



2017 中国互联网络安全大会
China Internet Security Conference

构建安全先行的金融云

张行

中国金融认证中心助理总经理

CFCA

中国金融认证中心
China Financial Certification Authority

引言

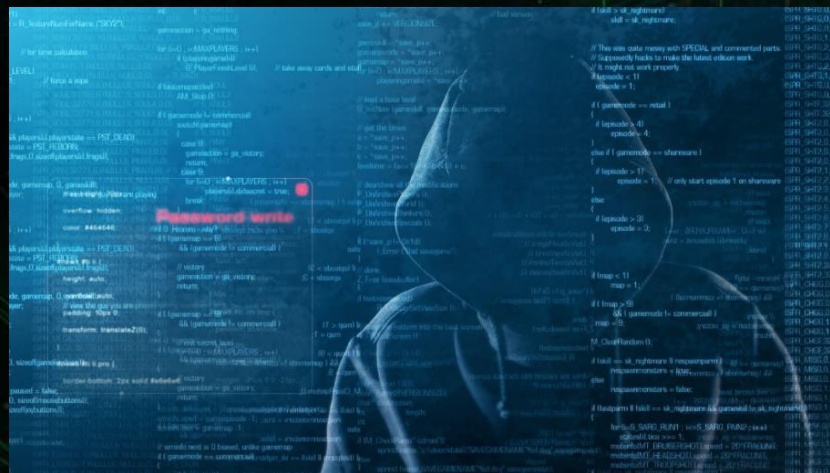
云计算的发展动态

国内各行各业也都在“跑步上云”。凭借云计算快速部署及专业管理，云计算部署模式已成为中小型企业的首选。基础服务和运维管理交给专业的云计算公司，以较低的成本获得快速的业务部署，而不需要自身构建IT服务系统，能让中小企业更加灵活的应对市场变化。弹性扩容，按需供给计算能力以应对突发意外的增长的特点吸引更多的大型企业采用云计算构建自己的服务系统。



引言

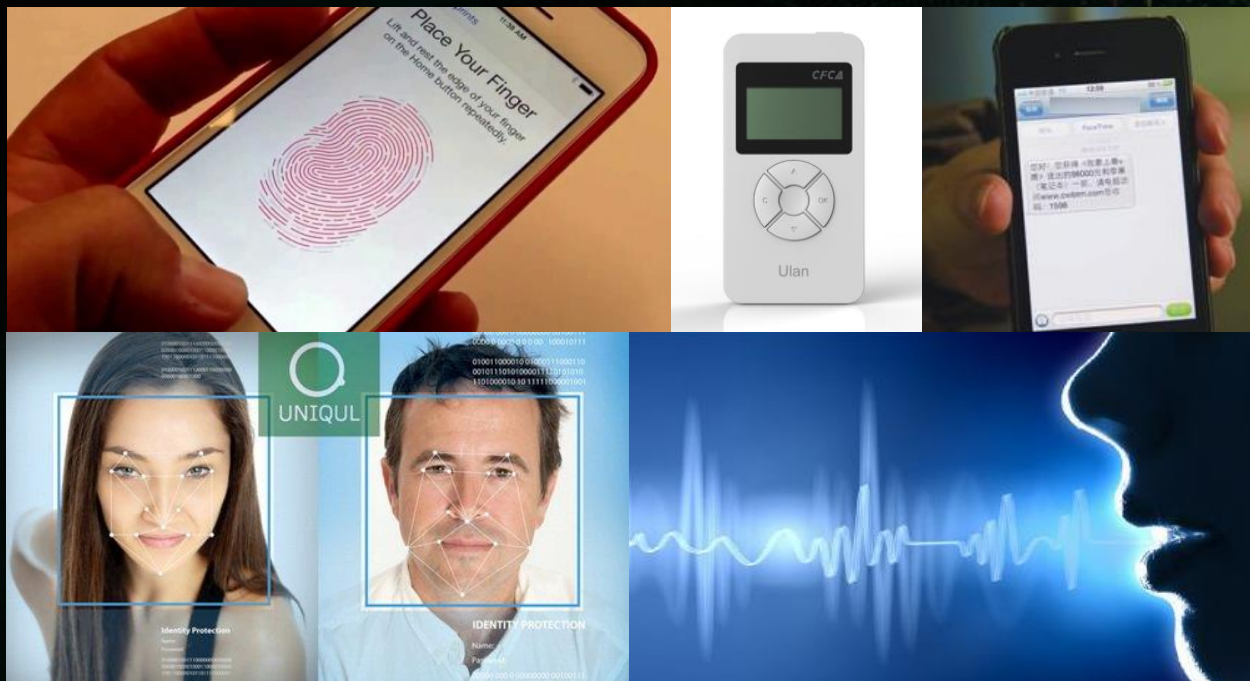
用户对数据安全的担忧



A1 身份认证

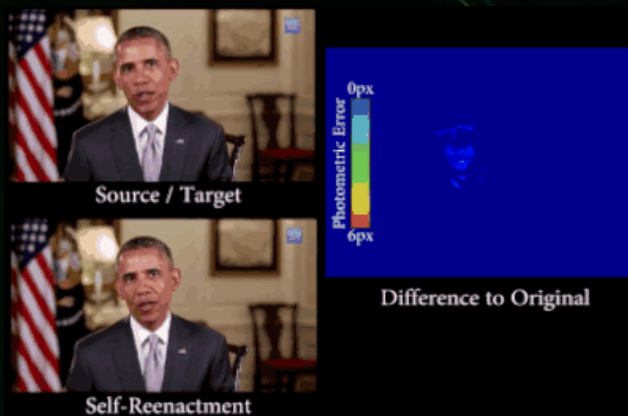
身份认证的几种方式

- / 指纹
- / 人脸
- / 虹膜
- / 声纹
- / 银行卡信息
- / 动态口令
- / 短信验证码
- / 数字证书等



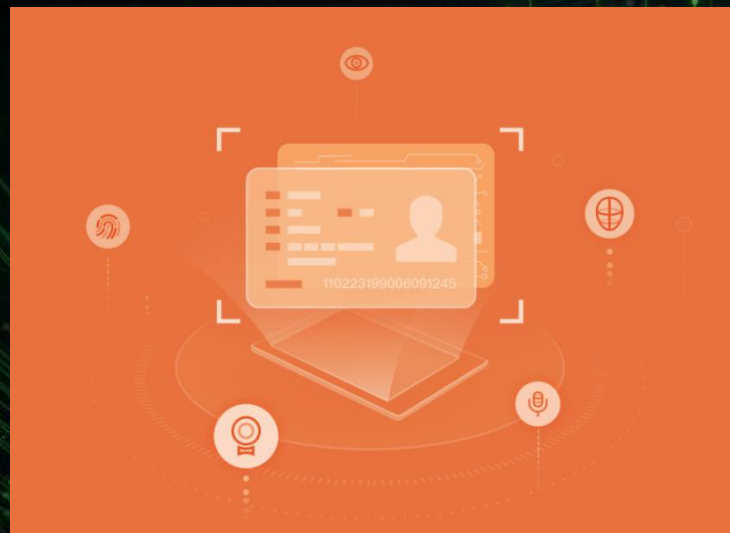
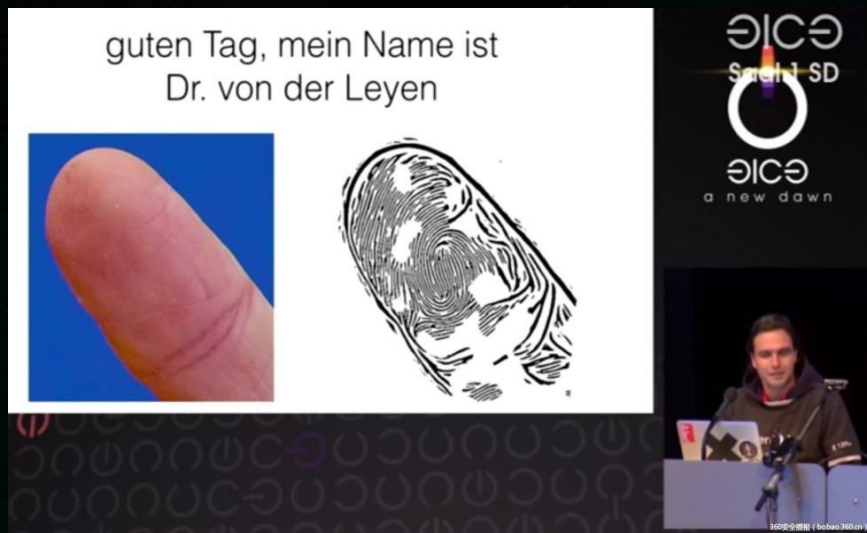
A2 身份认证

生物特征智能学习



A3 身份认证

PKI技术与生物技术相结合



A4 身份认证

PKI+生物识别技术的案例



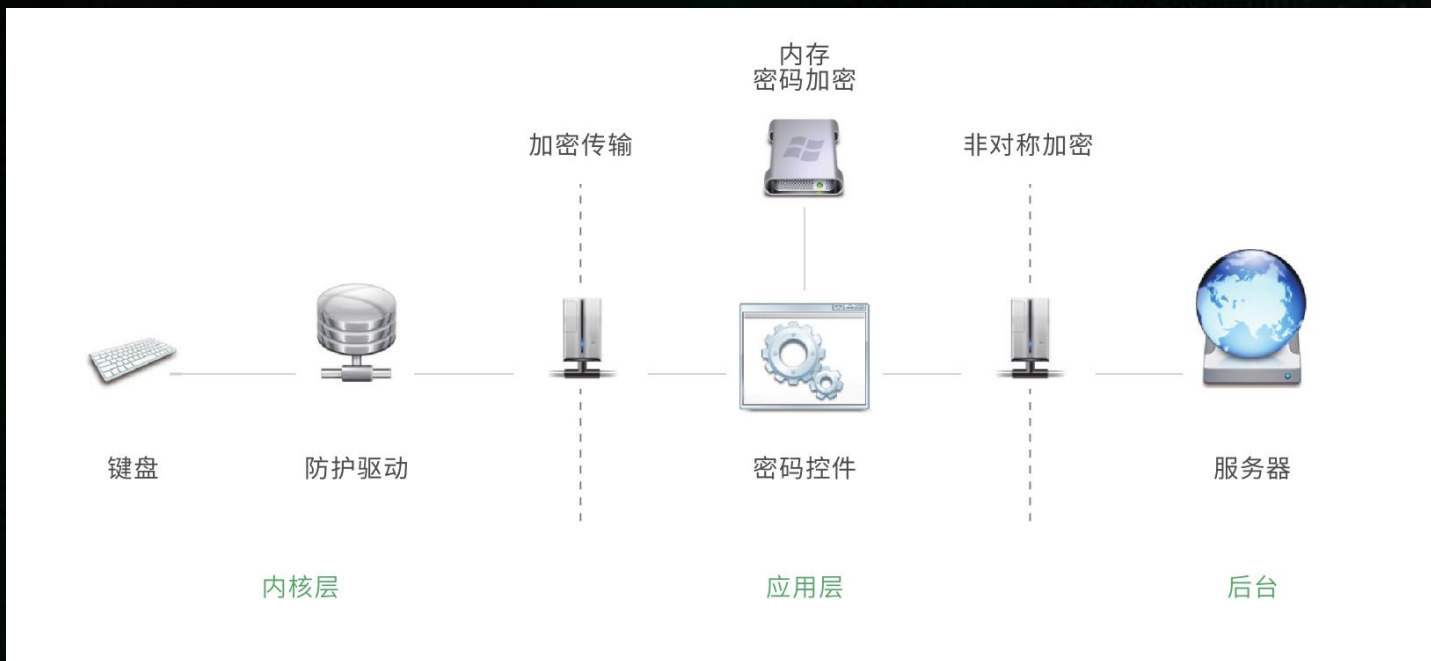
B1 数据源保护

数据安全输入产品



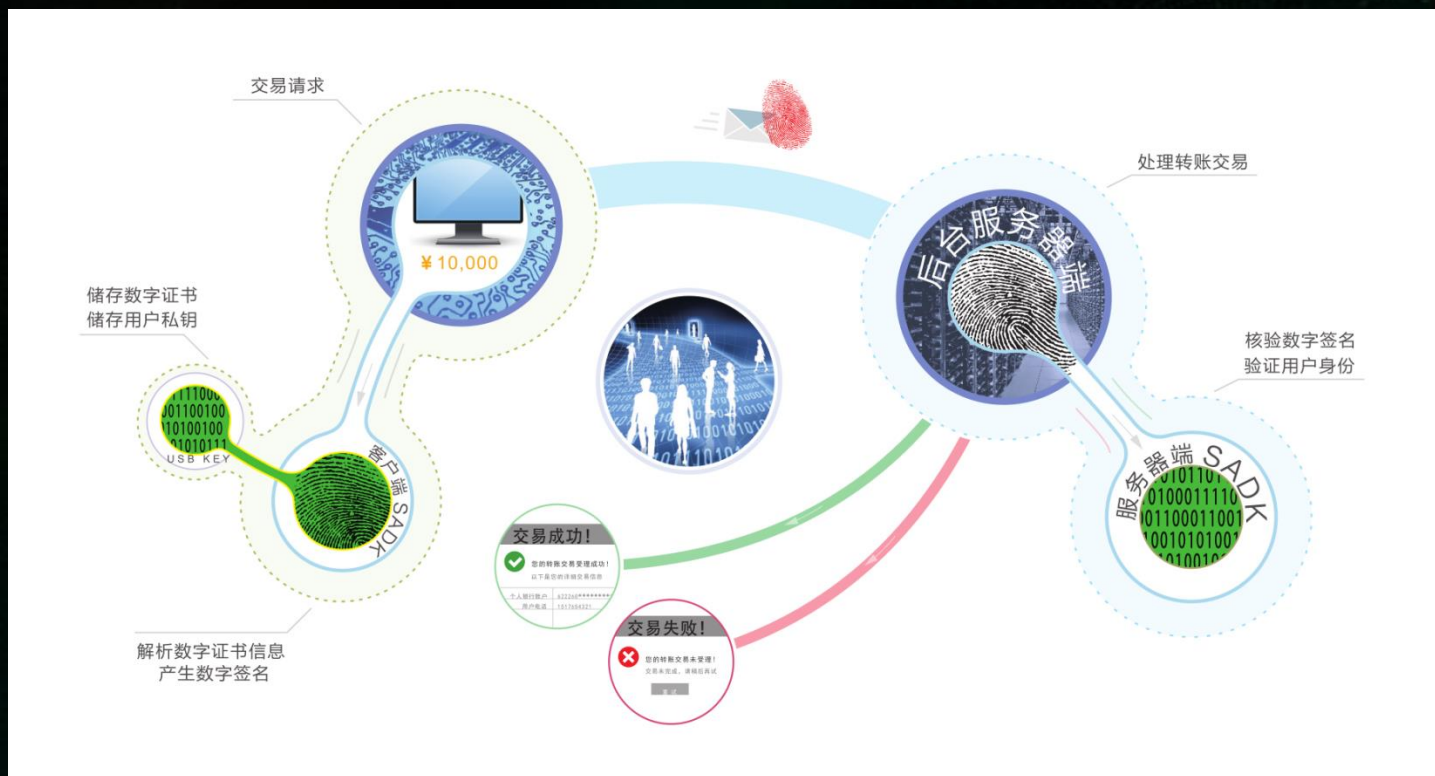
B2 数据源保护

敏感信息加密



B3 数据源保护

关键信息签名



B4 数据源保护

数据行为分析



Dwell Time

Key down Key up



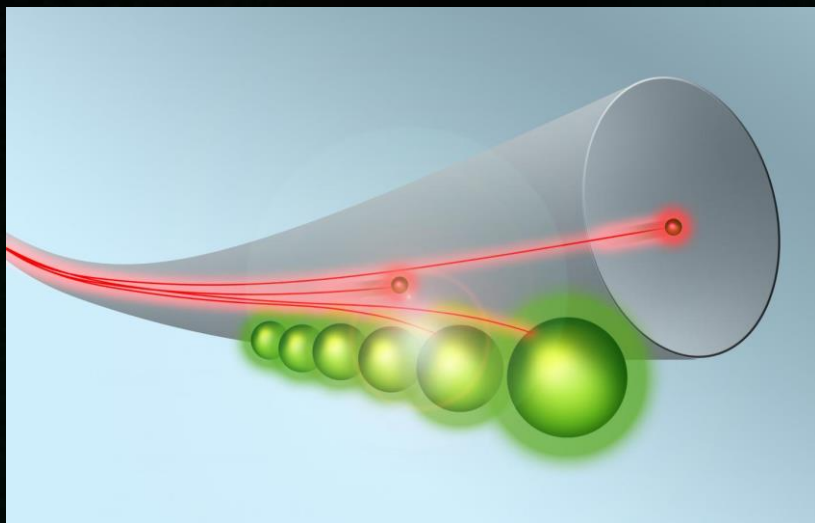
Flight Time

Previous
key up Next
key down



C1 数据传输安全

数据泄露与网络窃听



C2 数据传输安全

CFCA是国内唯一入根四大浏览器厂商的全球服务器证书颁发机构



Internet Explorer



Chrome



Firefox



Safari



Adobe

绿色地址栏、HTTPS加密访问

安全锁标识

https://www.cfca.com.cn/ 中金金融认证中心有限公司 (CN)

申请机构名称

网站可信认证 ✓
100%国产化 ✓
全球信任 ✓

WebTrust pwc

WebTrust pwc

WebTrust pwc

CFCA 站点认证

D1 数据存储安全

基于海量密钥应用模式的签名和加密



D2 数据存储安全

基于海量密钥应用模式的签名和加密



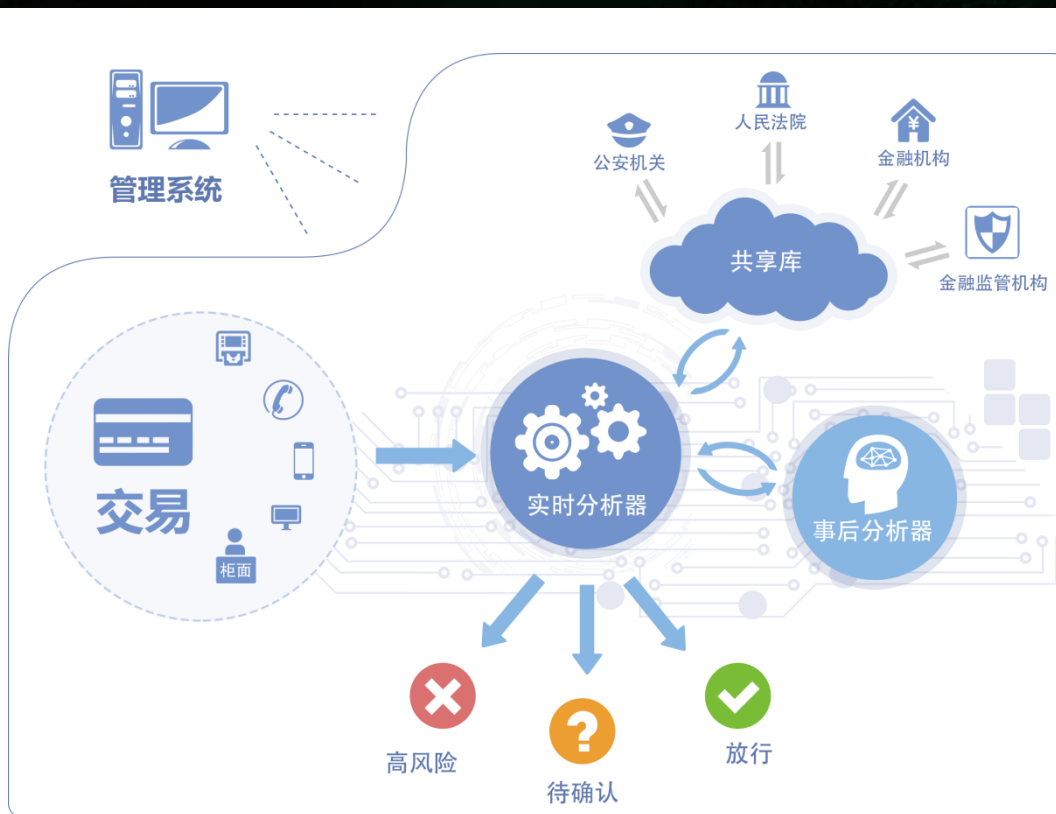
E1 数字签名

数字签名技术保证数据完整性、防篡改、防抵赖



F1 业务立体防护

机器学习等方法发现欺诈事件



展望

量子技术与PKI结合

量子物理与量子信息

量子计算与量子模拟

量子并行性

经典比特

0 或 1

00, 01, 10 或 11

000, 001, 010, ...

量子比特

0 + 1

00 + 01 + 10 + 11

000 + 001 + 010 + ...

万亿次计算机分解300位的大数

经典计算

量子计算

15万年

VS

1秒钟

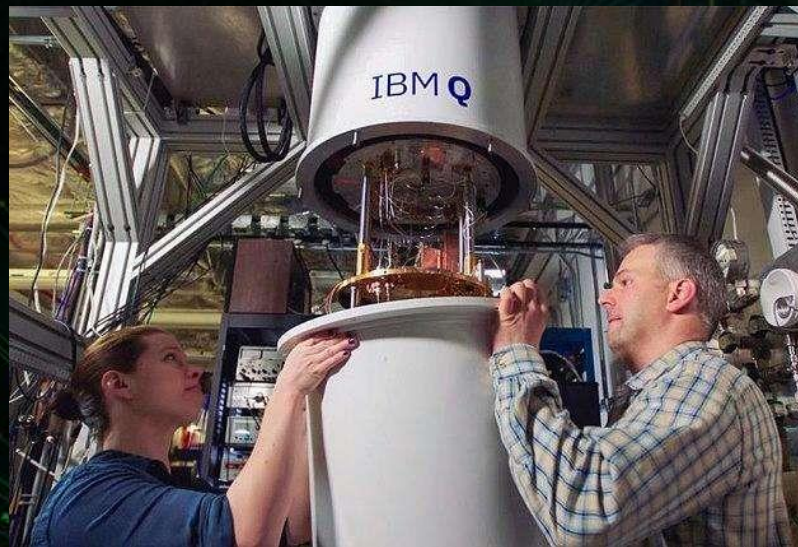
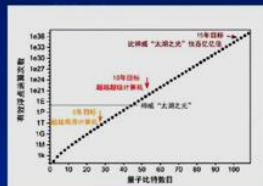
解决大规模计算难题

密码分析、气象预报、药物设计、金融分析、石油勘探.....

揭示新能源、新材料机制

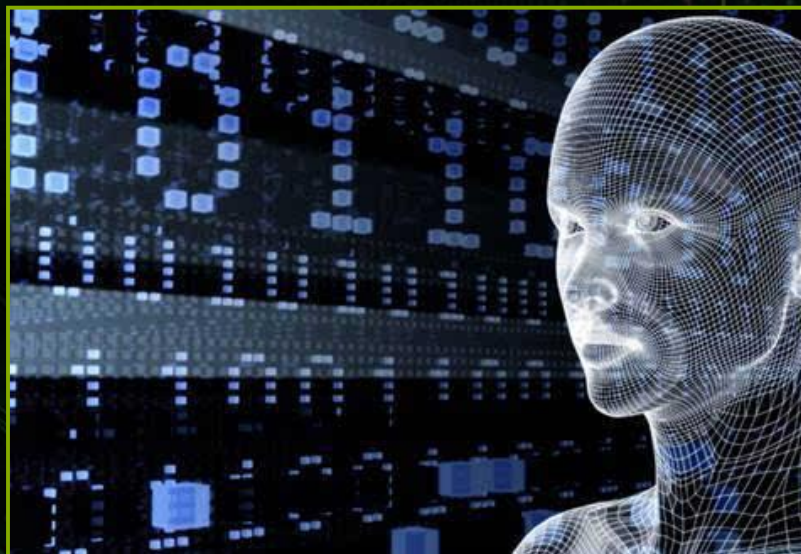
惯性约束核聚变、高温超导、高效固氮.....

计算能力随量子比特的
数目呈指数增长！



展望

人工智能



CFCA云上安全新方案

为云上客户提供全套产品服务



**传输安全
解决方案**



**安全存储
解决方案**



**电子合同/保单
解决方案**



**安全支付
解决方案**



**生物特征识别
解决方案**

谢 谢



中国互联网安全大会



360互联网安全中心