2016阿里安全峰会
2016 ALI SECURITY SUMMIT

高志权

三未信安 副总经理

基于密码技术的
云数据全生命周期保护

sansec 三未信安

云加密的领跑者

北京三未信安科技发展有限公司

- ➔成立于2008年8月
- ➔注册资金2000万元人民币
- ➔总部位于北京，在济南设有研发中心
- ➔商用密码产品生产定点单位
- ➔商用密码产品销售许可单位
- ➔信安标委成员单位
- ➔密码行业标准化技术委员会成员单位
- ➔现有员工130余人，其中博士6人，硕士20余人，研发人员占50%以上
- ➔与山东大学计算机学院共建了联合实验室，产、学、研合作，联合实验室有博、硕士十多人


商用密码产品生产定点单位证书

（国密局产字 SSC499 号）

北京三未信安科技发展有限公司：

兹批准你单位为商用密码产品生产定点单位。

生产范围：经国家密码管理机构批准的商用密码产品的开发，生产。

本证书有效期 3 年。自 2008 年 10 月 31 日至 2011 年 10 月 31 日。

特发此证。

国家密码管理局

2008 年 10 月 31 日


商用密码产品销售许可证

（国密局销字 SXS939 号）

单位名称：北京三未信安科技发展有限公司

经营范围：销售经国家密码管理局审批并通过指定检测机构产品质量检测的商用密码产品。

有 效 期：2009 年 2 月 19 日至 2012 年 2 月 19 日。

国家密码管理局

2009 年 2 月 19 日


荣誉证书

HONORARY CREDENTIAL

为表彰在密码科学技术工作中做出重大贡献，特颁发此证书，以资鼓励。

获奖项目：三未信安 PCI 密码卡及密码机
获奖单位：北京三未信安科技发展有限公司
奖励种类：科技进步奖
奖励等级：三等（省部级）
证 书 号：2011-MJ-32

密码科学技术进步奖励委员会
2011 年 12 月


荣誉证书

HONORARY CREDENTIAL

为表彰在密码科学技术工作中做出的重大贡献，特颁发此证书，以资鼓励。

获奖项目：SRJ1203 签名验证服务器
获奖单位：北京三未信安科技发展有限公司
奖励种类：科技进步奖
奖励等级：三等（省部级）
证 书 号：2013-MJ-21

密码科学技术进步奖励委员会
2013 年 12 月


北京市产品评价中心
Beijing Products Evaluation Center

证书

项目名称：三未信安 PCI 密码卡及密码机
主要完成单位：北京三未信安科技发展有限公司
主要完成人：张信公、程希敏、高志权、张玉国、李风杰、王永峰

被评选为 2013 年北京市产品评价中心产品质量创新贡献奖——创新成果奖

优秀奖

证书编号：BPEC-2013-013
有效查询：www.bpec.org.cn

北京市产品评价中心
二〇一三年十一月


质量管理体系认证证书

兹证明

北京三未信安科技发展有限公司

BCC IAF CNAS


信息安全管理体系认证证书

兹证明

北京三未信安科技发展有限公司

BCC CNAS

云数据的安全问题

- 边界安全防护思想不能适应云环境
- 攻击手段日益多样化、差异化
- 封、堵、查、杀的被动防御是防不胜防的
- 云中管理员拥有更大的权利

云计算面临的技术挑战

- 缺少安全根基
- 大数据、高并发的性能需求
- 国家对自主可控的要求
- 合规性和数据隐私

密码技术的优势

密码技术是有系统理论基础的技术

密码技术是主动的安全技术

密码技术可在各个层面实施

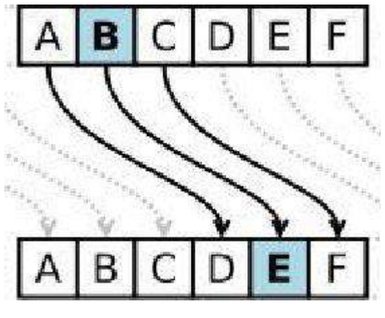
密码技术和数据的处理紧密结合，符合纵深保护策略

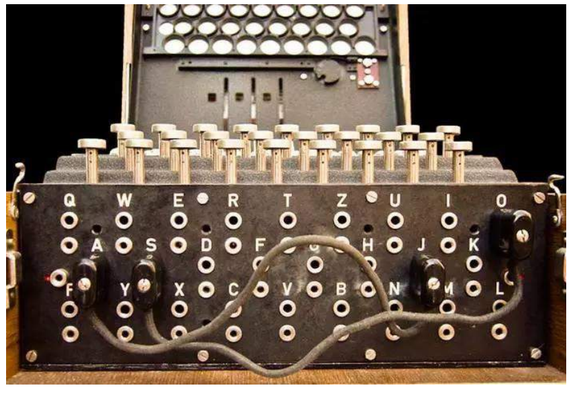
什么是密码？

密码？Password？Cryptographic！
密码已死？Passwords Are Dead！

对称加密？非对称密码？AES，DES，RSA，DSA，ECC，ECDSA，SM2/3/4，SHA，MD5，DH，MAC，HMAC，ECB，CBC，CFB，OFB，XTR，CTR…
PKI？数字证书？数字签名？SSL/TLS？HTTPS?

Diffie和Hellman为什么获图灵奖?





密码的作用

机密性

- 数据加密

完整性

- HASH
- 消息鉴别码MAC

身份鉴别

- 数字证书

不可否认性

- 数字签名
- 《电子签名法》

密码产品分类

密码算法芯片

随机数生成器

密码处理器芯片

密码算法软件

密码处理器软件

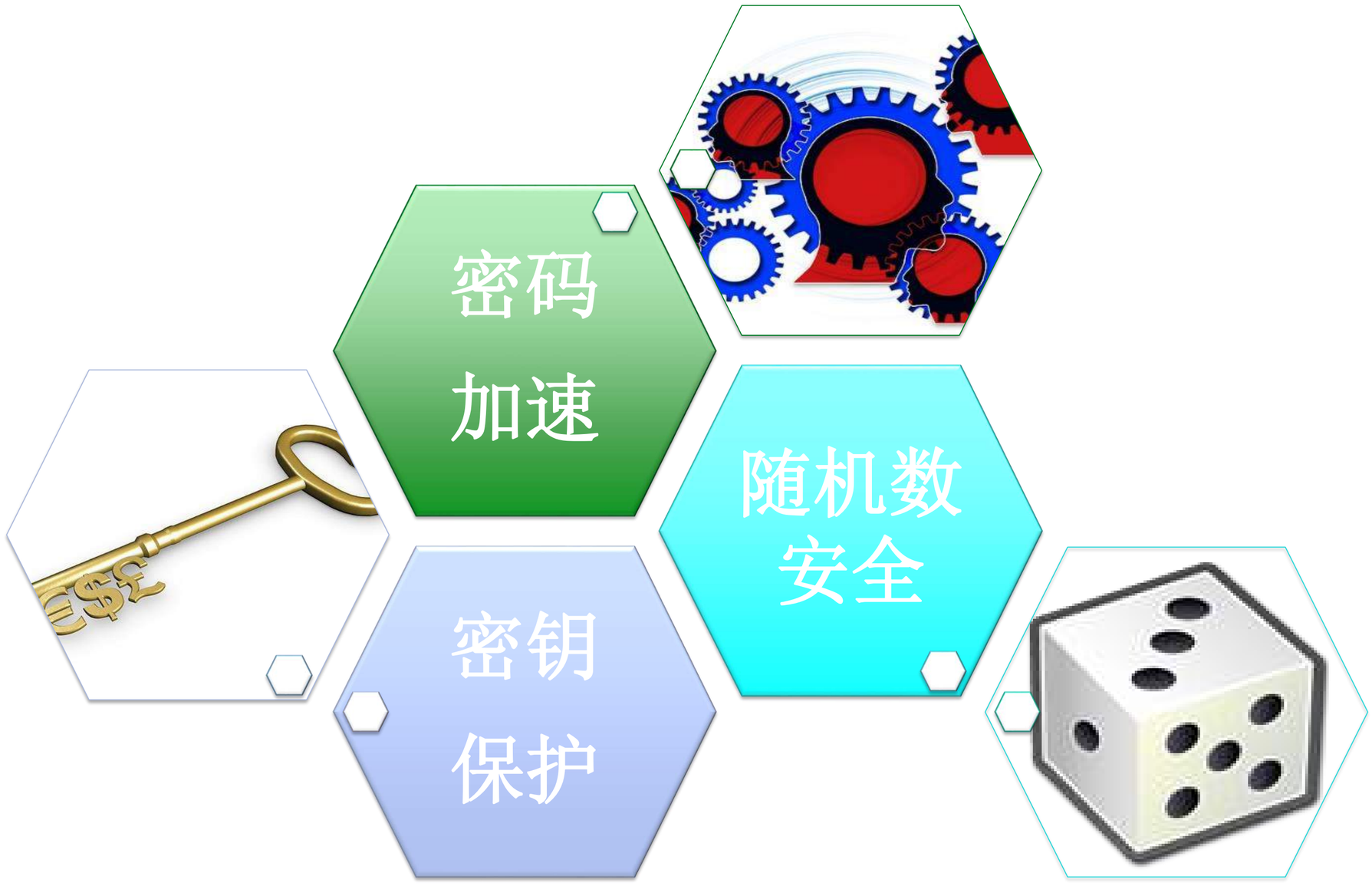
密码模块

密码机

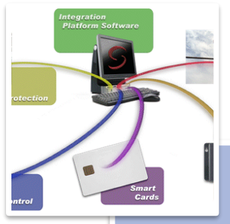
密码处理器板卡

密码系统

硬件密码的优势



硬件密码应用挑战



基础设施

- 性价比
- 可靠性
- 易用性

新场景

- 方案多样化
- 高性能
- 远程管理
- 虚拟化

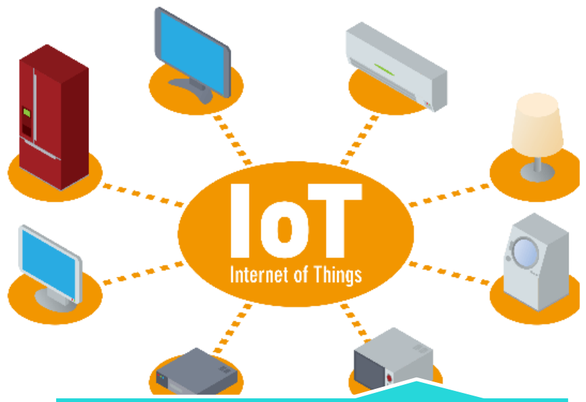
密码技术在云中不是没有用处，而是遇到各种限制和瓶颈

- ■形态？
- ■性能？？
- ■应用场景？？？

更丰富应用场景

云计算

大数据

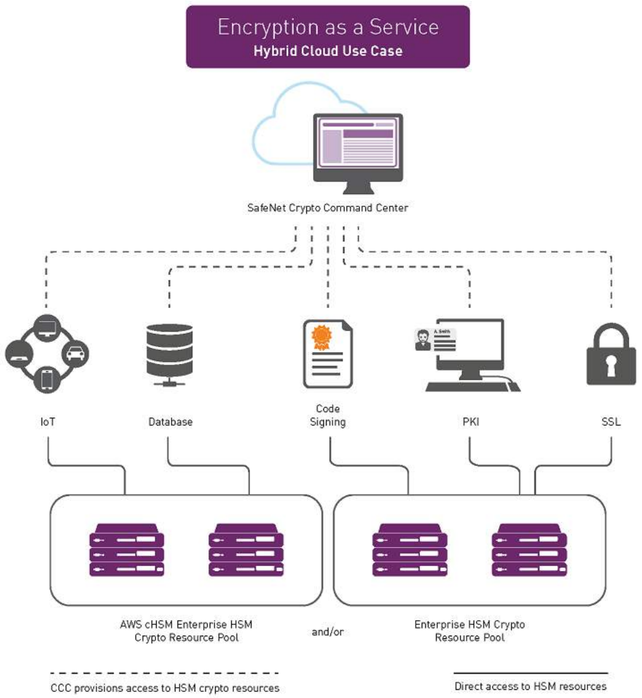


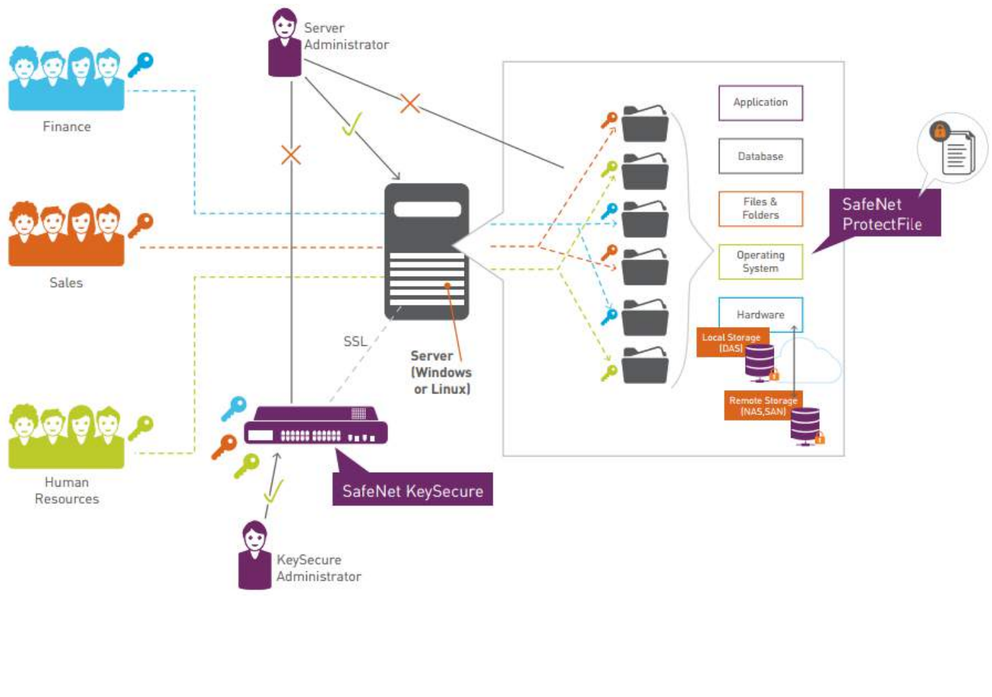
物联网

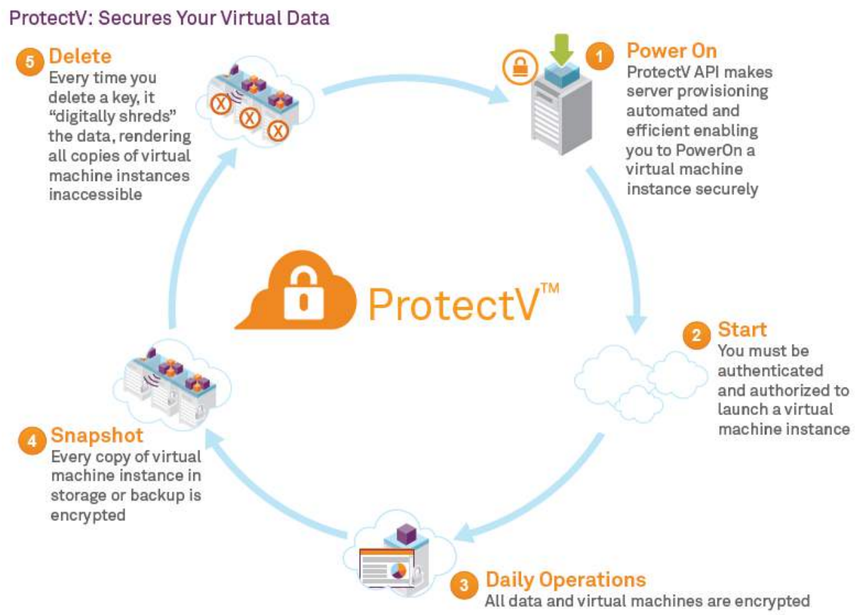
移动互联网

远程数据中心

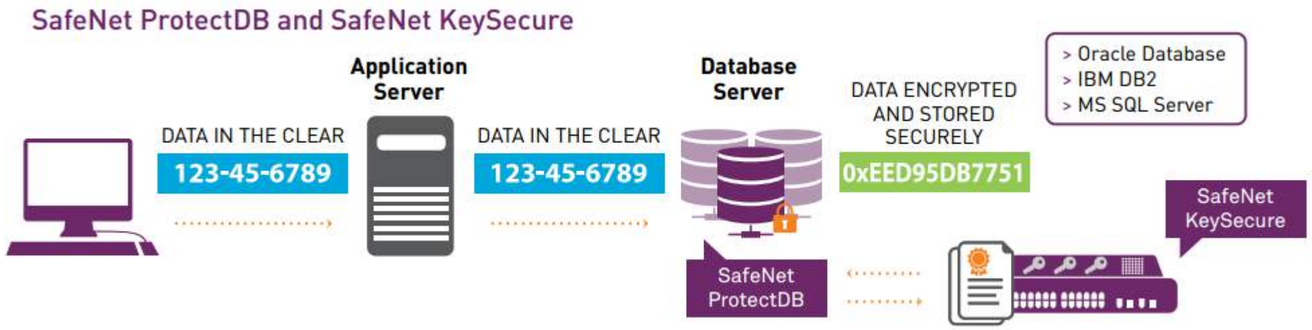
国外云密码产品情况







- Hardware Security Modules
- Key Management
- Data Center Encryption
- Virtual Machine Security
- Application Security
- High Speed Network Encryption
- Professional Data Protection Services



SafeNet

gemalto
security to be free

云密码技术框架

SaaS

- 云认证
- 云存储
- 云安全接入
- 云数据库加密
- 云环境加固

CaaS

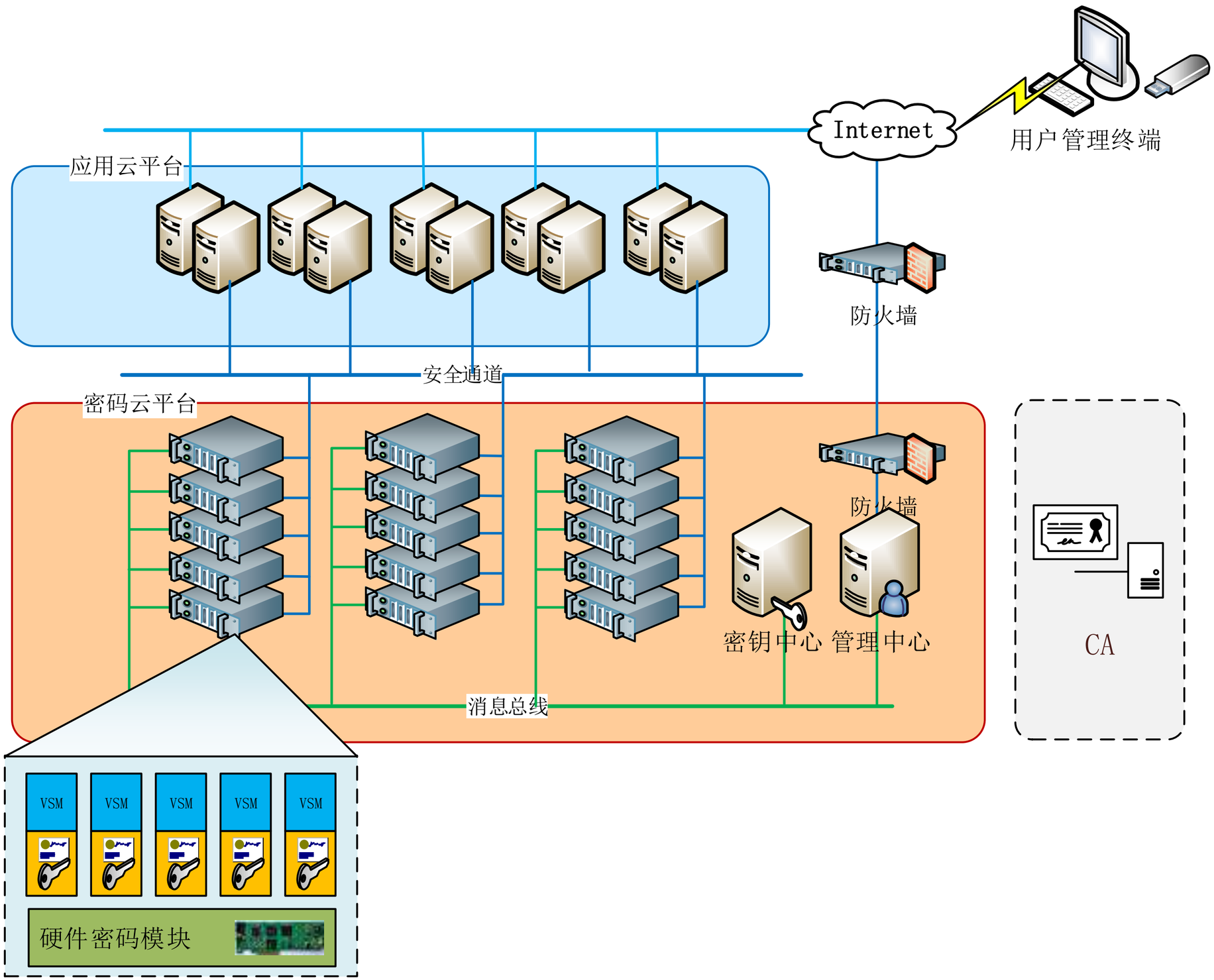
- 云加密
- 云签名
- 云密钥托管
- 云密码服务
  - 安全消息总线
  - 时间戳服务
  - 随机数服务

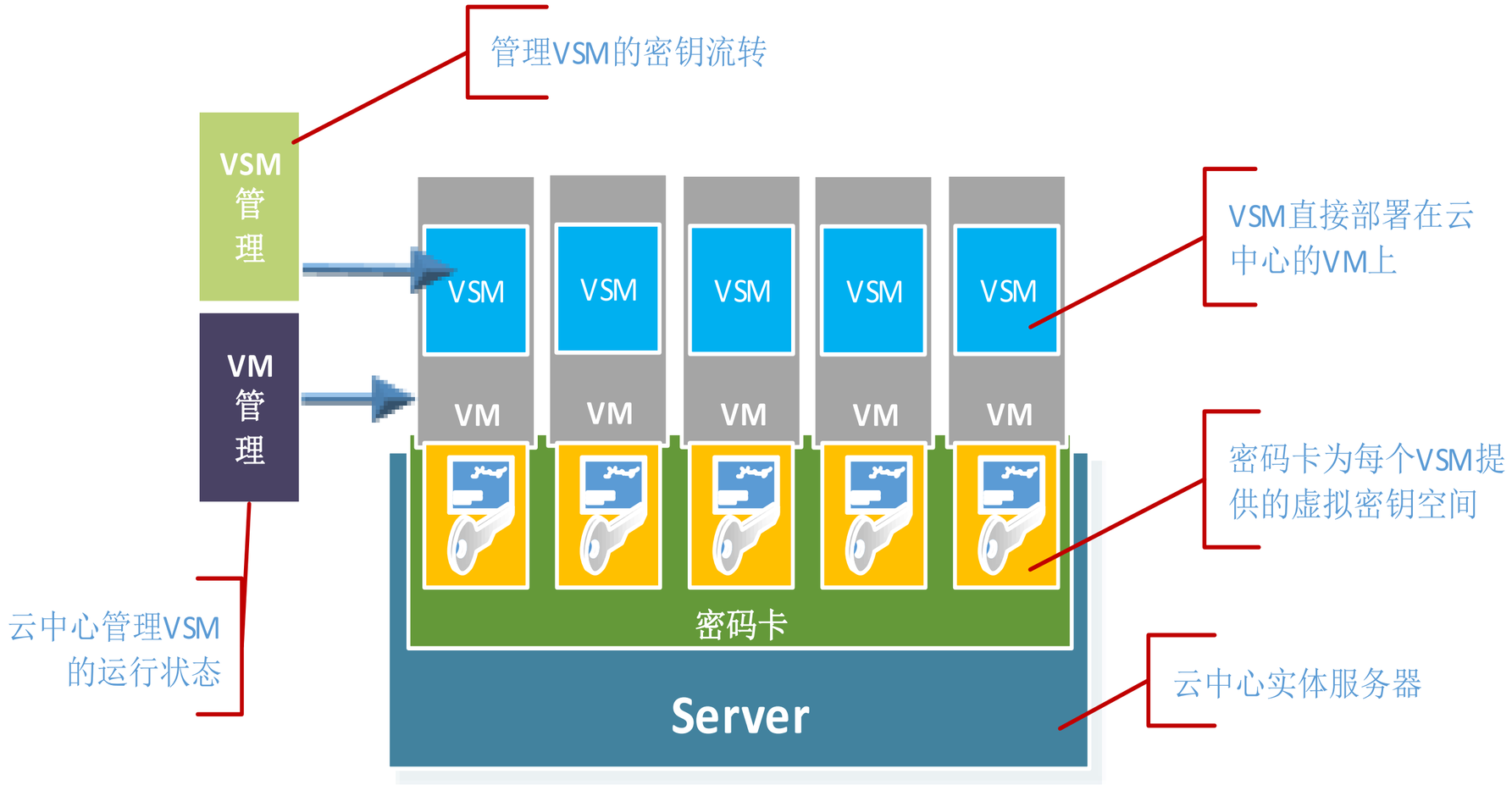
IaaS

- 云密码卡
- 云密码机
- 云密码平台

云密钥管理

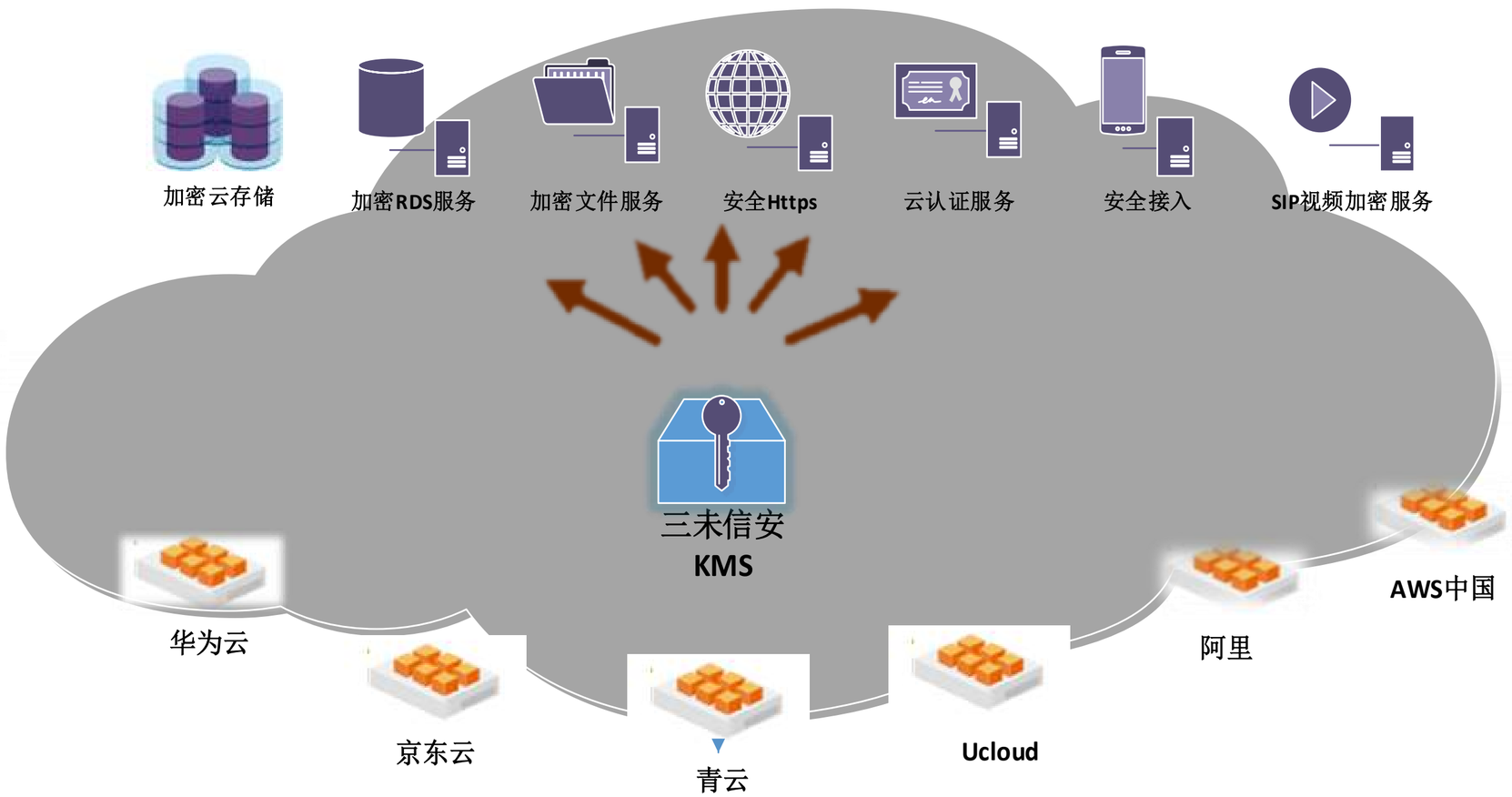
支持硬件虚拟化的云加密机





- 云密码服务模式：云密码机架构适合当前虚拟化和云环境下应用系统对密码服务及设备管理的需求。
- 密码机虚拟化：每台物理密码机可运行多个VSM虚拟密码机，每个VSM可对应用独立提供密码服务，并且各个VSM之间密钥完全隔离。
- 集中设备管理：统一的管理中心进行设备管理和监控，与用户密钥管理权限分离，保证用户密钥应用安全。
- 安全远程密钥管理：密钥管理由用户远程自行操作，满足认证权限的用户才能进行对应的密钥管理操作。
- 丰富的应用支持：可兼容传统密码应用接口，满足传统应用迁入虚拟化及云环境后对密码服务的需求。
- 白名单与网络隔离机制：VSM支持网络隔离，白名单外的主机访问VSM将被拒绝。
- 安全的业务调用：应用主机到VSM之间的业务调用采用加密通道，保护用户应用数据经过中间网络环节时的安全。

三未云加密服务



1、密钥生命周期管理

2、为PKI体系提供密钥管理

3、RACAL、PBOC 等金融密钥体系提供密钥管理

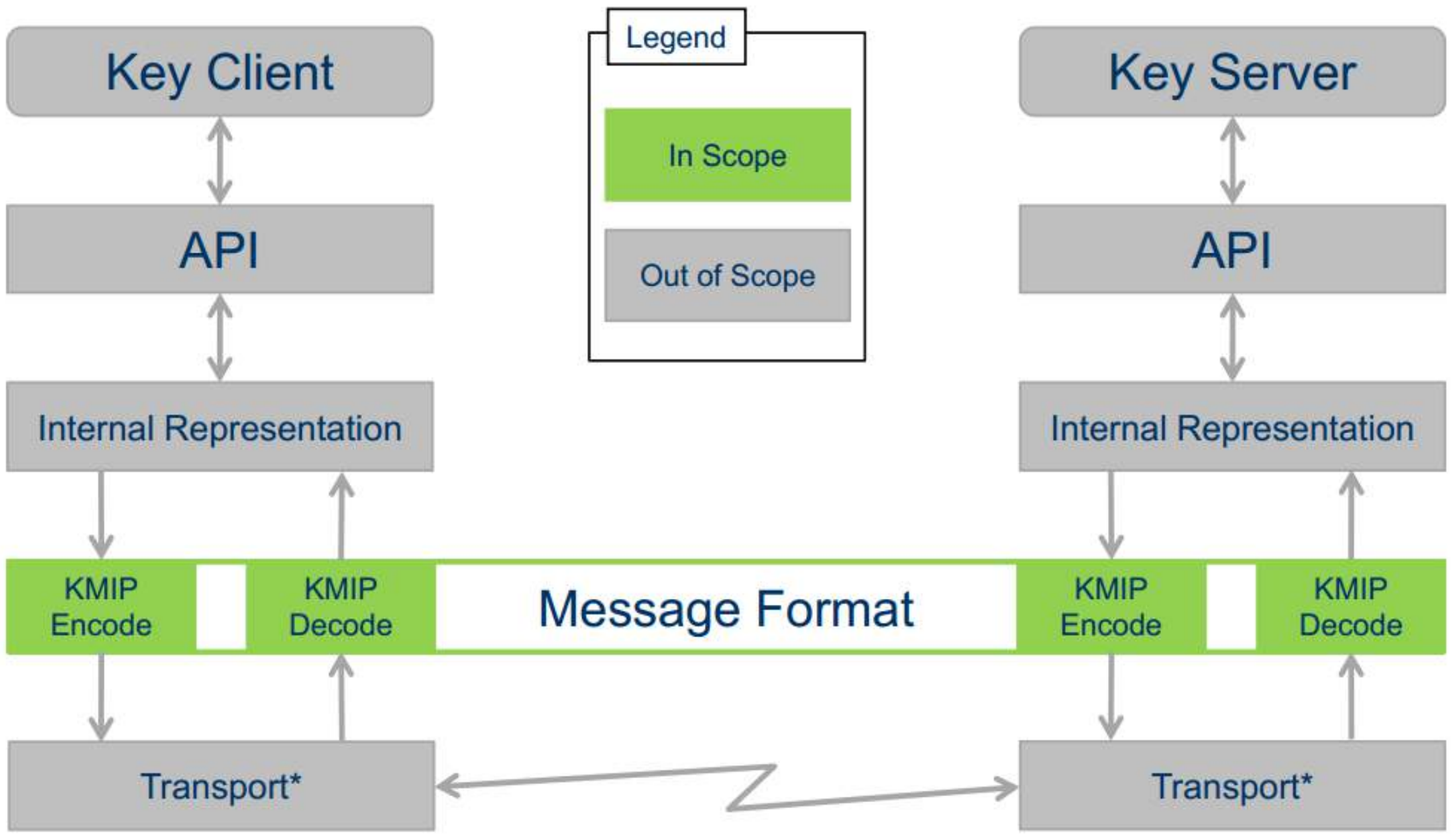
4、支持标准KMIP协议，云中协同密钥管理

5、在云密码机之上加入更细致强大的密钥管理功能

6、立即可用的密钥管理服务

7、支持虚拟化部署

KMIP让加密更易用



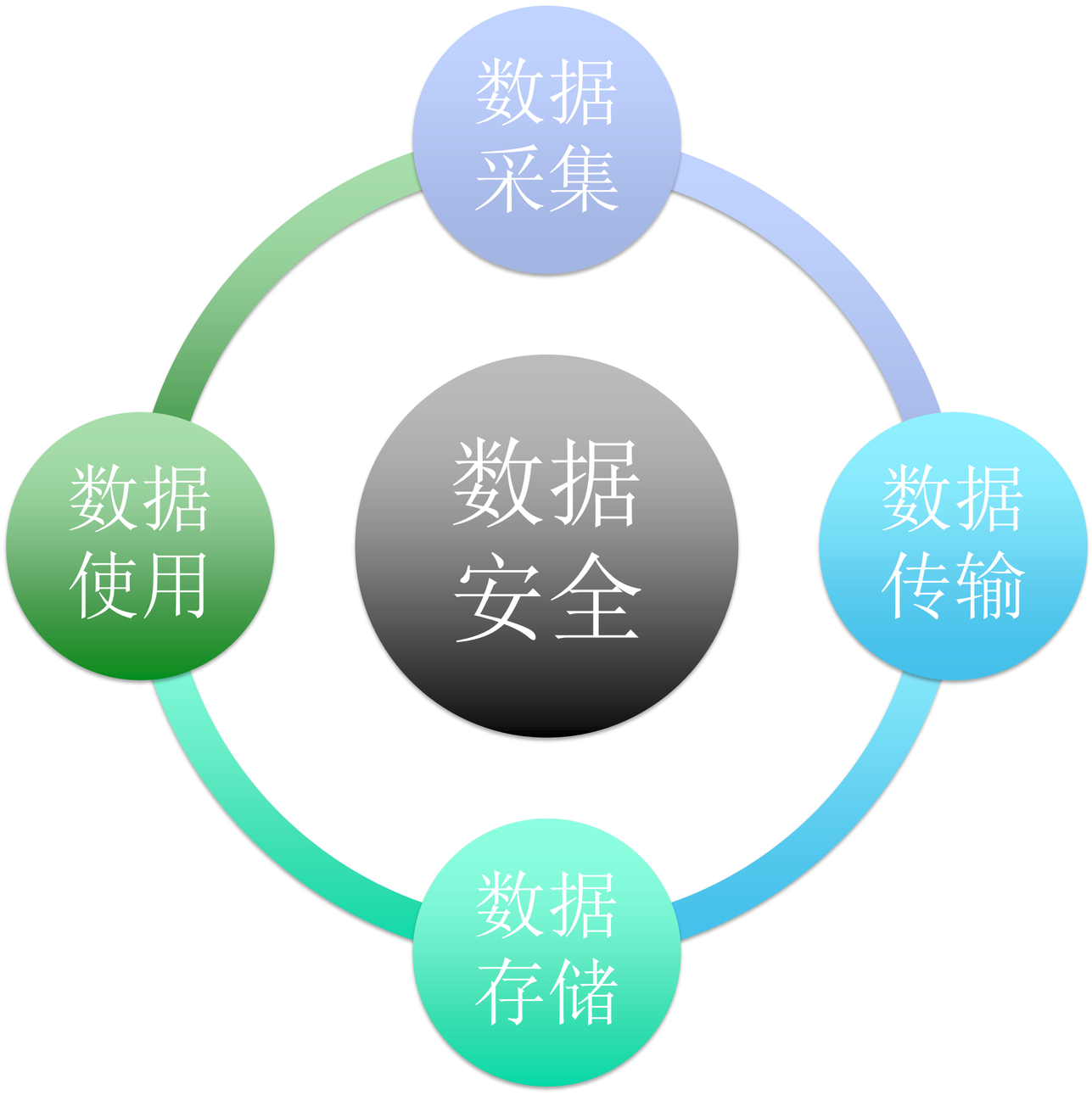
* Transport requires a secure communication protocol (e.g. HTTPS, TLS, etc…)

KMIP标准让加密变得更易于配置和管理

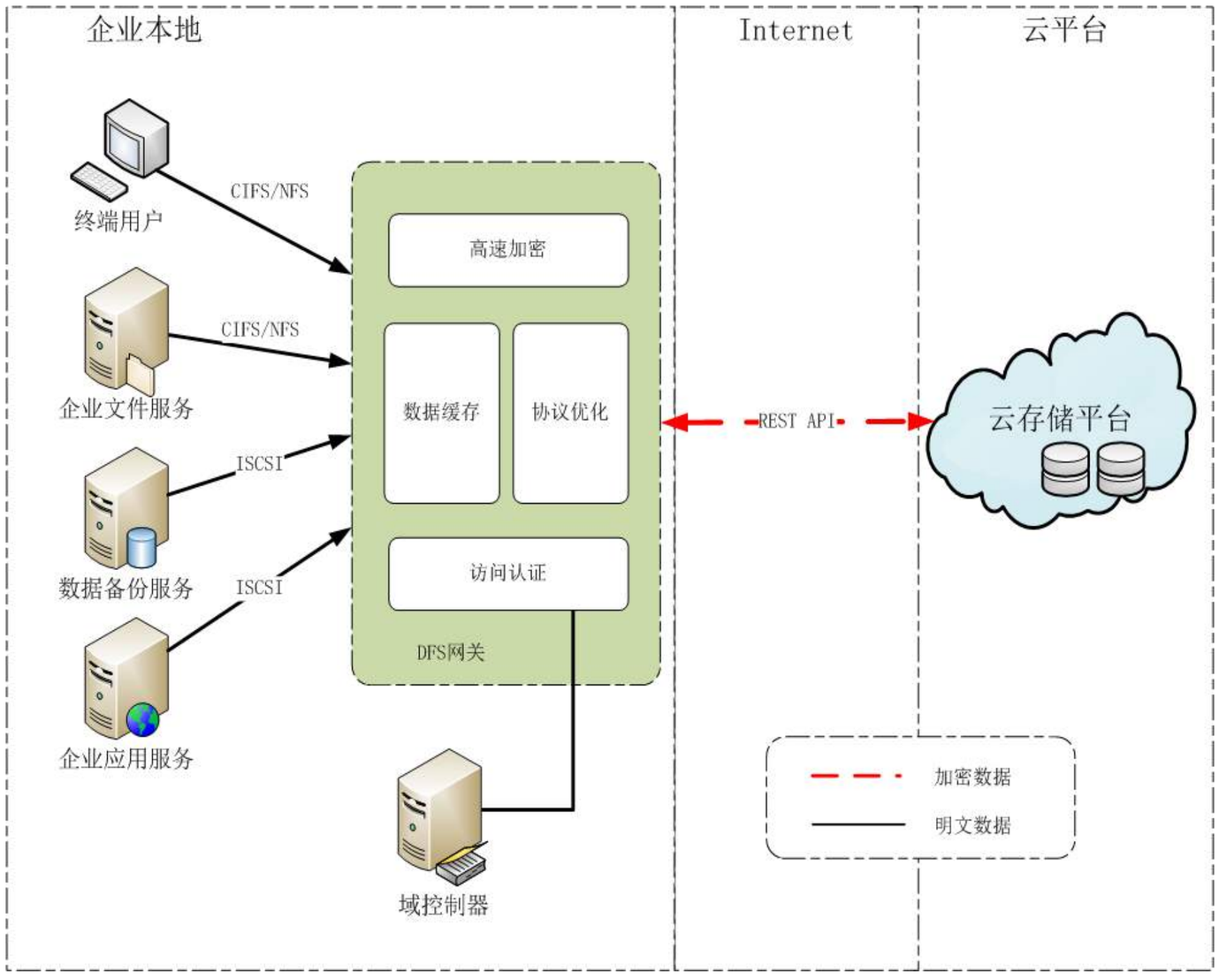
这种配置管理能力可以由密钥的使用者进行灵活的定制

随着加密技术在云端的应用越来越广泛，这种灵活性将变得越来越重要

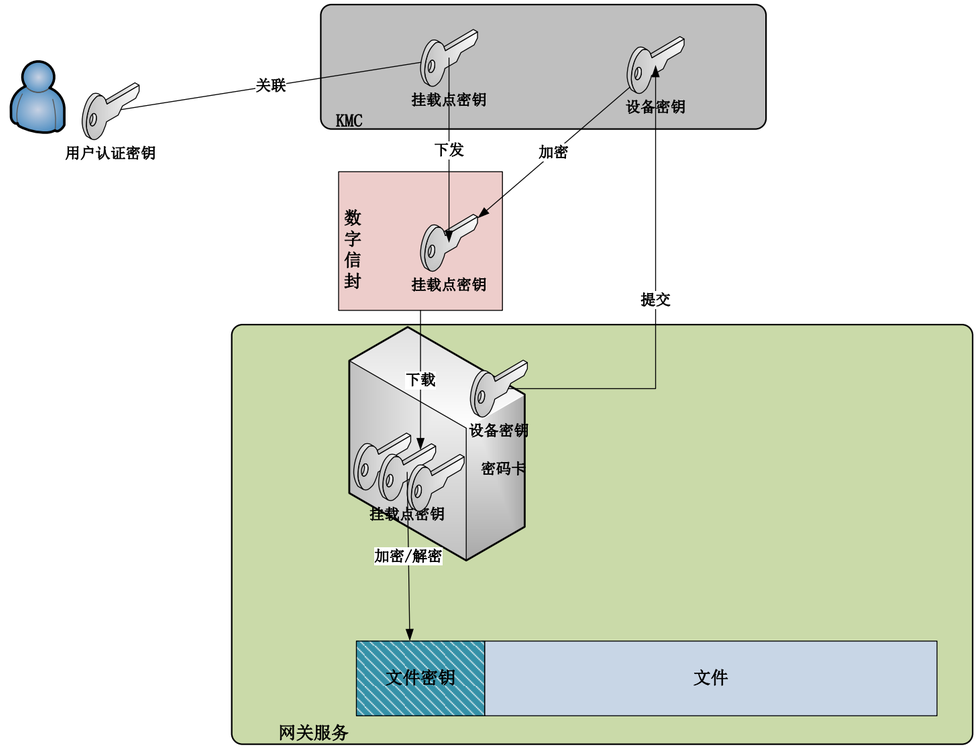
数据全生命周期



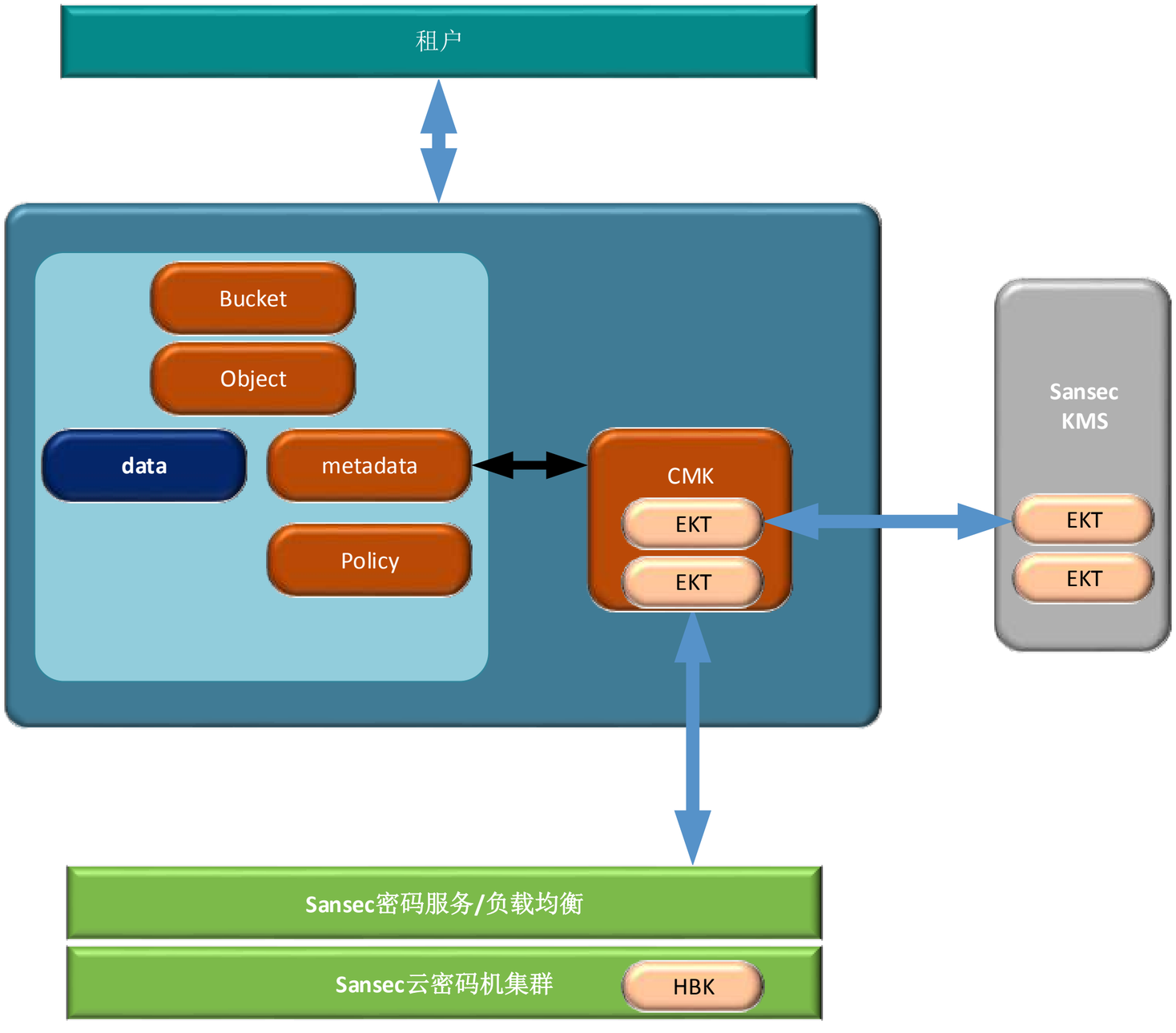
面向云存储服务的加密网关方案



- 云存储本地化
- 掌控密钥
- 高速加密
- 自动精简配置/按需分配空间
- 完整性保护/去重
- 快照/数据保护

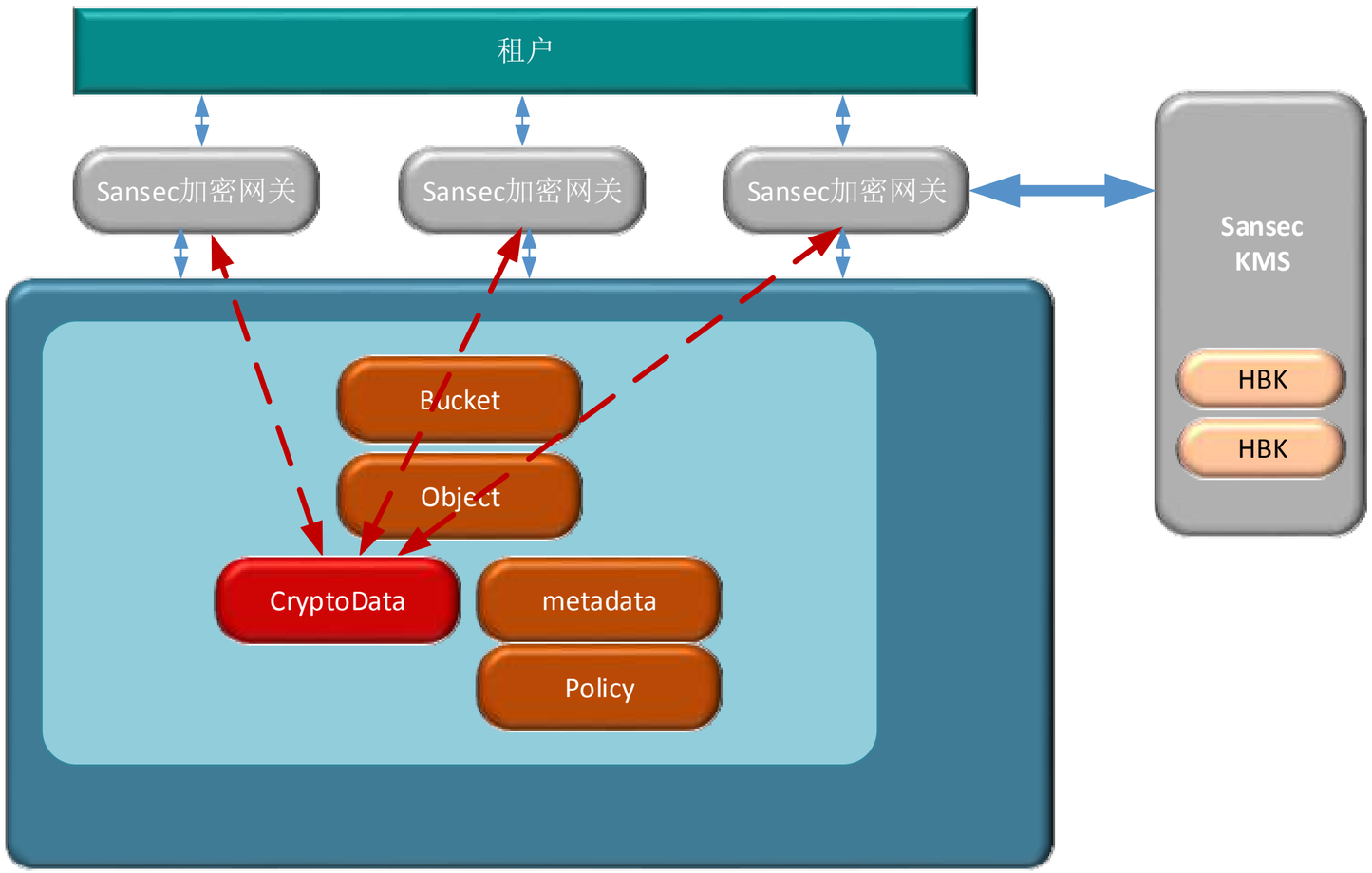


对象存储加密方案



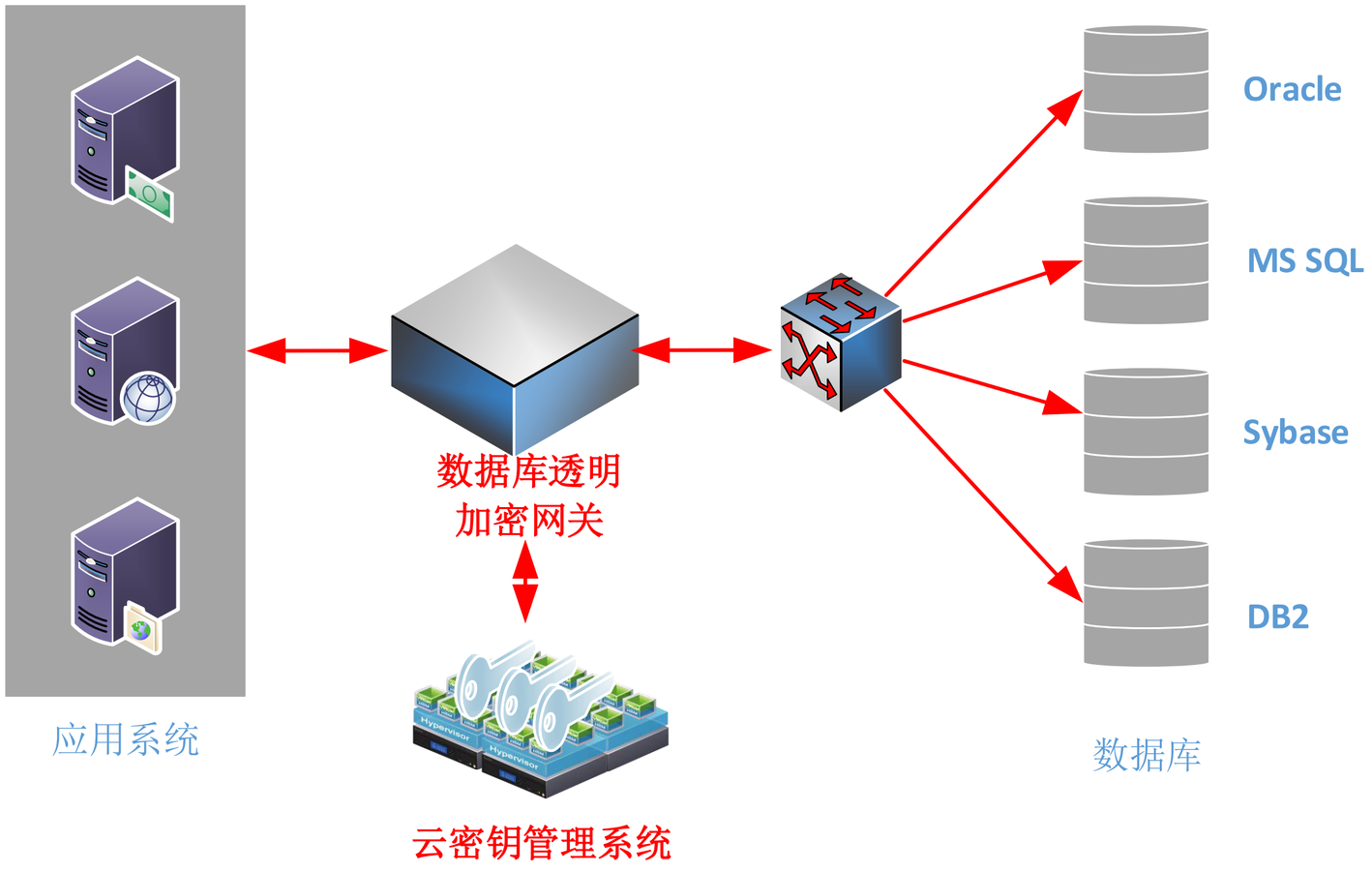
- 在DFS中为用户建立密钥管理容器；KMS作为密钥的产生源及密钥存储库提供密钥的一致性保证
- Sansec采用云密码机集群方式为DFS提供底层的密钥安全存储容器和密码运算功能
- Sansec通过密码服务层提供密码机集群的统一接口、负载均衡、密钥空间统一映射、故障自动处理等功能，保障DFS密码服务的高可用性
- DFS维护元数据与用户密钥的映射关系，必要时通过KMS获取受保护密钥EKT，并交由云密码机进行EKT的脱密及数据加解密功能。

对象存储云加密网关



- 实现透明，端到端加密。使用网关后，用户往DFS上存储数据的时候，无需用户做任何调用上的更改。
- 数据加密和解密由网关完成的，密钥由KMS进行统一管理，我们负责密钥和加密环境的安全；
- DFS 不会存储未加密的数据，也没有机会获得用户的数据加密密钥（由第三方KMS管理），这样的权责分离保证了华为不触碰用户数据的原则；
- 通过KMS可让用户灵活定制数据访问策略。

数据库加密方案



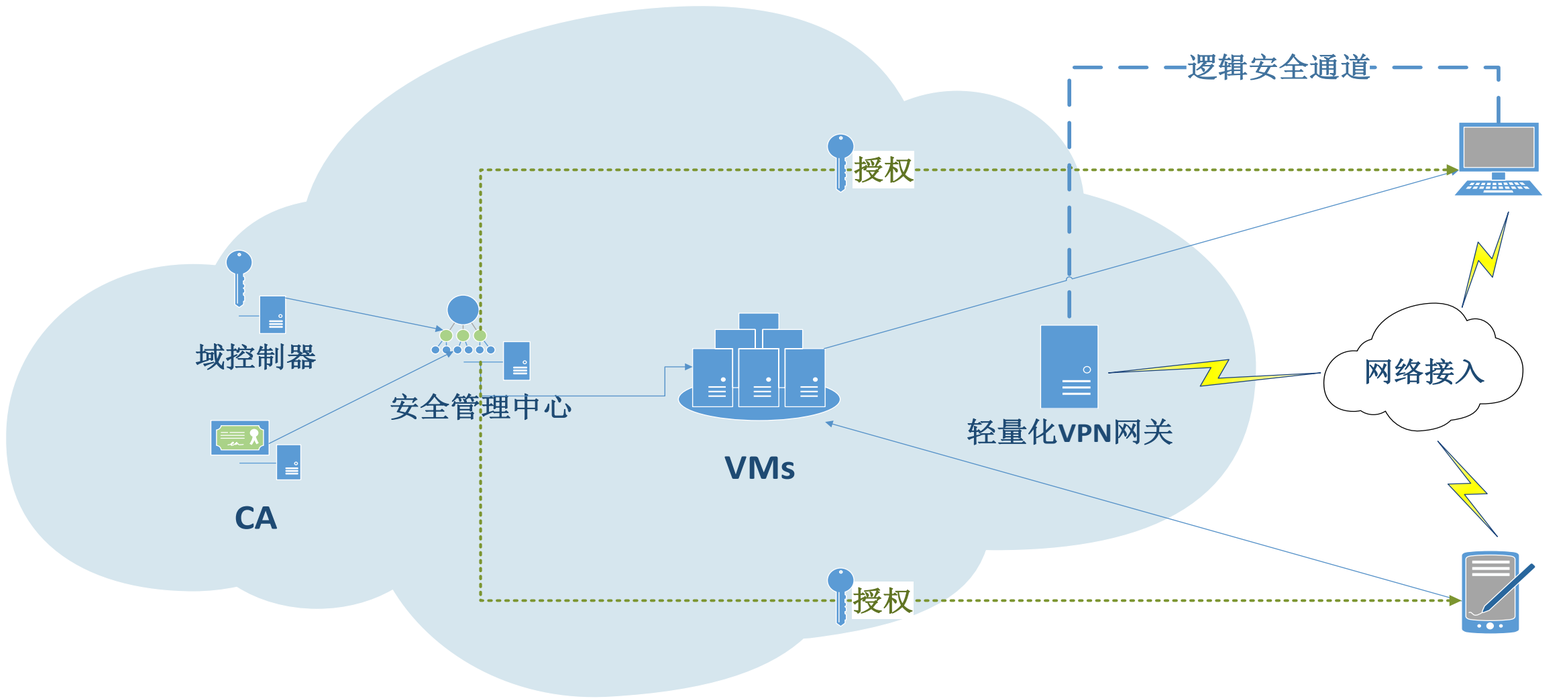
数据库透明加密

- 多种数据库SQL级透明加密
- 加密表空间、表及字段
- 查询优化
- 多字段类型支持

密钥管理

- 密钥安全存储
- 密钥集中管理
- 密钥使用授权

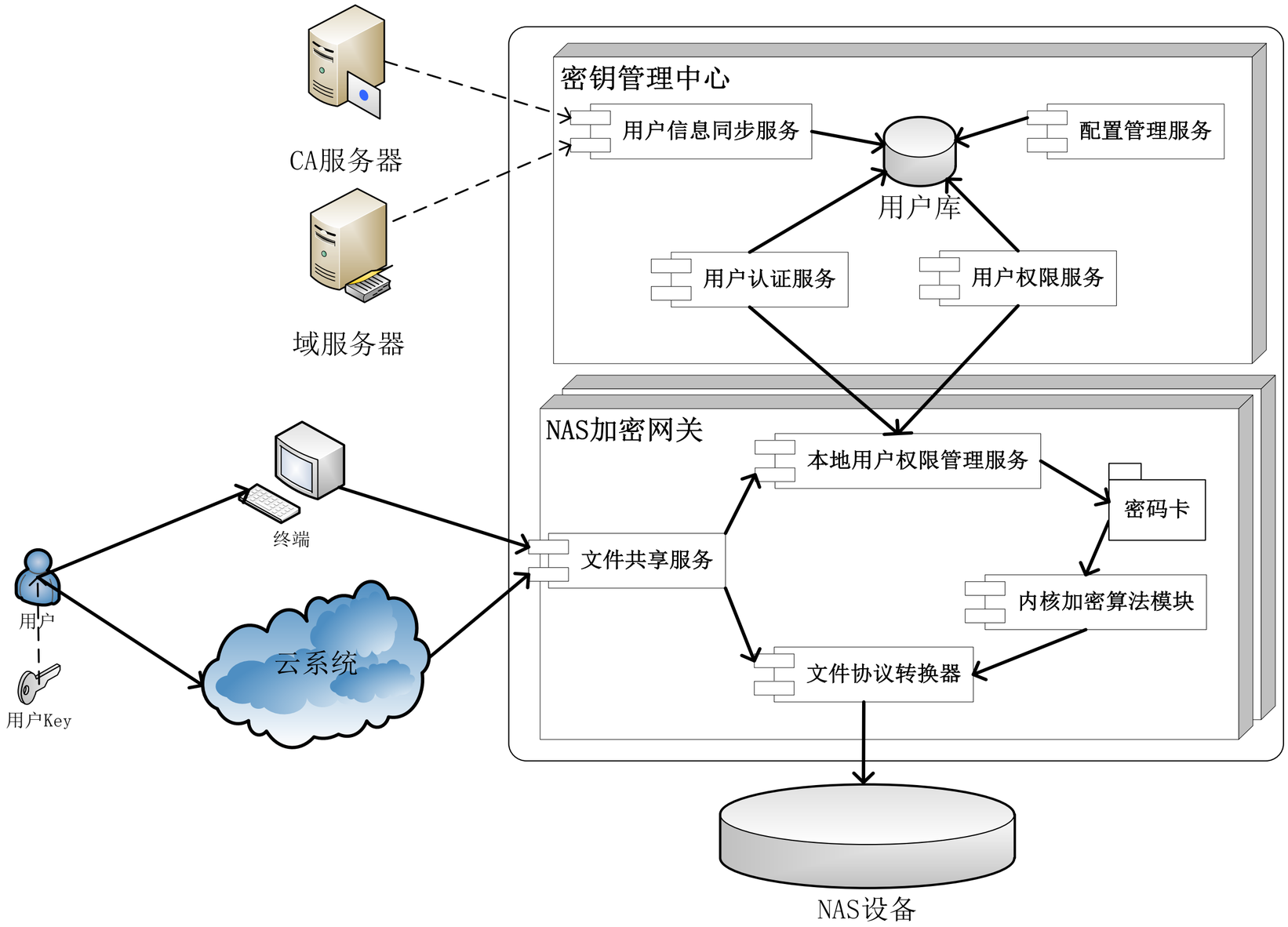
云桌面办公安全方案



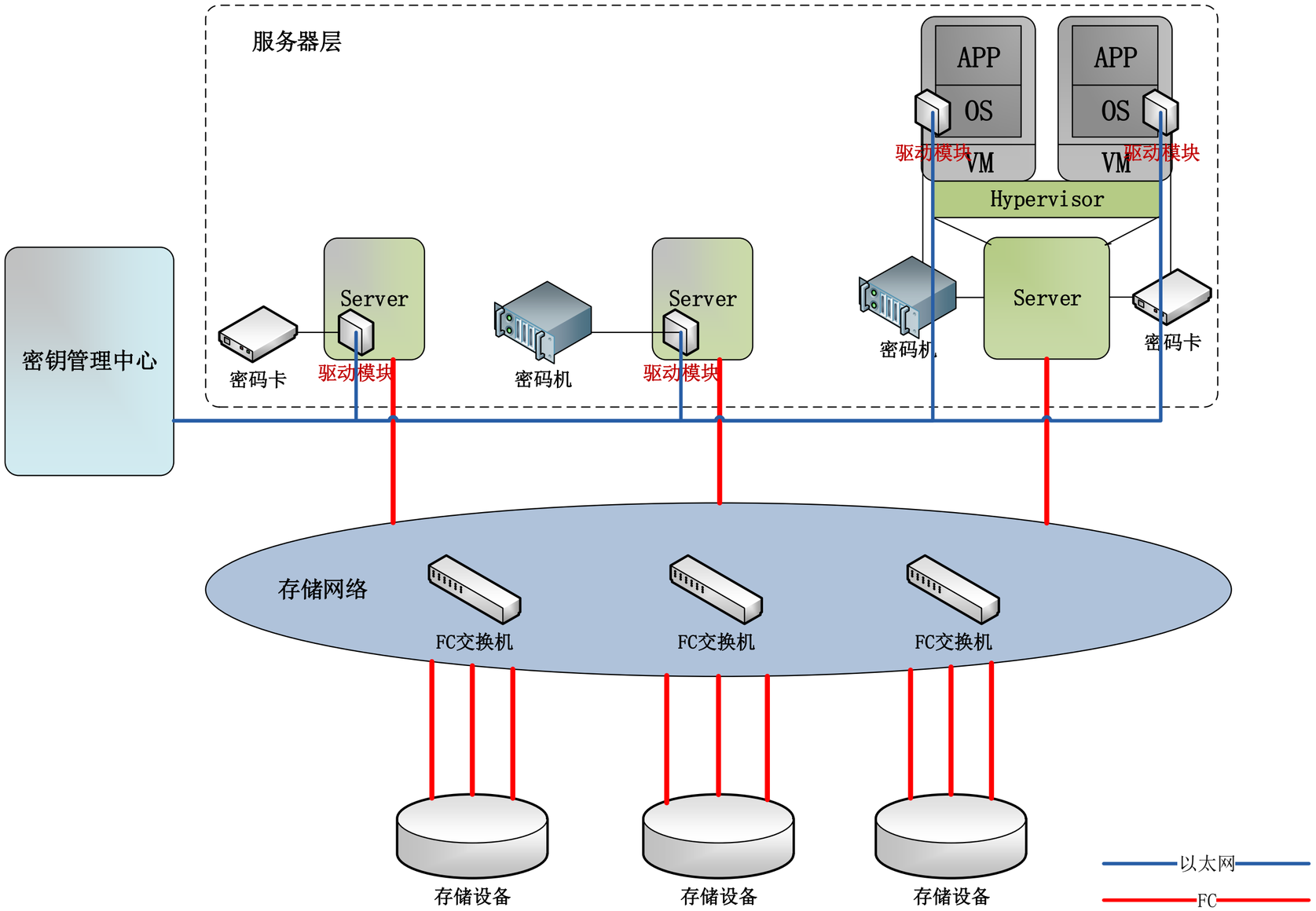
在云平台和云终端的数据安全防护方式中，采用双向认证、数据加密和数据完整性保护。

- ✓ **身份认证**：云平台和云终端在进行数据的交互之前，云终端和云平台首先验证对方身份的合法性，该过程通过签名验证和私有密钥验证来保证。双方认证通过，才进行下一步的数据交互，有效杜绝伪终端接入。
- ✓ **数据安全传输**：对于在云平台和云终端的敏感性数据，通过对称密钥加密，确保数据的保密性。为了防止密钥过度使用带来的安全风险，采用密钥协商机制，实现“一次一密”，确保密钥的安全性。
- ✓ **数据完整性**：对于关键数据，为了防止在传输过程中被篡改或破坏的数据被采纳，影响数据的真实性，需要加强数据的完整性保护，在传输数据后附加基于对称密钥的消息认证码MAC。
- ✓ **存储安全**：用户数据存储到NAS存储服务器时经过加密存储网关进行加密后存储。加密存储网关支持用户密钥管理、用户访问权限管理、数据透明加解密等安全功能，保证用户数据的安全隔离和保护。

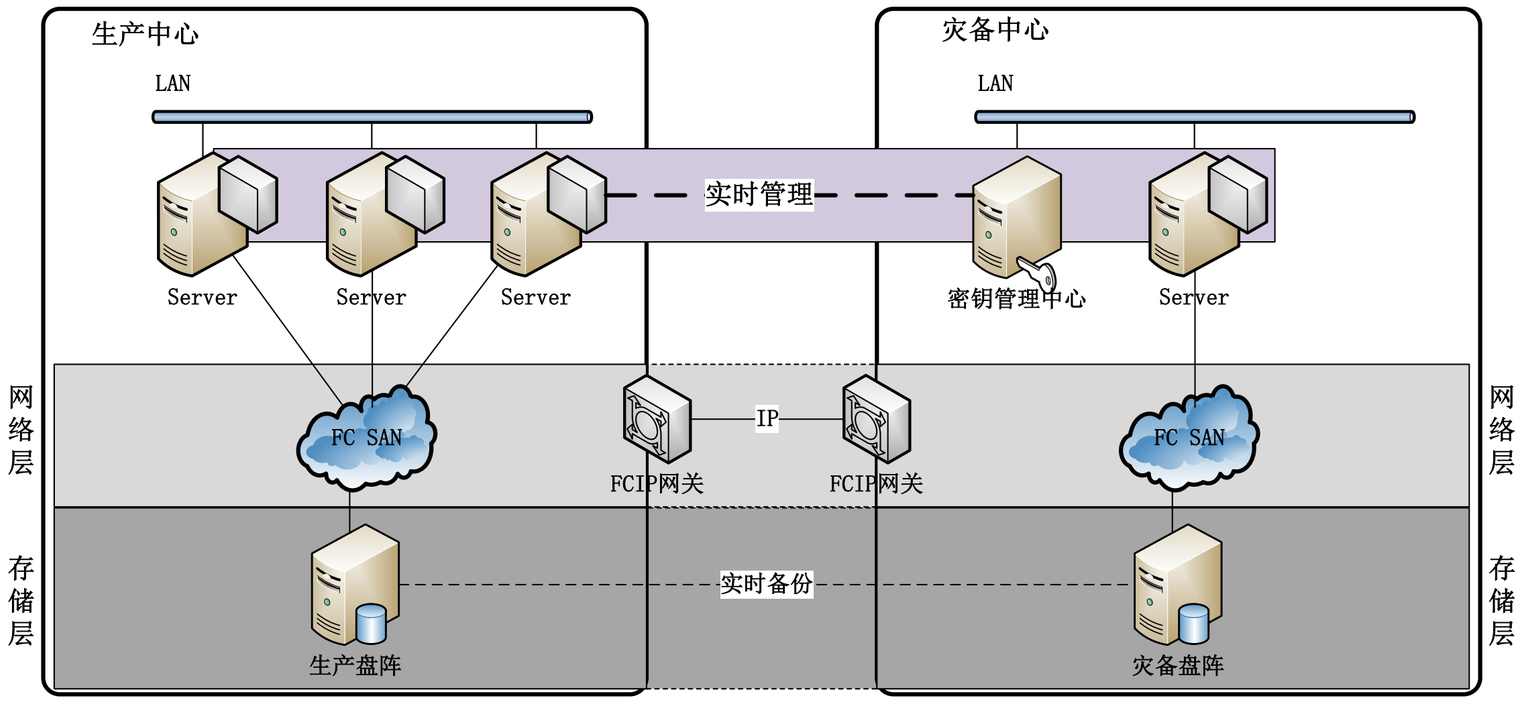
NAS存储加密网关


CA服务器
域服务器
密钥管理中心
用户信息同步服务
配置管理服务
用户库
用户认证服务
用户权限服务
NAS加密网关
本地用户权限管理服务
密码卡
文件共享服务
内核加密算法模块
文件协议转换器
终端
用户
用户Key
云系统
NAS设备

服务器/虚拟机隔离存储方案



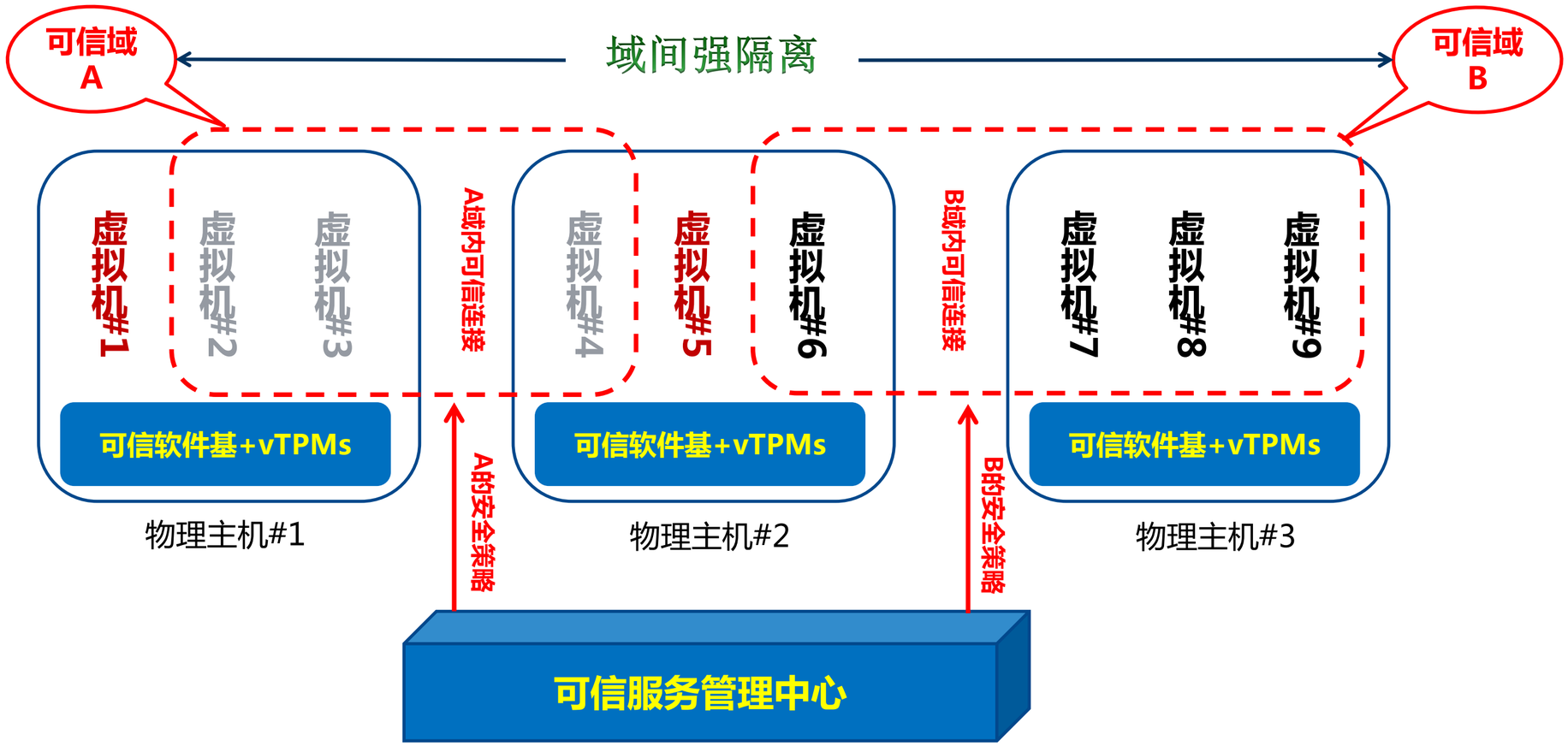
IO管控 | 虚机认证入池 | 透明加密 | 结合认证 | 安全隔离 | 存储节点保护



数据中心加密方案主要提供数据加密、安全管理两方面的功能。

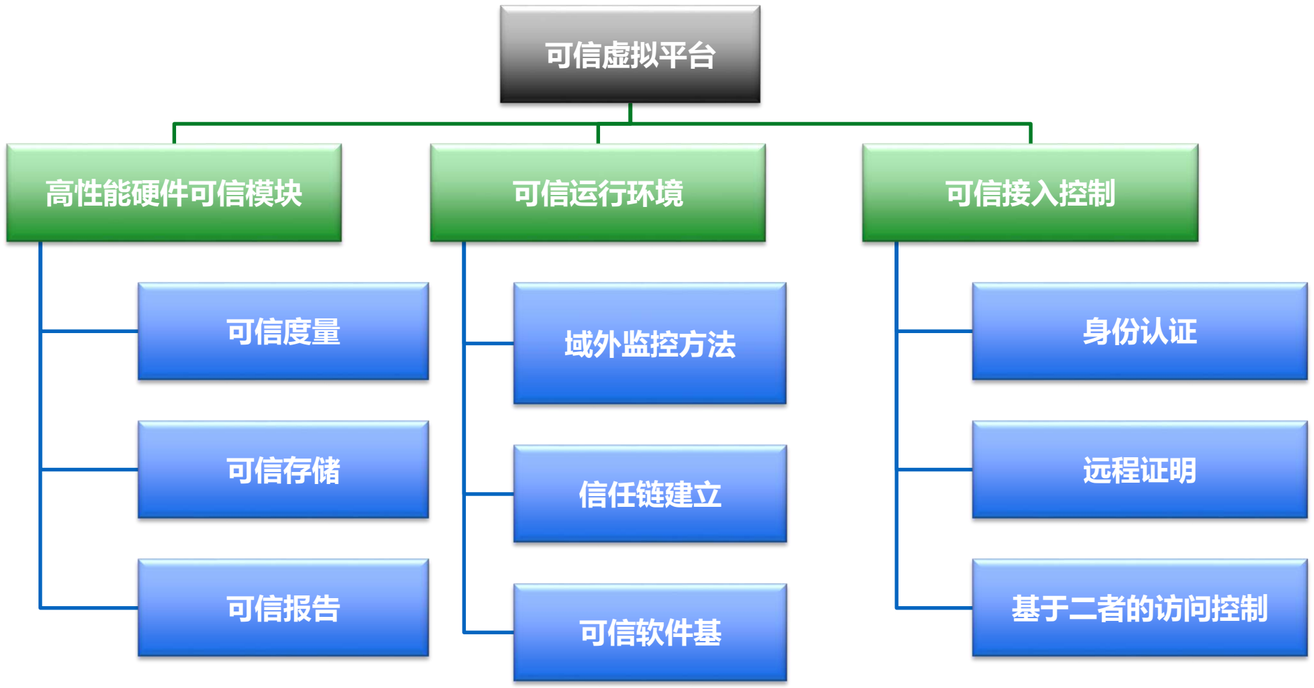
- **数据加密**
  - **高速内核加密模块：**软件层部署在Server或VM的操作系统层，采用内核加密模块，以及硬件缓存技术，以充分利用高速硬件资源。
  - **高速加密算法：**基于国际标准IEEE1619-2007，采用SM4-XTS高速国产加密算法，从应用于存储加密的可行性、硬件加速方法两方面解决了存储加密的算法瓶颈。
- **安全管理**
  - **密钥管理：**采用密钥管理中心（以下简称KMC）的方式统一管理密钥，KMC负责维护Server与密钥的映射关系、密钥的生命周期管理、密钥的安全使用等功能；
  - **认证授权：**每个Server都对应一块密码卡或一台密码机，可以通过第三方CA为该Server签发数字证书，证书密钥由密码卡或密码机安全保护。
  - **管理员控制：**实现“三员分离”的安全管理，由KMC管理员负责存储安全管理，维护用户密钥安全，系统管理员无法获取到用户数据的内容，实现权限分离。另有审计管理员，独立于其他人员权限。
  - **安全审计：**管理员、Server对存储的各种访问及操作日志可通过统一的审计平台进行审计管理。

可信虚拟机的总体架构



- 在服务器中插入PCI-E接口的HTM实现TPM功能，由于HTM强大的处理能力和存储容量，以及对虚拟化的支持，可以在卡内实现pTPM（物理TPM）和足够数量的vTPM（虚拟TPM）
- 即使内存容量不够，也可以使用pTPM的存储加密能力将暂时不用vTPM交换到宿主机的存储器中，在使用时调入
- vTPM在HTM中可以获得和pTPM等同的性能和安全级别。
- HTM支持TPM2.0标准，以满足项目的可信计算技术要求。

可信虚拟平台是一个软硬件结合的平台系统



高性能硬件可信模块

- 高性能密码算法与PCIE3.0多通道的实现
- 添加对SR-IOV技术的支持
- 提供可信度量，可信存储，可信报告的功能，实现足够数量的vTPM

虚拟机可信运行环境

- 主要研究基于域外监控的可信度量和控制技术
- 利用HTM提供的硬件vTPM支持，在VMM中度量虚拟镜像
- 通过域外监控模块，对系统的运行状态进行动态捕获

可信接入控制

- 制定虚拟机环境的配置基线
- 研究并构建完整有效的远程证明协议
- 并通过远程证明协议证明配置执行的正确性

Thank you