高速密码应用

助力数据安全

鹿淑煜

三未信安科技股份有限公司

Sansec Technology Company ., Ltd

数据安全政策与驱动

2017

《信息技术安全 个人信息安全规范》

规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度保障个人的合法权益和社会公共利益。

2018

《通用数据保护条例》（GDPR）

欧洲“史上最严”的数据保护条例——《通用数据保护条例》，针对欧洲自然人数据的管理和安全问题进行了规范的欧盟新规，GDPR给所有欧盟自然人保护自己个人资料提供了法律依据。

2019

《数据安全管理办法》（征求意见稿）

为维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全，由国家互联网信息办公室会同相关部门研究起草关于数据安全管理办法

2020

《数据安全法》制定

6月28日，数据安全法草案提请十三届全国人大常委会第二十次会议初次审议，按照总体国家安全观的要求，确立数据安全保护管理各项基本制度，提升国家数据安全保障能力，

数据安全威胁与密码学工具

数据安全面临的威胁

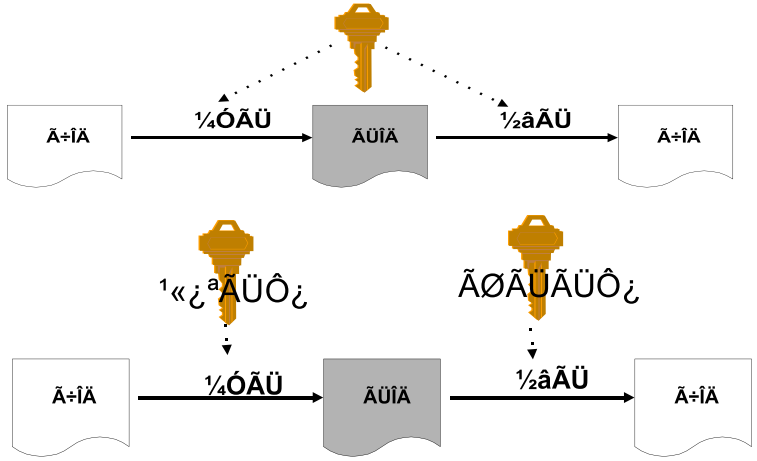
- 窃听（秘密泄露）
- 篡改（信息被修改）
- 伪装（伪装成真正的发送者）
- 否认（事后称自己没有做）

密码技术特性

- 机密性
- 完整性
- 真实性
- 不可否认性

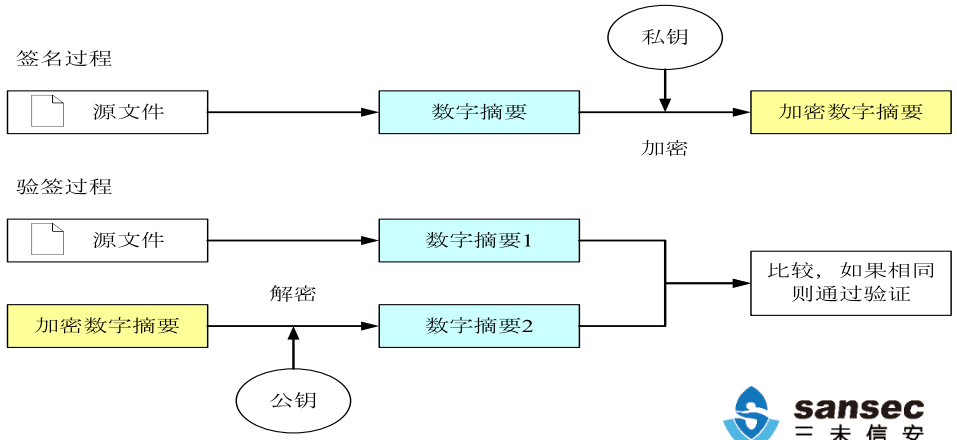
密码学工具

- 随机数生成
- 对称密码
- 非对称密码
- 单项散列函数
- 消息认证码
- 数字签名



（1）单向性（2）一一对应（3）定长输出

一种基于单向散列函数或对称密码的计算方法



sansec 三未信安

密码保障能力与合规要求

商用密码应用技术保障

密码安全技术保障

密码管理基础设施：密钥管理 / 信任管理 / 设备管理 / 运维管理

密码应用
- 采集数据保护
- 传输数据保护
- 存储数据保护
- 安全电子签章
- 安全电子邮件
- 统一身份鉴别
- 关键操作抗抵赖
- 其他
- 密码应用场景

密码服务
- 密码运算服务
- 安全认证服务
- 密钥管理服务
- 签名验签服务
- 完整性校验服务
- 证书管理服务
- 对内密码服务接口
- 对外密码服务接口

密码支撑
- 软件类
- 芯片类
- 背板模块类
- 办卡类
- 整机类
- 系统类
- 密码算法类
- 数据加解密类
- 认证鉴别类
- 证书管理类
- 密钥管理类
- 密码防伪类
- 综合类
- 密码产品
- 集成&联动
- 密码服务

密码资源
- 算法软件
- 算法IP
- 算法芯片
- 其他
- 序列算法
- 对称算法
- 公钥算法
- 杂凑算法
- 其他
- 基础密码算法

密码安全合规要求

技术要求

密码模块	采用符合相关标准要求的密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理
应用与数据安全	数据传输 / 数据存储 / 访问控制信息 / 日志记录 / 身份鉴别 / 应用程序安全控制
设备和计算安全	远程管理 / 访问控制信息 / 敏感标记 / 日志记录 / 身份鉴别 / 重要可执行程序完整性
网络和通信安全	通信过程中的敏感字段或通信报文 / 集中管控/ 通信数据 / 网络边界访问控制 / 身份鉴别/设备准入认证
物理和环境安全	身份鉴别 / 电子门禁进出记录 / 视频监控音像记录

安全管理
- 管理制度
- 人员管理
- 建设运行
- 应急处置

密钥管理
- 密钥生成
- 密钥使用
- 密钥分发
- 密钥归档
- 密钥存储
- 密钥销毁
- 备份与恢复
- 导入与导出

技术挑战与多维度场景需求

当前数据安全面临的主要十大技术挑战包括

- 分布式编程框架中的安全计算；
- 大数据计算框架的数据流安全；
- **非关系数据库的海量数据存储安全；**
- 审计日志的安全；
- 端点输入验证 / 过滤；
- 基于大数据的实时安全监控；
- **可扩展和可组合的隐私保护数据挖掘和分析；**
- **大数据的加密存储；**
- **细粒度访问控制；**
- **细粒度审计；**
- **数据流溯源。**

机密性

传输的重要数据、敏感字段或通信报文
存储的重要数据和敏感信息
身份鉴别信息
密钥数据

完整性

进入重要物理区域人员
通信双方实体
网络设备接入
登录操作系统和数据库系统
应用系统的用户

真实性

传输的重要数据、敏感信息或通信报文
存储的重要数据、文件和敏感信息
身份鉴别信息
密钥数据
日志记录
访问控制信息
重要信息资源安全标记
重要可执行程序
用可信计算技术建立视频监控音像记录
电子门禁系统进出记录

不可否认性

数据原发证据
数据接收证据等

以《GM/T0054 信息系统密码应用基本要求》中的密码应用场景为例

举例1：大数据安全环境下提出了高性能数据安全（加密）需求

当今社会进入大数据时代，越来越多的数据共享开放，交叉使用。针对关键信息基础设施缺乏保护、敏感数据泄露严重、信息访问权限混乱、个人敏感信息滥用等问题，急需通过加强网络空间安全保障、做好关键信息基础设施保护、强化数据加密、保护个人敏感信息等手段，保障大数据背景下的数据安全。大数据应用涉及到采集、传输、存储、处理、交换、销毁等各个环节，每个环节都面临不同的安全威胁，需要采取不同的安全防护措施，确保数据在各个环节的保密性、完整性、可用性，并且要采取分级分类、 去标识化、脱敏等方法保护用户个人信息安全。

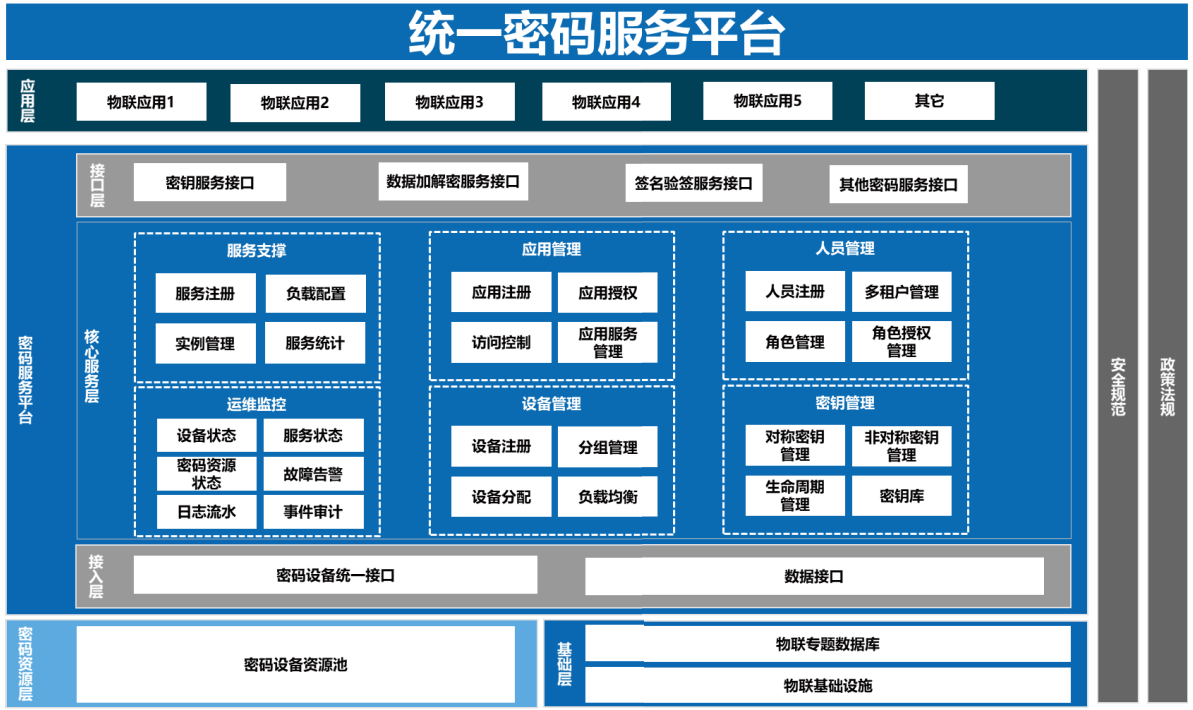
密码解决什么样的大数据安全需求

- **大数据平台**：密码技术的认证功能可以增强大数据平台组件间的身份认证或对Kerberos认证做安全加固
- **数据本身**：密码技术可以保证大数据平台上所承载的各类海量数据的机密性和完整性。

大数据安全中的密码应用有哪些新的需求

- **高性能数据加密**：传统的基于硬件密码产品进行集中加解密的方式已无法满足日益增长的海量数据的加密需求。
- **海量密钥集中管理**：目前大数据平台中缺乏统一集中的密钥管理体系，无法满足密钥集中管理的运维需求。
- **高安全的密钥管理**：目前大数据平台中多采用伪随机数生成密钥，并采用文件形式存储密钥，无法满足在生产环境下的业务安全性需要
- **密码应用合规**：目前大数据平台中的密码算法和协议均采用国际算法和标准，无法满足我国目前的网络安全相关规定

举例2：多类型、异构化的底层支撑设备乱象，证明统一密码服务能力亟待提升

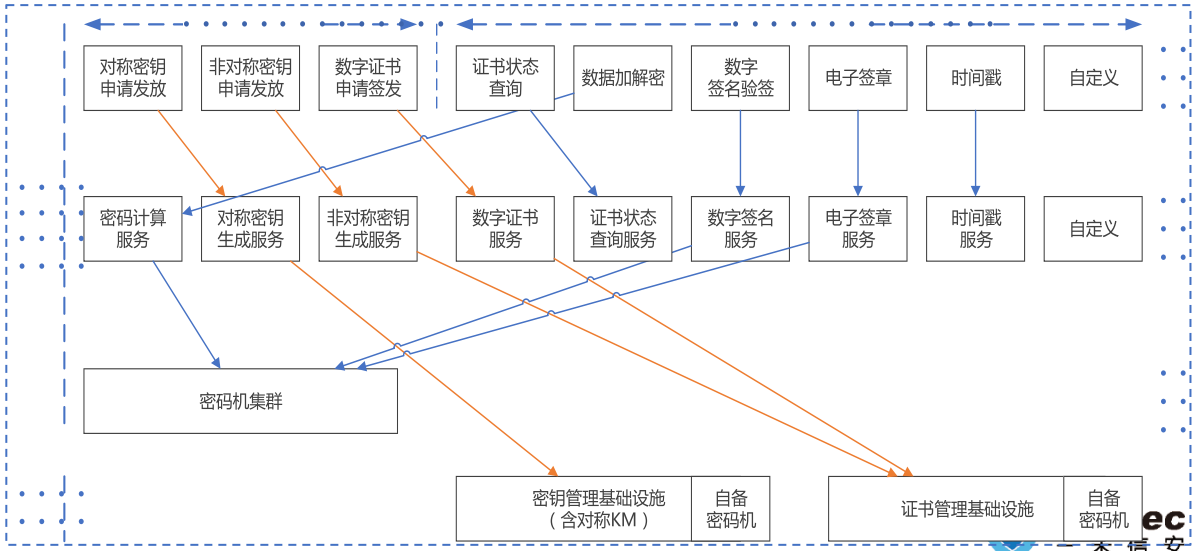


统一密码服务平台

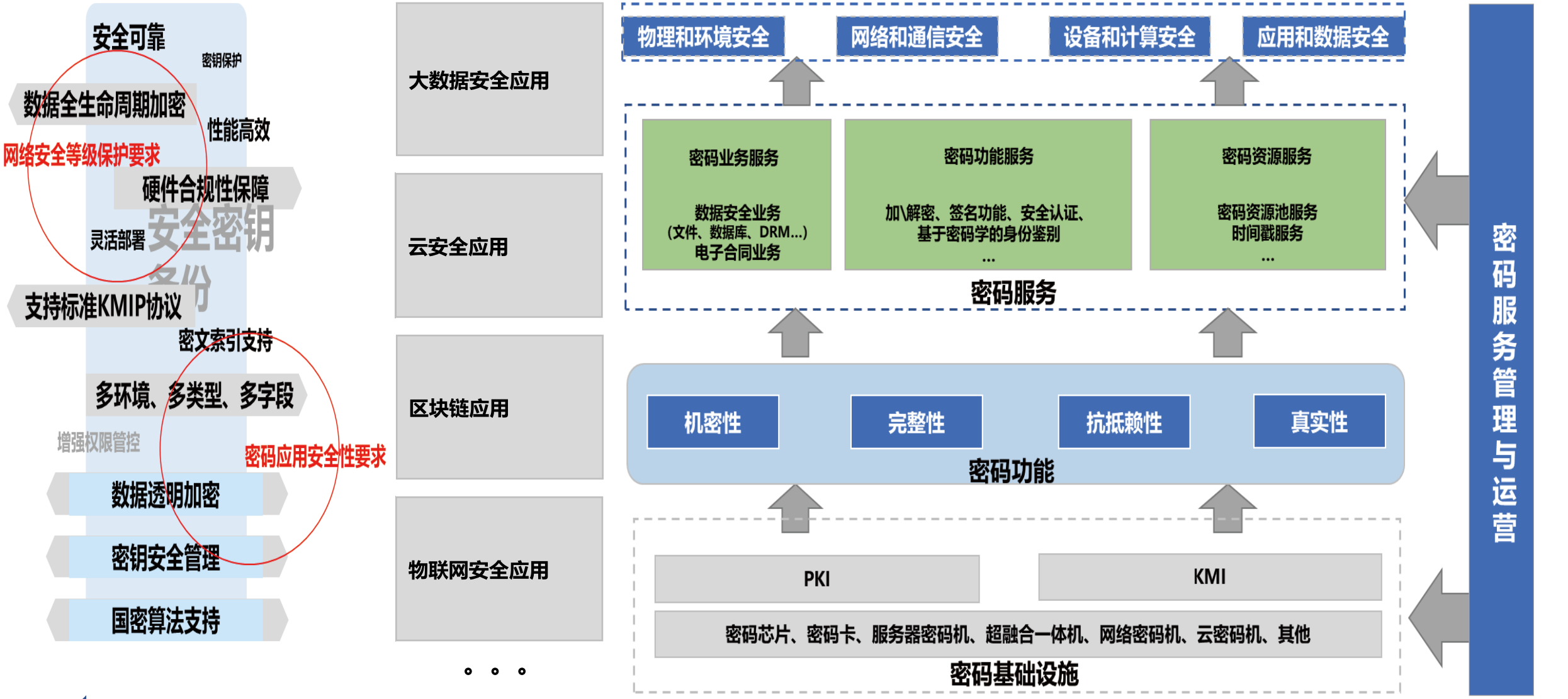
统一密码服务平台是**对现有商用密码管理体系的继承和发展**，由密码基础设施和密码服务平台（含密码服务组件）组成。密码基础设施管理对称密钥和非对称数字证书，并通过密码服务平台**对上层多种业务提供统一密码服务**

商用密码基础设施应用瓶颈：

1. 密码技术和设备**种类繁多**，没有统一的接口和标准导致应用和开发的成本巨大；
2. 个别业务独占硬件设备，导致加密机重复投资，**运算资源浪费**，运维管理困难；
3. 专业程度不同，业务对于**加密服务的使用缺乏专业指导**，存在一定的安全隐患；
4. 密钥管理和使用**分散**，用户需要自己维护密钥与业务，与密码设备之间的关系，繁琐且存在安全风险；
5. 多种密码设备管理的可信性问题、如何**安全高效**的使用密码服务的问题。



总结1：密码保障体系的不断健全,催生多样化的高速密码应用场景

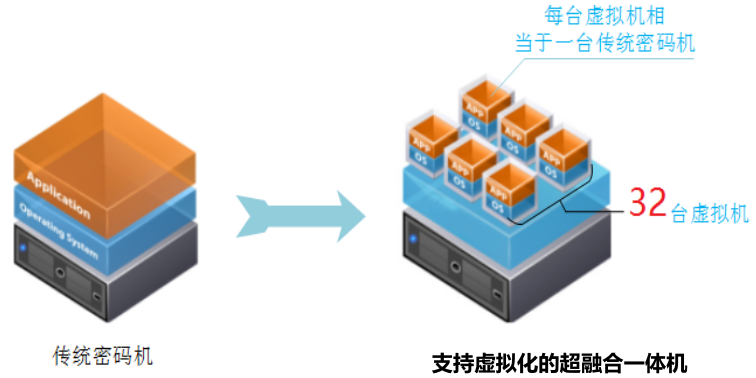


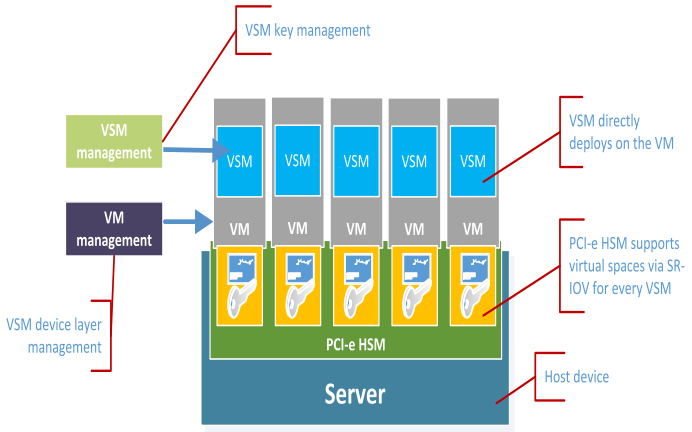
多场景 衍生 多技术领域 应用 逐渐健全的密码技术保障体系

sansec 三未信安

总结2：密码应用需求的多样化，促进了高速密码基础设施的发展

超融合密码资源池通过虚拟化技术将多种密码应用产品进行灵活部署、弹性扩展、集群负载的安全密码应用，产品具备统一的综合运维管理能力，可实现资源、策略、权限的集中管理，提高了密码应用的部署交付能力，可实现系统建设中安全能力的快速构建与灵活扩展。





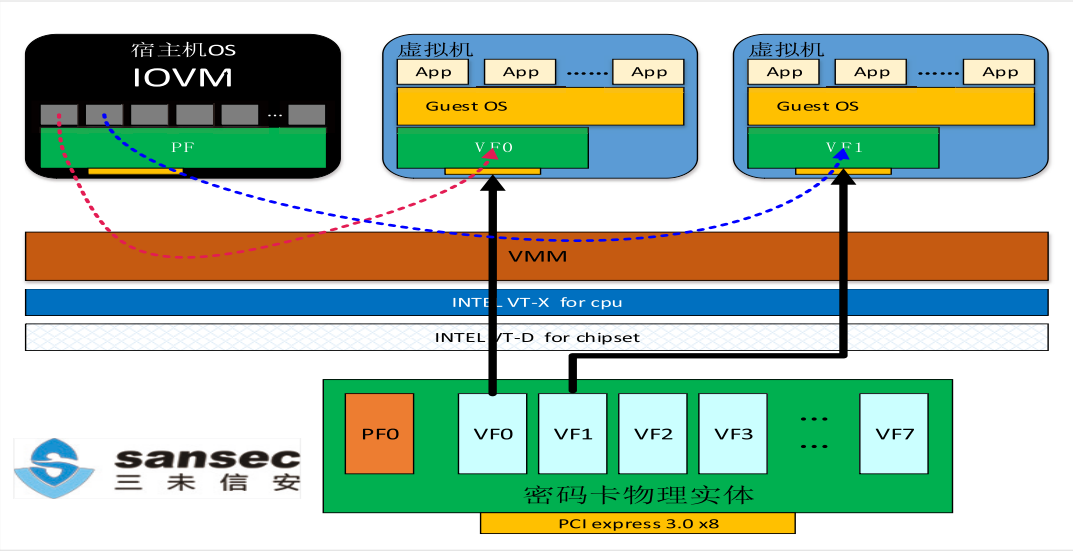
高速密码基础设施

一体化交付方案

sansec 三未信安

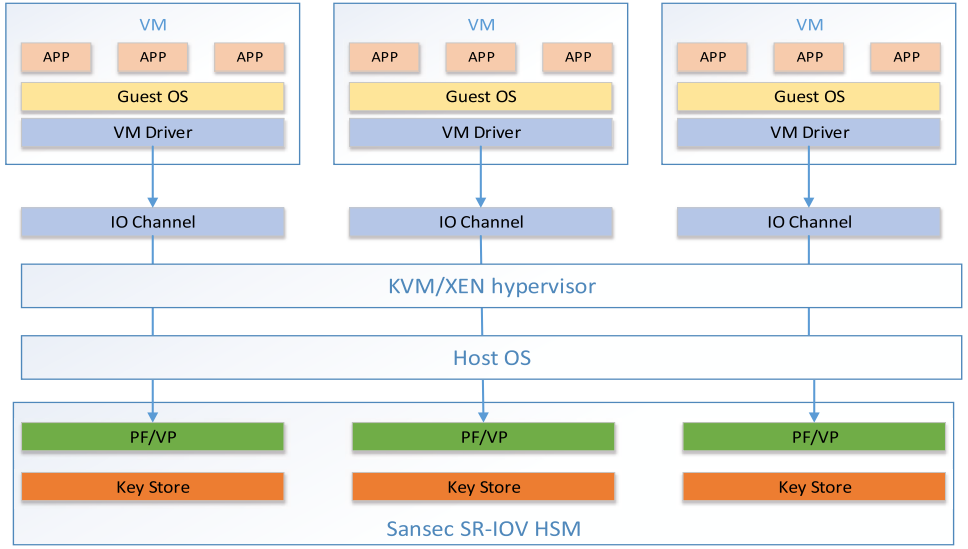
安全实践1-高性能的底层密码运算支撑

为确保密码算法的自主可控，降低敏感信息泄露和信息系统遭受攻击的风险，国家密码管理局制定并发布了国产加密算法及相关密码行业标准。但相对于国外的同类密码算法，市场上现存的国产密码算法芯片在运算速度的明显慢于国外密码算法芯片，难以满足日益增长的**海量数据加解密速度要求**。因此，首先要实现国产密码算法的FPGA高速实现，突破当前所用国产密码算法芯片处理速度慢的瓶颈，以解决目前市场所用国产密码芯片运算速度低的问题。



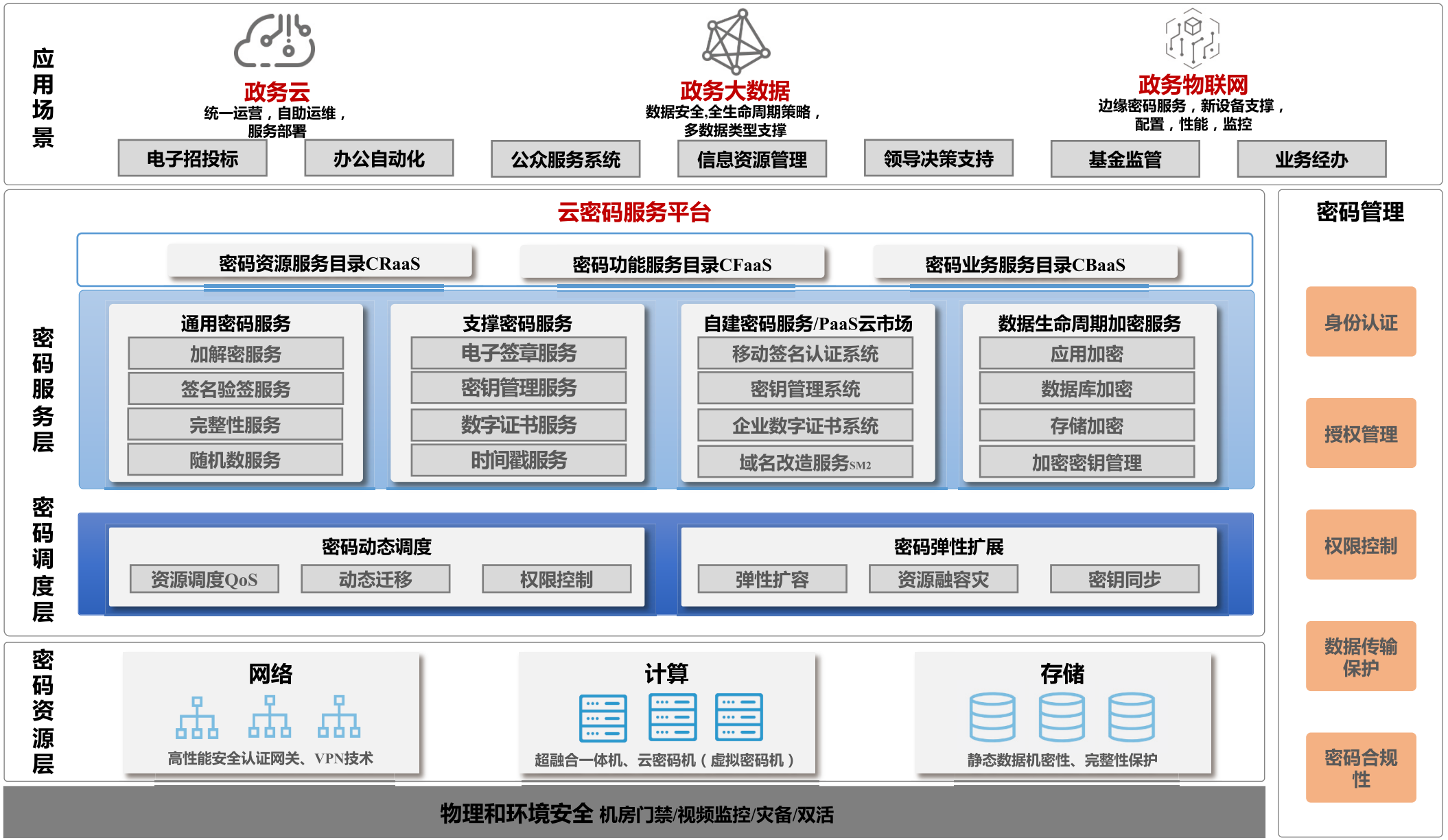
多VF方式高速密码卡结构设计

设计理念



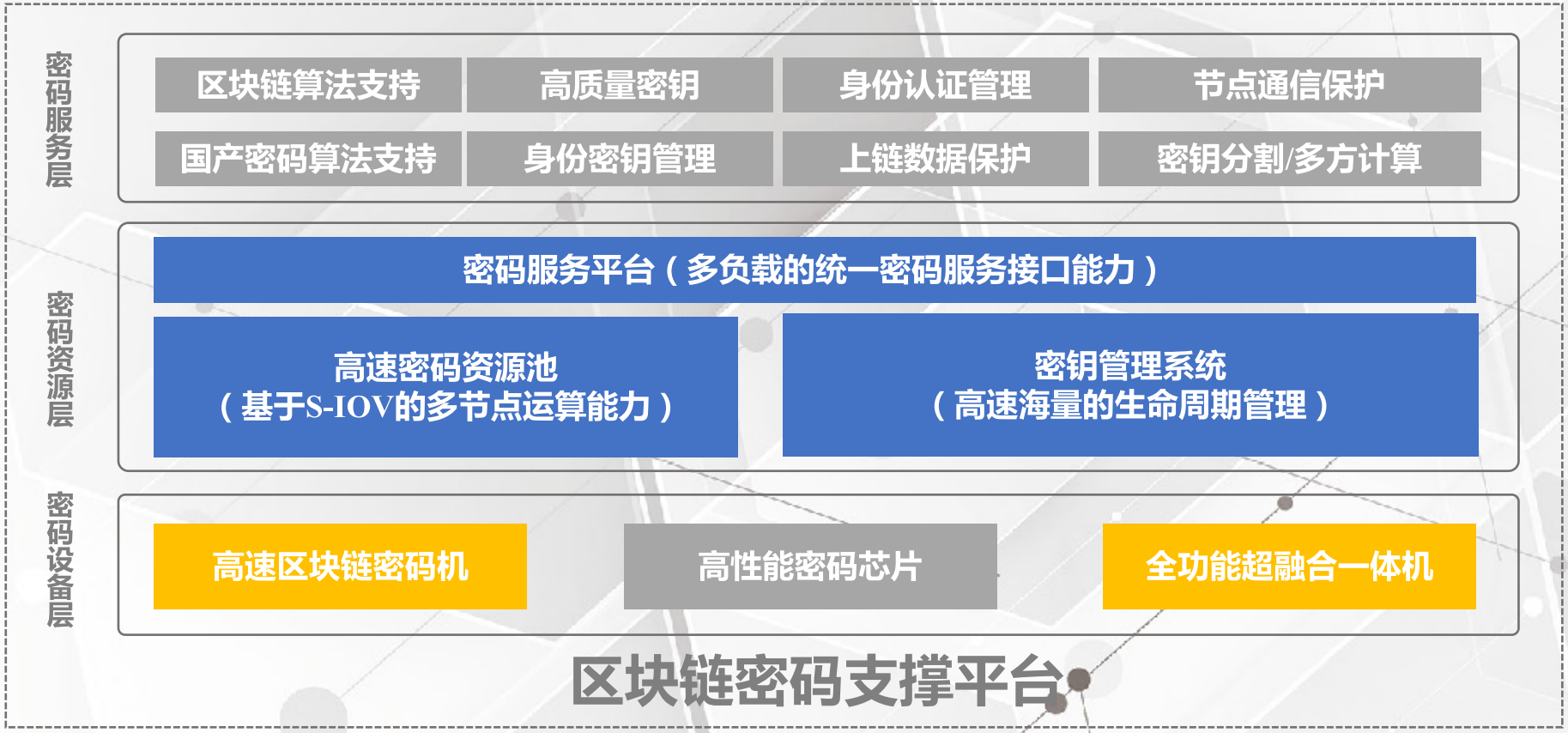
多PF方式高速密码卡结构设计

安全实践2-基于弹性负载的高速云密码服务支撑



安全实践3-基于融合架构的区块链密码平台支撑

区块链平台依靠密码资源层为平台提供安全、合规、高性能的密码资源及服务，使用符合国家密码管理局监管要求的密码设备为支撑。密码资源层提供的安全能力覆盖密钥的安全生成与存储、密钥的运算，以及终端设备的密钥存储安全性及密钥运算安全性。



安全实践4-IoT 物联网密码技术保障

物联网中大量的需要密码保护云端、管理端、设备端的交互和联系。

保证身份的可信　保证通道的可信

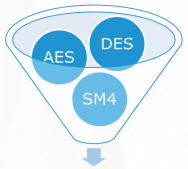
保证数据的可信　保证终端的可信

安全运营商和IoT制造商　数据安全存储

终端加密保护（密码白盒）　数据应用安全

认证授权控制　终端离线认证

安全数据通信　SOC安全调试



多算法支持


密钥动态更新

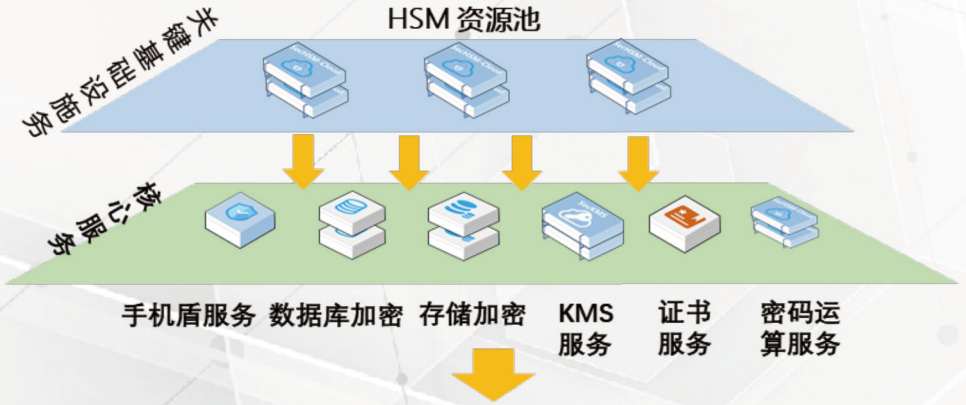
多平台支持


设备绑定

高速密码服务

轻量级密码算法&协议

多类型密码运算模块

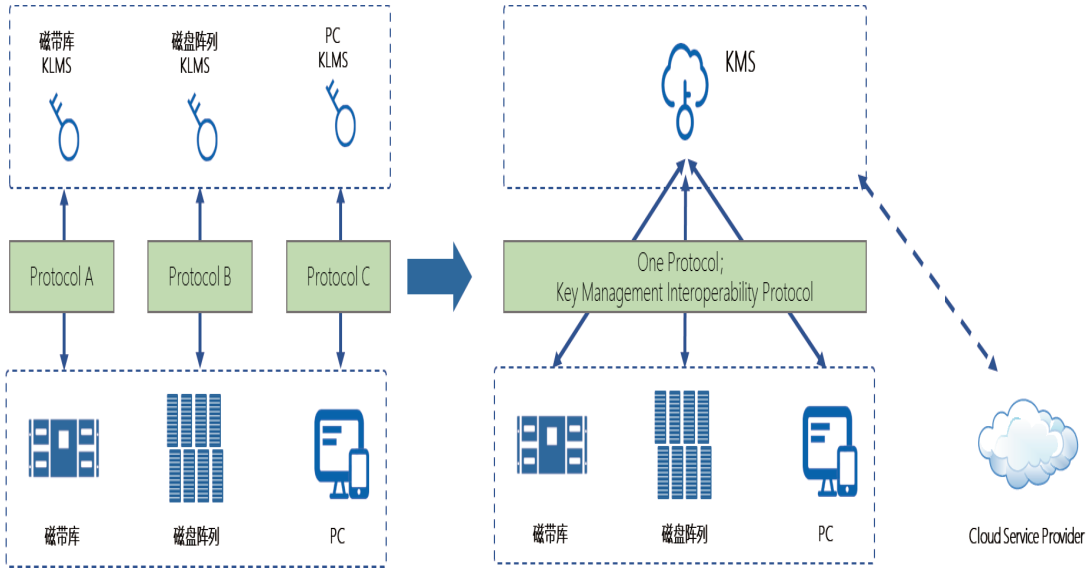





安全实践5-大数据环境下的海量密钥管理与数据保护

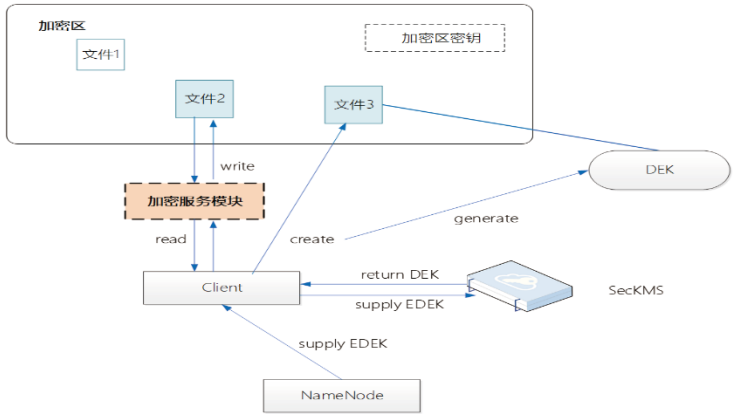
密钥全生命周期的管理包括：密钥生成、存储、分发、导入/导出、备份/恢复、归档和销毁等环节。SecKMS，作为企业级密钥管理系统，尤其适用多个具有不同密管接口的加密使用场景，兼容云环境和传统IDC。

基于KMIP（Key Management Interoperability Protocol）协议进行密钥全生命周期的管理。密钥生成、导入、获取数可达5000W，KMIP协议管理密钥量达40W。

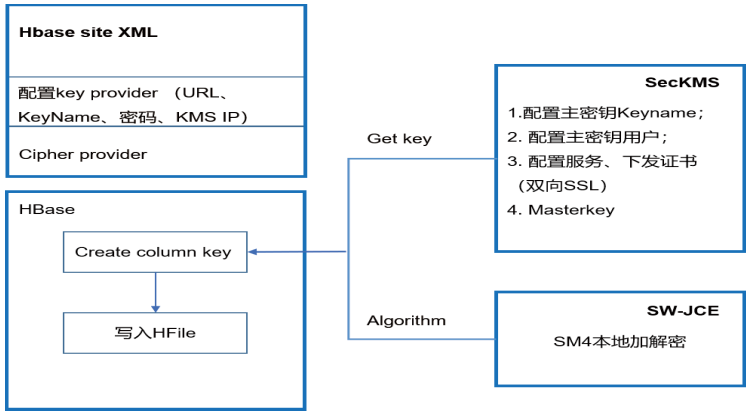


基于KMIP协议的通信标准化能力

面向HDFS组件的
非结构化数据保护



面向Hbase的
结构化数据保护



针对Hadoop大数环境的数据加密安全解决方案，以数据存储为核心保护环节，实现面向HDFS、Hbase的高性能密码支撑能力。

sansec
三未信安

Thanks

三未信安　　您身边的密码服务专家