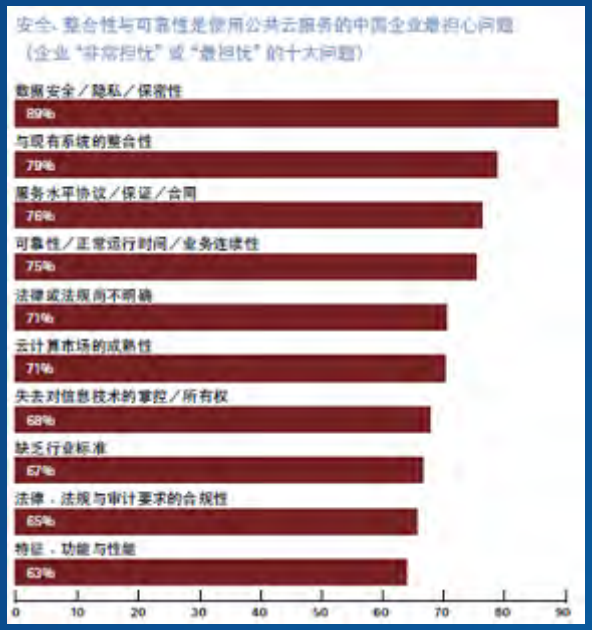
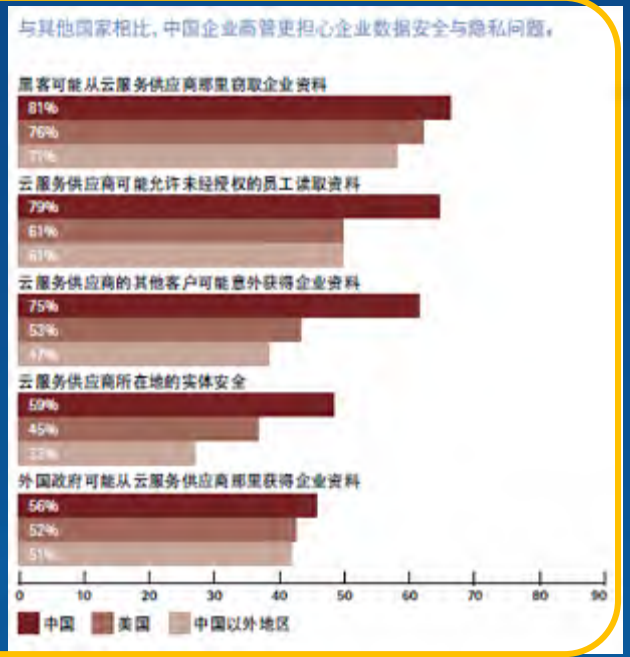
云加密技术应用与发展

DT时代，数据就是企业的核心资产
黑客也是这样认为的!

安全 网上调查



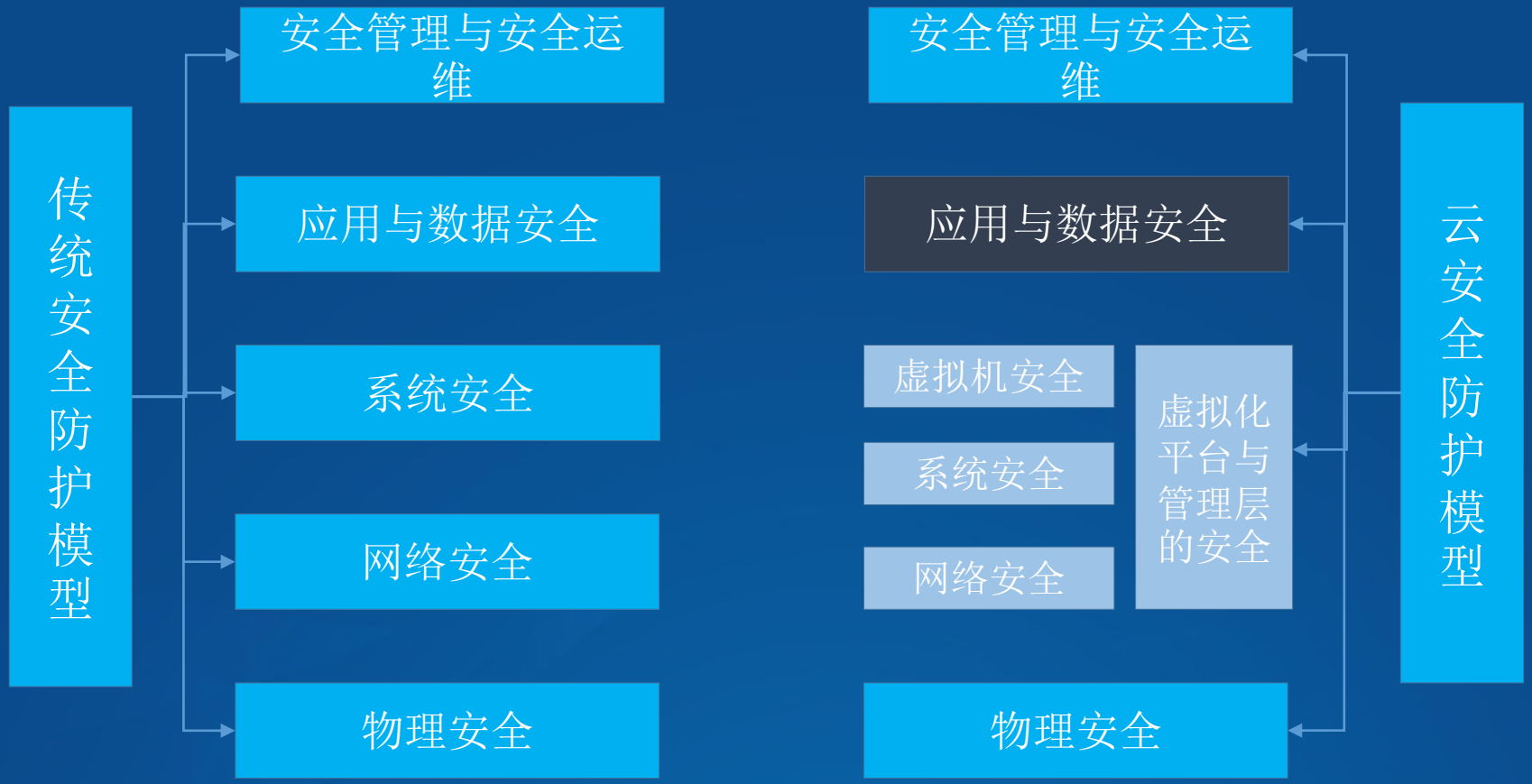


安全 数据安全标准

- 2015年7月，阿里云全球率先发起“数据保护倡议”。
- 基于云计算的电子政务公共平台安全技术规范
- 云计算等级保护标准

安全 上云障碍

- 如何保证黑客入侵后无法拿到敏感数据？
- 如何确保即使云服务商也无法拿到客户的敏感数据？
- 如何满足加密合规要求，尤其金融行业?


传统安全防护模型
安全管理与安全运维
应用与数据安全
系统安全
网络安全
物理安全
云安全防护模型
安全管理与安全运维
应用与数据安全
虚拟机安全
系统安全
网络安全
虚拟化平台与管理层的安全
物理安全

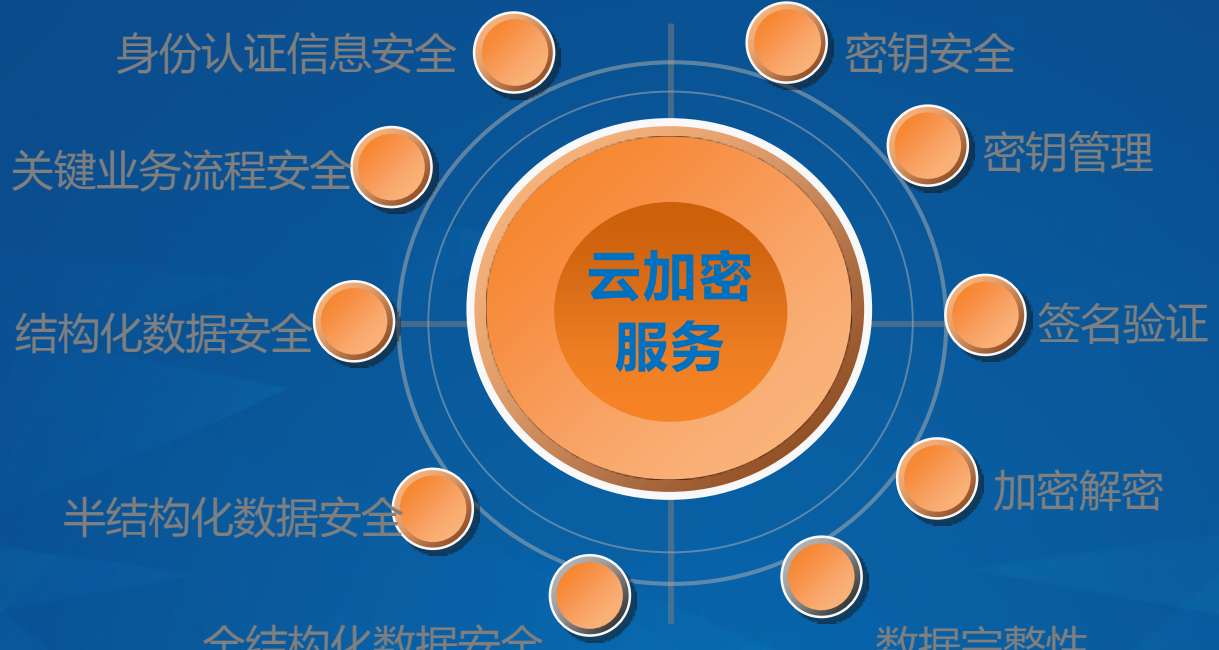
2015年7月中央网信办《关于加强党政部门云计算服务网络安全管理的意见》

四大原则

① 安全管理责任不变
② 安全管理标准不变
③ 数据归属关系不变
④ 敏感信息不出境

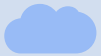
关于加密服务

业务需求不变： 机密性、完整性、不可抵赖性
行业监管要求不变：商用密码管理条例
密码设备的核心功能不变：密钥安全管理+密码算法服务
产品形态不变： 硬件芯片、硬件设备
产品功能不变： 服务器密码机、金融数据密码机、签名验签服务器



高性能　　密钥管理　　可伸缩

行业监管　　安全隔离　　高可用性

变化类型	变化内容	变化带来的新需求
 业务模型变化	旧：厂商->用户->应用	① 资源管理与密钥管理分离 ② 只有用户才能管理和使用自己的资源
	新：厂商->云服务商->用户->应用	
 服务特性变化	旧：密码设备能力固定、服务功能固化、物理设备热备	③ 计算资源可漂移 ④ 计算能力动态扩展 ⑤ 计算资源可管理 ⑥ 服务功能可管理
	新：高可用性、弹性计算、可管理	
 部署模式变化	旧：应用与设备直连、管理员近程管理、物理设备独占	⑦ 设备支持远程安全管理 ⑧ 不同用户之间安全隔离 ⑨ 应用与资源的认证与通讯加密
	新：应用与设备通过虚拟子网连接、管理员通过网络远程管理、物理设备共享	

❖国内外发展现状对比：

国外发展现状

- Safenet、Thalas等加密厂商纷纷在产品中支持虚拟化
- 2013年，亚马逊云在国外发布云加密服务，包括CloudHSM和KMS两种服务形式
- 2016年，微软推出云加密服务KeyValt

国内发展现状

- 在获得国家发改委信息安全专项扶持下，2015年10月，江南天安推出国内第一款支持虚拟化的加密产品：SJJ1528云加密服务器
- 2015年12月，阿里云和江南天安联合发布国内第一款云加密产品

2014年3月

与各大云服务商调研，了解云计算对密码设备的需求

2014年

江南天安投入开发新一代云服务器密码机，并获得国家发改委信息安全专项扶持。

2015年10月

SJJ1528通过国家密码管理局安全性审查

2015年12月

阿里云与江南天安召开云加密服务发布会，同时开始提供公测服务

2016年3月

阿里云 云加密服务正式上线

至今

相关产品标准规范已经在密标委正式立项

十余家主要云服务商展开合作

面向云综合应用

SJJ1528云服务器密码机

面向支付业务

面向PKI应用

面向签名认证应用

密码设备管理系统

SJJ1511
金融数据密码机

SJJ1310
金融数据密码机

SJJ1321-A
金融数据密码机

SJJ1507-A服务器密码机

SJJ1507-A
服务器密码机

SJJ1402加密服务器

时间戳服务器

SRJ1001
应用安全认证网关

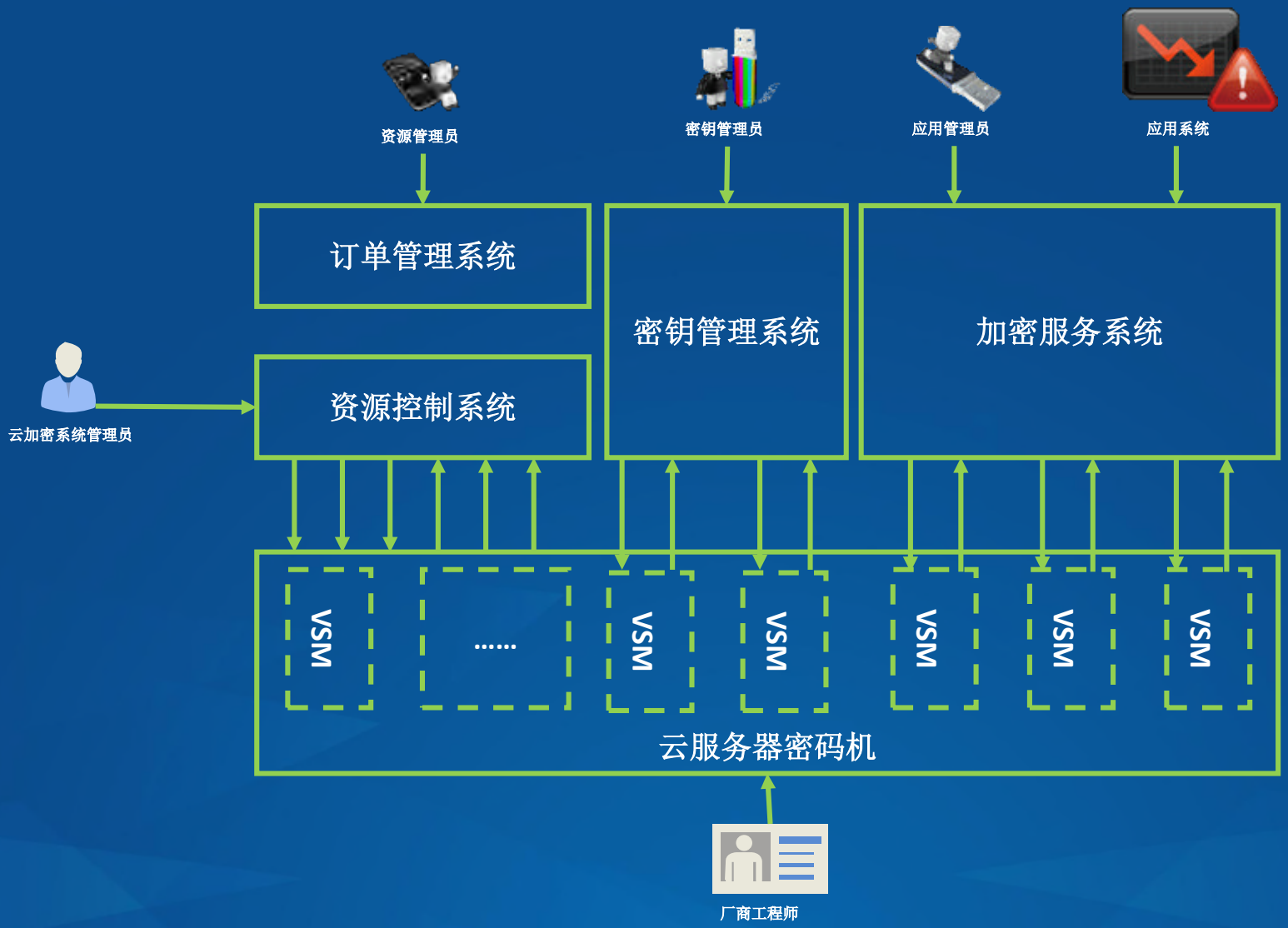
SRJ1303
签名验证服务器

SJJ1313USB密码器

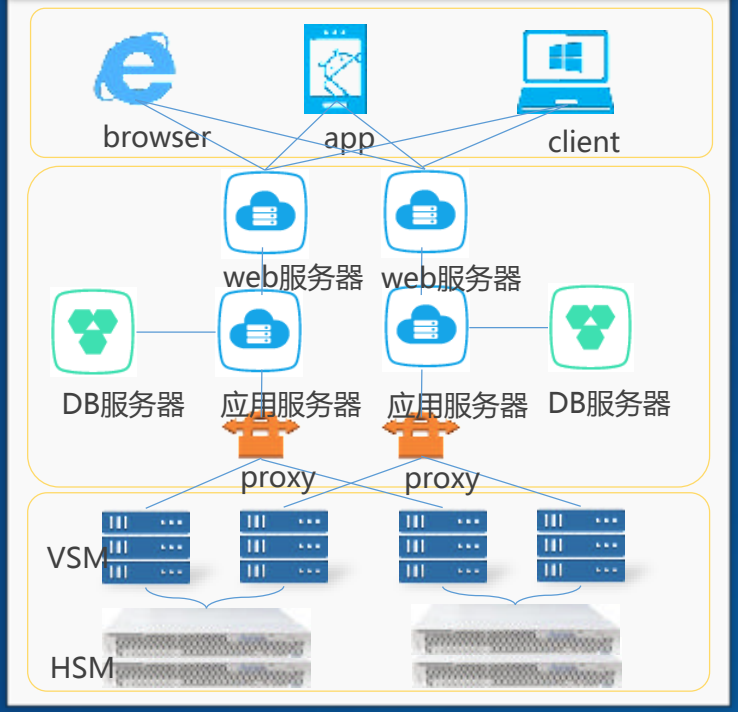
SJK1322 PCI-E密码卡

基础硬件设备


授权管理系统
厂商
云服务提供商
云密码服务管理系统
平台密钥管理机
授权文件
资源准入
资源管理
用户密钥
安全通讯
云密码计算资源
VSM管理软件
管理用户
应用授权
ATM
云端应用
安全通讯代理软件


资源管理员
密钥管理员
应用管理员
应用系统
订单管理系统
密钥管理系统
加密服务系统
资源控制系统
云加密系统管理员
VSM
.....
VSM
VSM
VSM
VSM
VSM
云服务器密码机
厂商工程师

应用场景



其他典型应用

- 支付应用
- 电子政务应用
- 电子票据应用
- 企业信息系统应用

敏感数据加密

面临挑战：

- 黑客攻破网络，拖库导致数据泄露风险；
- 内部非授权用户非法访问，篡改数据、泄露数据风险。

解决方案：

- 数据在数据库存储时通过vsm加密后存储，保证数据的机密性；
- 数据在数据库存储时通过VSM进行完整性校验，保证数据的完整性；
- 加密密钥采用VSM生成和管理，保证了加密密钥的安全性。

客户价值：

- 杜绝了明文数据泄露、被篡改的风险；
- 提升了系统的健壮性和客户价值。

应用领域

- 政务、电商、门户、WEB站点等各类包含大量个人敏感信息的系统应用中。

密钥管理

可伸缩

高性能

安全隔离

高可用性

兼容传统设备

提供与传统密码设备相同的功能与接口，可完全兼容传统应用，方便传统应用向云端迁移。

节省设备投资

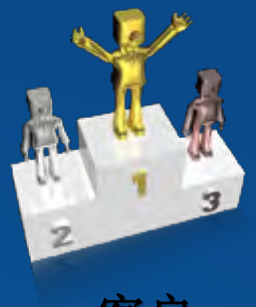
节省管理成本
节省人力投入
节能电能消耗

高可靠性

产品采用多级阵列技术，支持VSM集群、热备，切实保障用户的业务连续性；

满足资源动态分配

访问高峰时动态增加资源
访问低谷时动态释放资源



客户

行业

是国密算法推广的抓手

解决了云端应用如何使用国密算法的问题

是破解产业困局的钥匙

密码产品对性能的非理性追求、恶意价格战已经开始对产业造成损害
产业升级、业务模式变化是破解困局的可行方案

是扩大密码应用的推动力

除了传统的金融、政务等应用外，越来越多的互联网应用可以使用密码产品

是云端自主可控的关键

计算、网络、存储是云服务的主要形式
唯有加密技术能够保证云端数据安全性

敏感数据保护 | 虚拟机加密 | 数据库加密 | 大数据安全 | 密钥管理

金融交易 | 政企应用 | 电子合同 | 数字版权保护 | 安防视频监控 | 区块链应用

目标：基于云加密和密钥管理能力，整合安全技术和安全应用，扩大云加密技术支撑能力和应用范围，共同为云计算行业发展保驾护航。

政务云密码支撑平台

金融云密码支撑平台

互联网密码支撑平台

云加密

安全产品厂商

基础软件厂商

构建云加密开放生态系统

云服务商

应用厂商

2005

信息安全服务

- 等级保护标准
- 信息安全咨询
- 攻防技术
- 安全测评
- 安全建设
- 安全运维

2009

国产商用密码产品

- 金融密码产品
- 政企密码产品
- 第一个全国产试点应用
- 视频加密、应急广播

2014

云密码技术领跑者

- 第一款产品
- 第一个商用服务

The 8th China Cloud Computing Conference

Thank you

TASS