# 移动互联网时代下的身份安全探讨

张 行

中国金融认证中心副总经理

作者版权所有
请勿转载

# 你是谁




作者版权所有
请勿转载

On the Internet, nobody knows you're a dog.

# 移动互联到万物互联



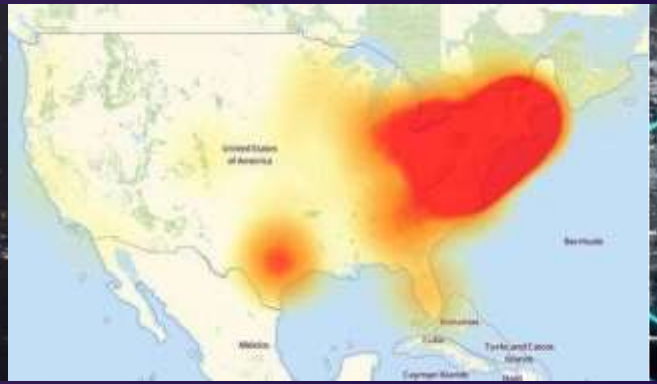



作者版权所有
请勿转载

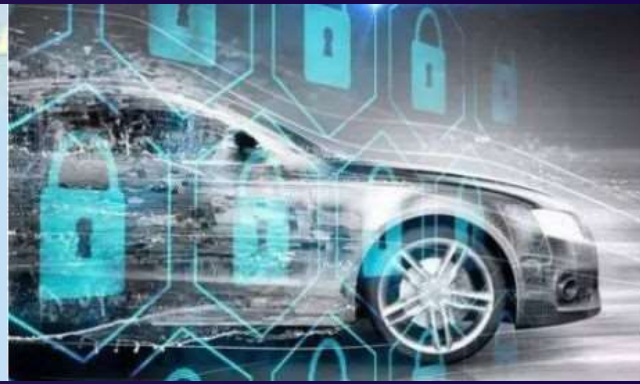
# 身份即安全



乌克兰停电危机



美国网络瘫痪事件



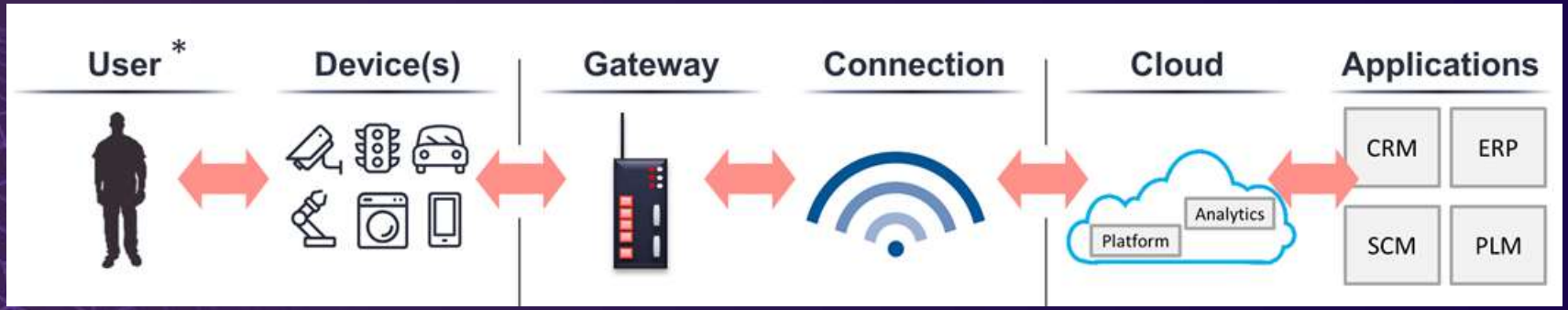
无人驾驶汽车被远程控制

作者版权所有
请勿转载

# 身份安全问题



用户 | 终端设备 | 网关 | 云服务 | 业务系统




作者版权所有
请勿转载

用户及设备身份安全

云端身份安全

# 分层次多维度的身份认证体系



| | | | | | |
|---|---|---|---|---|---|
| **应用层** | 商业银行 | 电商平台 | 供应链平台 | 互联网金融 | … … |
| **平台层**<br>（在法律框架下可监管、可审计） | 征信服务平台 | CFCA数据服务平台 | … … | | |
| **社会资源** | 金融 | 医疗卫生 | 教育 | 通信 | 保险 | … … |
| **权威数据** | 人口数据 | 工商数据 | 税务数据 | 社保数据 | … … |

作者版权所有
请勿转载

# 用户身份鉴别模型




作者版权所有
请勿转载

# 身份安全需求




作者版权所有
请勿转载

# 身份凭证




作者版权所有
请勿转载

# 数字证书与第三方电子认证




公钥是公开的，不再担心被窃听，但是接收者依然无法判断收到的公钥是否是合法的，因为有可能是中间人假冒的。事实上，仅靠公钥密码本身，无法防御中间人攻击。于是，需要（认证机构）对公钥进行签名，从而确认公钥没有被篡改，加了数字签名的公钥称为 **数字证书。**

有了数字证书作为证明，可以有效的防御中间人攻击，随之带来了一系列非技术性工作，例如，谁来发证书？如何发证书？不同机构的证书怎么互认？纸质证书作废容易，数字证书如何作废？解决这些问题，需要制定统一的规则，即CA认证。**只有合法、公正的第三方CA认证机构，才能保障整个PKI体系的安全。**

# 公钥基础设施



**公钥基础设施**（Public Key Infrastructure，PKI）是指支持公钥管理体制的基础设施，提供鉴别、加密、[illegible]的不可否认性服务。通俗的讲，PKI是集机构、系统（硬件和软件）、人员、程序、策略和协议为一体，利用公钥概念和技术来实现和提供安全服务的、具有普适性的安全基础设施。


作者版权所有
请勿转载

# 基于PKI身份凭证的安全应用



供应链金融

电子政务


区块链

手机银行

电子招投标

作者版权所有
请勿转载

消费金融

...

# 生物识别与人工智能



## AI 模拟脸部动作，伪造视频

“奥巴马”：“特朗普总统完全就是个笨蛋。”

作者版权所有
请勿转载

# 生物识别与人工智能



## AI 模拟脸部动作，伪造视频

作者版权所有
请勿转载

明星换头：成功将神奇女侠女主角盖尔加朵的脸移植到一名成人女演员身上

# 数字证书+生物识别，可以形成多证据链、多因子的安全认证过程



CFCA与生物识别厂商在金融领域合作的案例


作者版权所有
请勿转载

# 移动端安全



**轻量化**

解决硬证书在移动终端中普及率低的痛点

**系统兼容**

保持与现有PKI认证系统的技术一致性，无需额外系统建设

**易用性好**

支持指纹、人脸、虹膜等生物特征识别技术



# 数字证书+TEE+SE+生物识别，可以保障交易安全、改善用户体验



在TEE可信任执行环境中进行支付交易时，调用SE安全单元中数字证书进行电子签名的环节，不再输入密码，而是通过按个指纹或者其它生物识别技术来完成交易；同时数字证书还可以对生物特征进行加密，保障生物特征存储与传输的安全。数字证书、电子签名能够保障关键交易的完整性、不可否认性、机密性以及法律效力；生物识别技术则能够为用户带来便捷、顺畅的用户体验。

作者版权所有
请勿转载

在TEE可信执行环境下完成电子签名；数字证书存储于SE中，不可导出、安全性高

# 站点身份与安全



2018年5月24日，欧盟正式颁布GDPR（General Data Protection Regulation，通用数据保护条例）并开始实施，强调要求欧盟成员国境内个人隐私数据使用安全方式进行传输和保存 。

美国发布HTTPS-Only标准，要求所有的联邦政府网站2016年12月31以前必须使用全站HTTPS加密连接。截至到2018年12月31日，美国政府使用的.gov域名SSL证书使用率已达到100%。

苹果要求开发者必须使用ATS（APP Transport Security APP传输安全）保护数据传输安全，即iOS应用内的链接使用HTTPS连接。自2017年1月1日起，所有iOS应用**必须**使用ATS才能满足商店（App Store）发布要求，否则将拒绝审核并下架不符合要求的应用。



谷歌发布Chrome 68版本操作系统，所有未部署SSL证书的网站均会被标记“不安全”的提示。

# 站点身份安全与加密传输



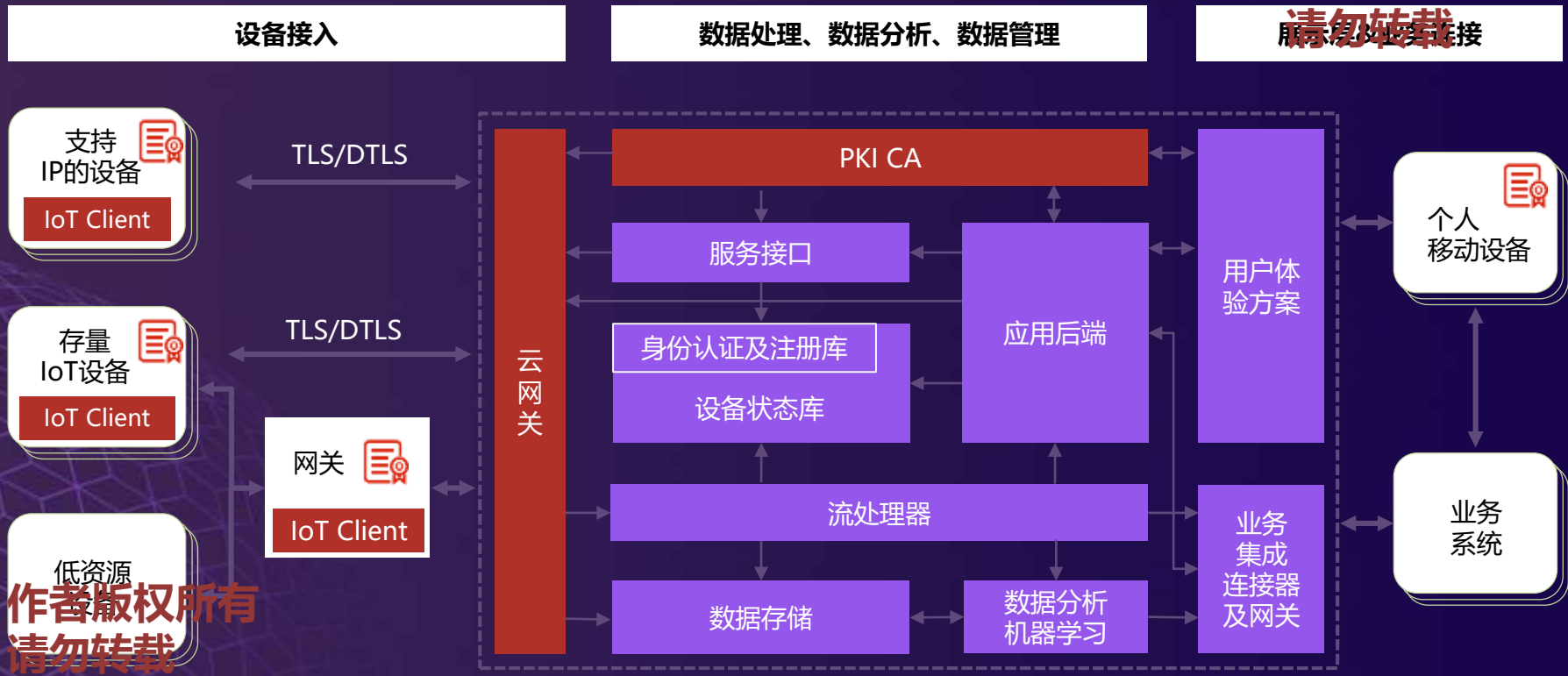
Internet Explorer　Chrome　Firefox　Safari　Adobe


作者版权所有
请勿转载

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

# 物联网安全体系





# 设备身份安全



- 数据采集设备
- 车联网
- 智能医疗设备
- WIFI 智能路由器
- 智能家居系统
- 机器人
- 工业自动化
- 装备智能制造
- 可穿戴设备
- 家居安全系统
- 智能视频监控

作者版权所有
请勿转载

# 多维度防范，保证身份及交易安全

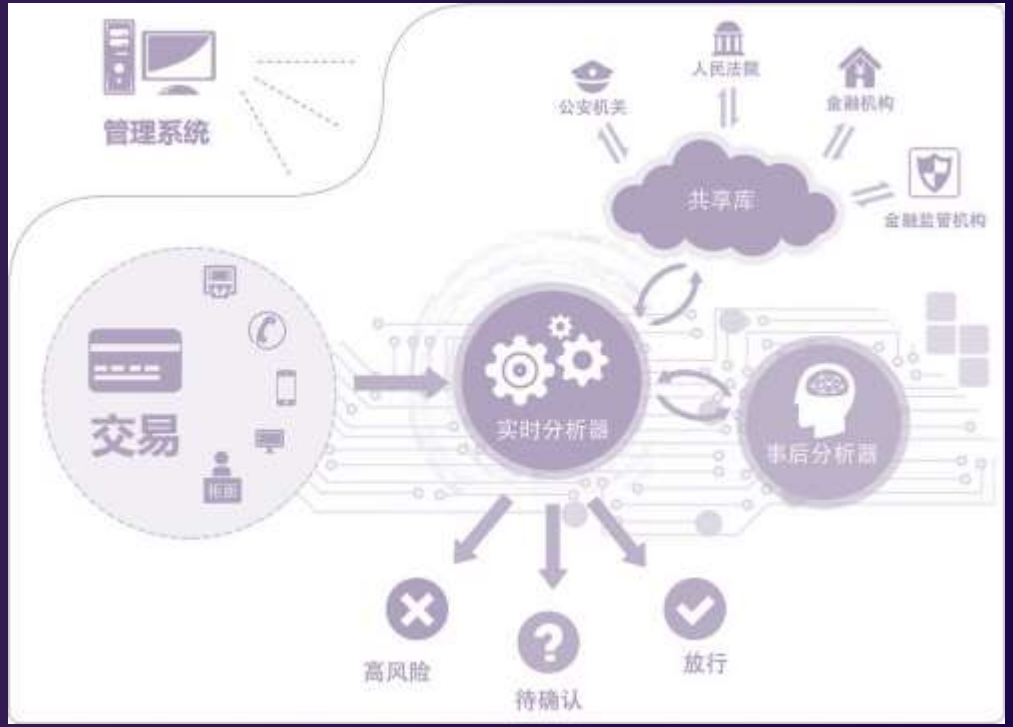


大数据

反欺诈

协同防范

作者版权所有
请勿转载



# 谢 谢!

作者版权所有
请勿转载