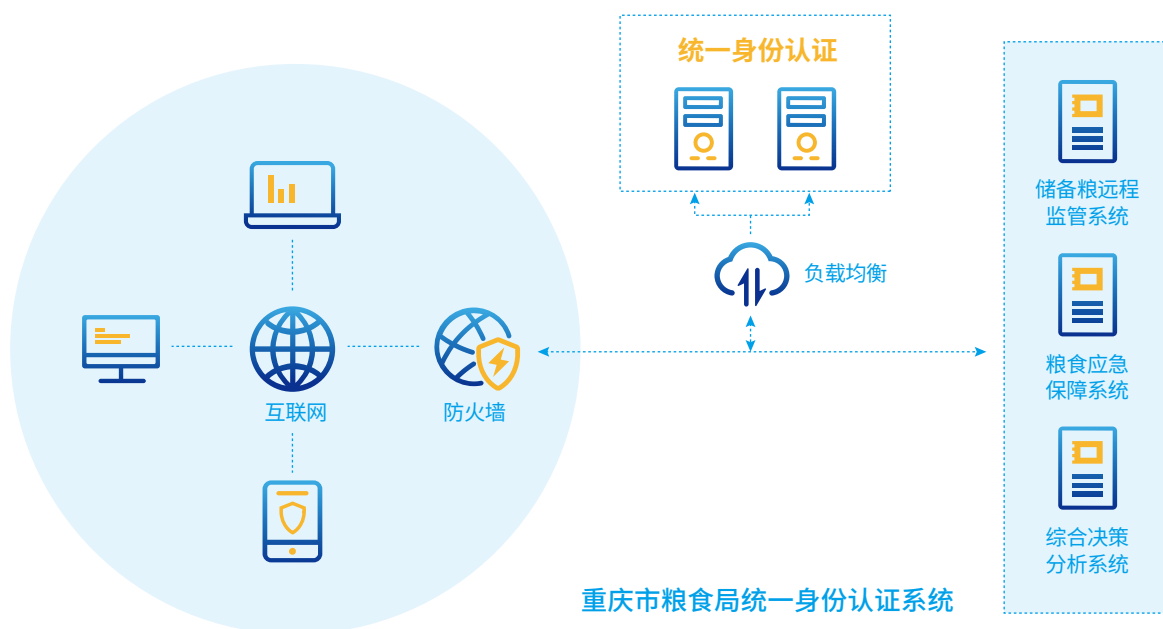
#### 高可用性

支持负载均衡和集群部署,有效规避单点故障风险。

## 典型应用

### TYPICAL APPLICATIONS

重庆市粮食局部署了航天信息统一身份认证系统,使用口令、短信验证码、数字证书等多认证方式,为约2000名用户提供统一身份认证服务,已实现10余个业务系统的集中登录认证,从安全性、易用性、可扩展性等方面有效提升了该单位的信息化安全服务能力。



## 主要客户

### MAJOR CUSTOMERS



工信部



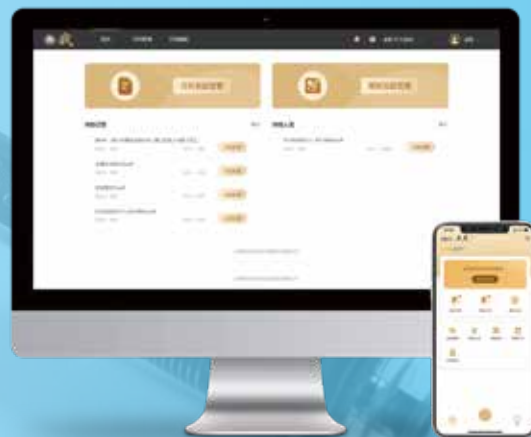
重庆市粮食局



天津市药监局

## 是我电子签名云平台

“是我”电子签名云平台是一套完整的全生态电子签名密码服务平台，是围绕可信数字身份构建的密码安全基础设施，可在多种应用场景中提供可信身份证明和可信行为证据，有效抗抵赖。平台基于手机盾和密码技术，构建电子签署等常用业务场景的密码应用，并支持安全便捷的API服务，满足用户多行业多场景下的安全需求。



“是我”应用页面

### 产品功能

#### PRODUCT FUNCTION



#### 认证服务

基于人脸识别技术，对接权威机构，支持在线真人认证与企业实名认证，实现快速精准核验，确保身份真实性。



#### 移动证书

对接权威CA机构签发数字证书，结合移动协同签名技术，完全体现数字证书持有人真实意愿。



#### 电子签名

安全可靠合规，具有法律效力，防篡改、抗抵赖，确保签署主体真实性。



#### 文档签署

采用可视化电子签署技术，易操作，支持多种签署顺序和流转模式，适用性强，满足多种需求。



#### 合同模板

支持创建版式合同文件，批量发起签署操作，便捷、快速、高效。



#### 考勤打卡

接入精准定位服务，结合安全可靠防作弊技术，确保打卡真实有效。



#### 签到登记

快速创建活动 and 登记表，基于电子签名技术进行扫码签到、登记。



#### 现场认证

运用移动证书、身份认证技术，随时随地出示安全可信电子身份证明。



#### 开放API接口

丰富的API接口，包括实名认证、电子合同、合同模板、扫码登录等能力，与业务系统快速集成。

# 产品特点

## PRODUCT FEATURES



### 抗抵赖性强

数字证书的密钥由持有人完全控制,体现用户意愿,使用证书进行数字签名时,可确保行为抗抵赖。



### 法律效力强

使用符合国家法规要求的电子签约流程与数字签名技术,确保电子合同合法有效。



### 安全系数高

用户数据安全脱敏存储,对接存证平台,操作证据保全。



### 对接方式广

支持“是我”应用对接,提供高效便捷易用的API服务,满足客户定制化集成需求。

# 应用领域

## APPLICATION FIELD

### 企业应用

电子合同、  
业务系统审批、  
会议签到、  
访客登记等。

### 人力资源

电子劳动合同、  
离职证明、  
收入证明等。

### 医疗行业

电子病历、  
知情同意书、  
电子处方等。

### 金融行业

电子保单、  
电子合同、  
电子交易等。

### 政务行业

办公审批、  
电子政务  
网上办事、  
电子身份证明等。

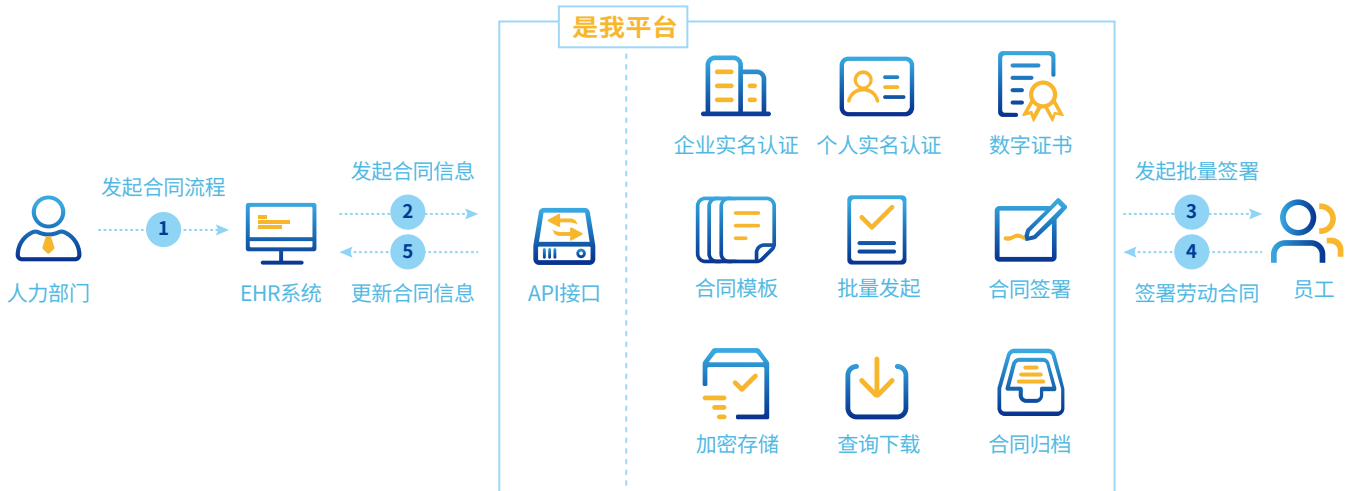
### 教育行业

电子成绩单、  
电子毕业证、  
家长知情  
同意书等。

# 典型应用

## TYPICAL APPLICATIONS

利用数字签名、身份认证、防篡改等信息安全技术,为电子合同提供完善的安全保证和坚实的法律保护。数字签名技术保障电子合同可靠性,使得其在签署后不可更改。符合《电子签名法》要求,确保电子合同具备与相应纸质合同具有同等法律效力,同时可提供电子签名验证报告,当出现纠纷或需要立案时,作为辅助材料提交给相关的仲裁机构或司法机构。



人力资源电子劳动合同解决方案

## 航天信息手机盾

航天信息手机盾产品旨在解决传统USBKey在移动互联网应用中使用不便的问题,使用手机替代USBKey,基于SM2的协同签名算法,将用户密钥碎片化处理,分别存储于移动端和云端,形成移动终端+云端的立体保护,确保用户密钥安全,同时提供易用和高安全性的数字证书和签名验签、加密解密等基础密码接口服务,产品具备国家密码管理局认定的安全二级密码模块资质。



协同签名原理示意图

### 产品功能

#### PRODUCT FUNCTION



#### 证书管理

手机盾SDK提供全生命周期的移动数字证书管理功能,包括生成证书请求、证书导入、证书更新、删除证书、证书查验等,支持双证书。



#### 签名验签

基于协同签名技术实现SM2协同密钥生成、协同签名、协同解密等功能,支持标准SM2验签和加密。



#### 国密算法

手机盾SDK支持SM3、SM4国密算法并提供应用接口。



#### 安全环境检测

基于ROOT或越狱检测、防调试等移动安全监测技术,确保手机盾所在移动端为安全运行环境。



#### 密钥管理

管理端支持用户密钥的冻结、解冻管理,可对异常状态的用户密钥进行冻结,确保密钥使用安全。



# 产品特点

## PRODUCT FEATURES

### 密钥安全

基于SM2的密钥分片、协同签名技术，在密码运算和存储阶段均不合成原始私钥，有效保护用户密钥安全。

### 通信安全

基于国密SSL，确保移动端数据通信安全。

### 数据安全

使用SM4白盒技术有效隐藏加密密钥，保护移动端用户敏感数据。

### 认证安全

支持PIN码认证和生物识别快速认证（指纹/面部识别）。

### 输入安全

敏感数据采用安全软键盘输入，键盘字符随机混排，输入字符加密，输入无明文和触控回显，防截屏录屏。

### 设备安全

采用移动设备特征识别技术，有效防止设备克隆。

### 应用安全

使用移动安全加固技术，有效抵御动态和静态攻击。

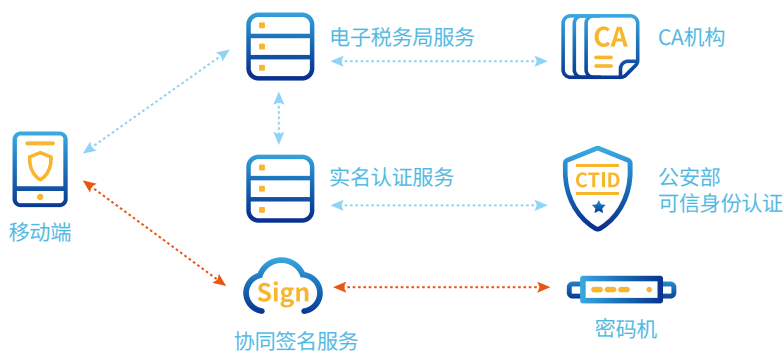
### 全面兼容

通过扫码签名方式，将移动端的手机盾安全能力扩展到传统PC端。

## 典型应用

### TYPICAL APPLICATIONS

移动实名办税App集成航天信息手机盾SDK，为实名认证通过的用户签发数字证书，该证书可代表此用户的实名身份。用户在后续移动办税过程中，使用数字证书对业务进行数字签名，保证业务数据的完整性、真实性和不可抵赖性。



移动实名办税系统

## 主要客户

### MAJOR CUSTOMERS



安徽省国税局



甘肃省林草局



山东卓码

## 荣誉资质

### HONORARY CERTIFICATE



航天信息医用签APP针对医疗行业的电子认证需求,基于手机盾和电子签章技术实现。医护人员和病患可直接使用手机设备对电子病历、检验报告、知情同意书等医疗文件进行安全可靠的电子签名或签章,确保医疗数据具备法律效力。



### 医用签APP界面

APP INTERFACE

### 产品功能

PRODUCT FUNCTION

#### 移动证书

医护人员可使用手机验证码、人脸比对等方式在线完成身份认证,一键申请个人专属数字证书,此证书用于医疗文书的电子签名、电子签章和业务系统授权登录等操作。

#### 时间可信

基于国家授时中心权威时间源,采用时间戳技术对医疗信息系统的任何操作加盖可信时间戳,为医疗信息系统提供权威、精准和可信时间认证服务,以确保操作记录的时间可靠性。

#### 患者签名

可短信通知病患或家属在移动端预览待签署的知情同意书、手术通知单等,在线实名认证并采集手写签名笔迹完成签署。

#### 医护签章

为医护人员提供推送签章、扫码签章、批量签章等签署模式,满足医院内各类电子文书的签署需求。

#### 授权登录

医生可通过扫码,快捷登录PC端各业务系统,实现基于数字证书的安全登录认证,无需记忆各系统繁琐的密码。

#### 用户管理

用户管理员权限根据院区分级设置,可对辖区用户进行全生命周期的管理,包括预导入、停用激活、禁用等。

# 产品特点

## PRODUCT FEATURES



### 使用便捷

使用手机、PAD在线完成身份认证及电子签名操作，避免USBkey申领遗失补办等管理成本高、使用不便的问题。



### 部署灵活

医用签支持云服务接入、私有化、部分私有化部署方式，使用云服务接入时，医疗数据原文仅需在医院内网的前置服务器处理，有效保护医疗数据安全。



### 省时高效

使用电子签名代替传统纸质签名，节约办公资源、提升医院业务流转效率，便于存档和查阅。



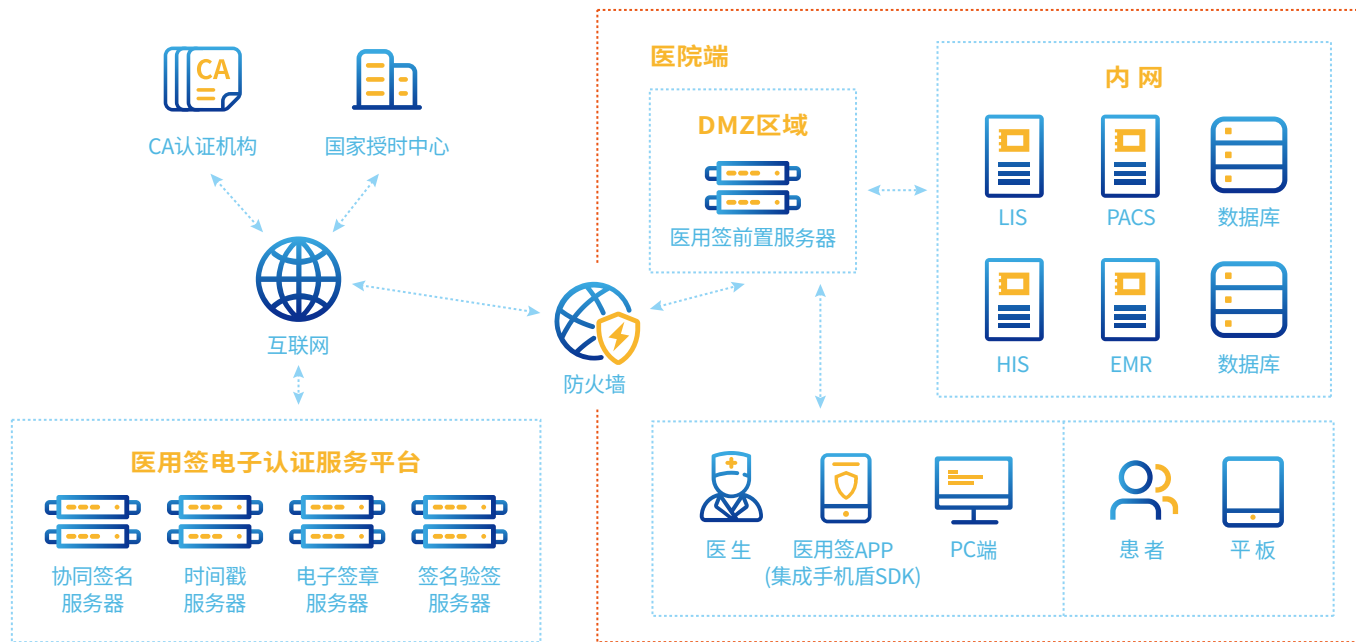
### 应用广泛

基于网络既适用于医院传统内网诊疗业务，也可应用于互联网医院场景。

# 典型应用

## TYPICAL APPLICATIONS

康宁医院通过部署航天信息医用签前置服务器，快速引入了医用签电子认证云服务，目前已对接院内HIS、LIS、RIS等信息系统。医护人员使用个人手机对电子病历、检验报告等医疗文件进行电子签章，病患及家属使用科室公用的PAD设备预览并签署知情同意书等文件，审核通过的待归档PDF病案自动进行机构归档签章并完成归档，满足了医院提高诊疗效率、降低诊疗成本以及电子病历系统评级的需求。



康宁医院医用签系统部署图

## 主要客户

MAJOR CUSTOMERS



温州卫健委



康宁医院

共聚智慧 共享安全 共创美好

航天信息股份有限公司

地址:北京市海淀区杏石口路甲18号 邮编:100195  
电话:(+8610)88896666 传真:(+8610)88896888