

基于智能穿戴设备的认证与支付应用探讨



汪雪林

北京握奇数据系统有限公司

目 录



1 认证与支付技术发展趋势概述

2 基于智能穿戴设备的认证与支付解决方案

3 握奇实践分享

4 未来展望

现阶段广泛使用的认证与支付工具



现阶段广泛使用的认证与支付工具



认证与支付工具演进趋势

高通计划以370亿美元收购NXP

2016-10-25 09:24:24 来源: usinenouvelle

内容摘要

高通（Qualcomm）计划以370亿美元的价格收购NX公司，收购NXP对于高通来说，将加强其在汽车行业组件市场上的份额，以抵消智能手机销量的下滑。



据外媒2016年10月21日的最新报道称，相关人士透露称高通（Qualcomm）计划以370亿美元（约合340亿欧元）的价格收购NXP Semiconductors的协议即将达成。

收购NXP对于高通来说，将加强其在汽车行业组件市场上的份额，以抵消智能手机销量的下滑，以及来自中国和台湾竞争对手的影响。

据消息人士称，高通最终以110美元每股的价格收购NXP，下周双方将正式对外发布此次收购合作。不过，该消息人士还表示，现在并没有确定，一切都可能在最后一分钟发生改变。

到目前为止，高通和NXP并没有立即回应这一信息。

受此消息影响，NXP在证券市场上的股价在当天14:35GMT下跌了2.75%至101.65美元，而高通的股价则是上涨了2.26%至68.86美元，这表明投资者更看好高通公司。

（本文由科技世界网编译，如需转载，请注明来源自 [科技世界网](#)）

中金国盛认证中心

华为麒麟960芯片通过移动金融技术服务认证

2016-10-18 中金国盛认证中心

华为麒麟960芯片通过
移动金融技术服务认证

【中国，北京，2016年10月18日】中金国盛认证中心宣布，华为公司研发的麒麟Kirin 960（HiSEC1.0）手机芯片由中金国盛认证中心授权的检测机构检测，经中金国盛认证中心进行认证,符合《JR/T0098.2-2012 中国金融移动支付 检测规范 第2部分：安全芯片》标准要求,通过移动金融技术服务认证（证书编号：CFNR201602810005）。

移动金融技术服务认证是中金国盛认证中心依据人民银行发布的《中国金融移动支付技术标准》而设立的一项认证制度,经过国家认监委批准于2014年开始实施。该认证制度通过对移动金融业务中关键环节产品的检测认证，对通过检测认证的机构证明由中金国盛认证中心颁发认证证书证明其相关产品的标准符合性和安全性，并在证书有效期内对获证机构相关产品进行监督审核，确保其持续符合。中金国盛认证中心作为辅助社会监管、推动标准落地的重要手段和工具，开展移动金融技术服务认证，致力于推动移动金融产业的健康、蓬勃发展。

麒麟Kirin 960（HiSEC1.0）芯片具备核心技术，采用16nm FFPlus工艺，具备防物理攻击能力，不用通过额外的安全元件即可满足智能手机的安全要求，实现安全可控，为数字普惠金融、保护金融消费者权益提供了保障。

中国移动 VPN 下午7:28 24%

source.android.com

Source Devices Security Compatibility

Trusty TEE

Trusty is a set of software components supporting a Trusted Execution Environment (TEE) on mobile devices.

Trusty consists of:

- An operating system (the Trusty OS) that runs on a processor intended to provide a TEE
- Drivers for the Android kernel (Linux) to facilitate communication with applications running under the Trusty OS
- A set of libraries for Android systems software to facilitate communication with trusted applications executed within the Trusty OS using the kernel drivers

Important: Trusty and the Trusty API are subject to change.

For information about the Trusty API, see the [API Reference](#).

Uses and examples

Any TEE OS (not just Trusty) can be used for TEE implementations.

A TEE processor is typically a separate microprocessor in the system or a virtualized instance of the main processor. The TEE processor is isolated from the rest of the system using memory and I/O protection mechanisms supported by the hardware.

TEE processors have become a mainstay in today's mobile devices. The main processor on these devices is considered "untrusted" and cannot access certain areas of RAM, hardware registers and fuses where secret data (such as device-specific cryptographic keys) is stored by the manufacturer. Software running on the main processor delegates any operations that require use of secret data to the TEE processor.

The most widely known example of this in the Android ecosystem is the [DRM framework](#) for protected content. Software running on the

为了安全，总是握奇

a.com.cn

认证与支付工具演进趋势

平台化：

随着手机性能和安全性的提升，手机逐渐演变成为安全平台和应用平台

应用化（去硬件化）：

各种认证与支付工具成为手机上的一个软件应用程序

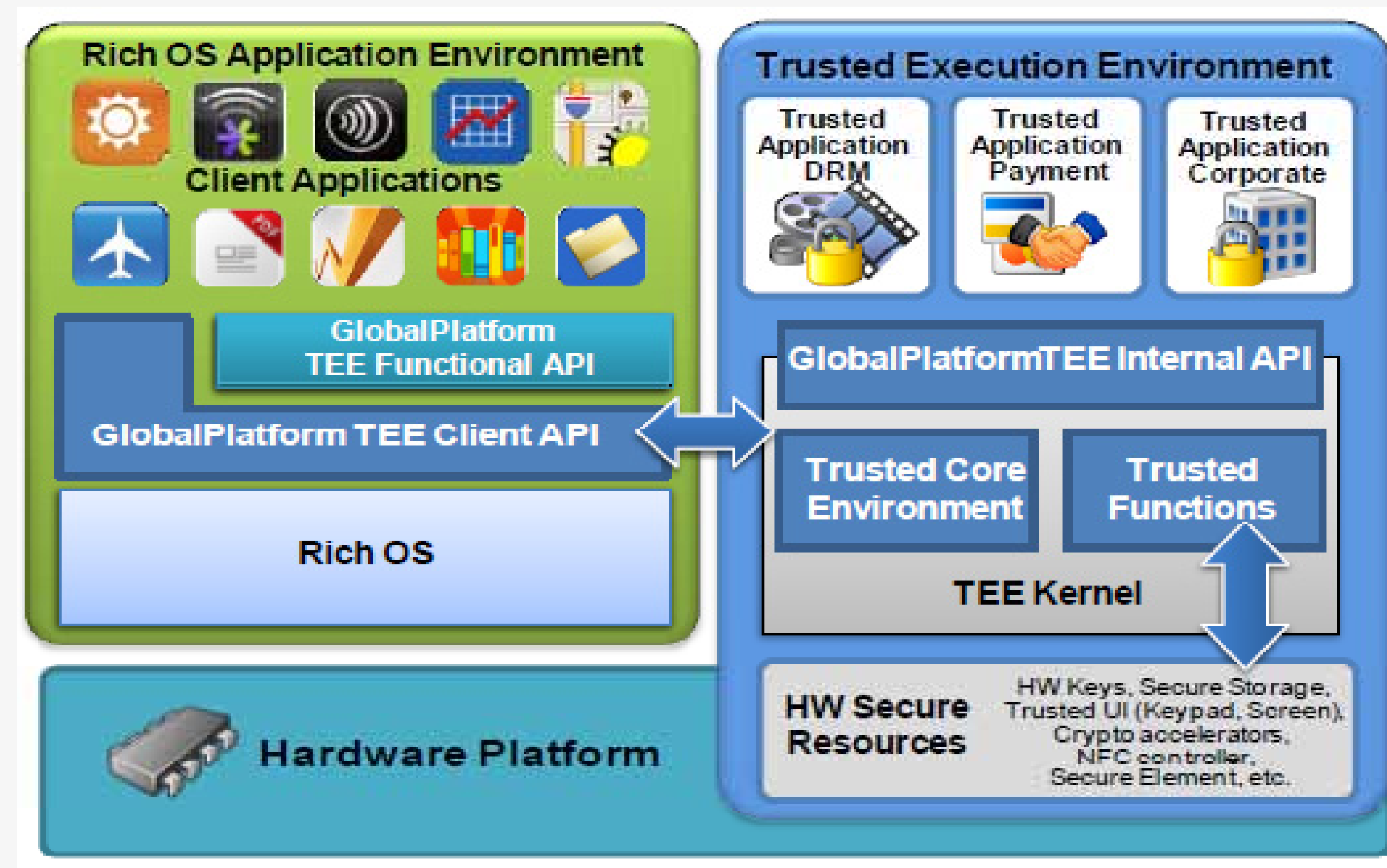
手机作为安全平台的技术基础

硬件：性能和接口能力的提升

基于硬件的安全能力（如TrustZone）

安全：TEE、SE、生物认证

协议或标准：FIDO、HCE、
IFAA、SORTER



目 录



1 认证与支付技术发展趋势概述

2 基于智能穿戴设备的认证与支付解决方案

3 握奇实践分享

4 未来展望

为什么选择智能穿戴设备？

TEE解决方案面临的安全问题

TrustZone不再安全 白帽黑客任意指纹解锁华为P9Lite

2016-10-24 11:03:55 6404 次阅读 0 次推荐 稿源：雷锋网 8 条评论

来自美国的安全研究团队Shellphish在GeekPwn大会上展示了通过篡改TrustZone里的指纹验证模块，任意指纹及皮肤接触即可解锁华为P9 Lite手机的技术。他们利用了HUAWEI P9 Lite中 Trustzone的漏洞，实现手机的信息泄露，并在华为信任运行环境中进行本地提权，从而获得从0权限到root到Trustzone的代码执行权。通过利用这些漏洞，攻击者不仅能获得安全区的敏感数据，还能直接进入支付等最高权限场景。





这个漏洞也可以被用于攻击HUAWEI P9系列的更早的型号（比如P8 Lite）。任何使用HUAWEI TrustZone的HUAWEI设备很可能都受到这个漏洞的影响。指纹识别搭配TrustZone作为最新的手机安全技术，曾被视为手机安全的最后一道防线。但是现在黑客突破了这道防线，令TrustZone的分区保护形同虚设。

除了华为P9lite任意指纹解锁的破解，在此次GeekPwn白帽黑客大会上，传奇黑客Geohot现身讲述他从黑客转型人工智能研究的心路历程，身残志坚的小霍金 “Stephen Chave” “现场攻破自己所乘坐的医疗轮椅。

三星Galaxy S5最新漏洞：黑客可窃取用户指纹数据

JackFree 2015-04-28 +3 共45344人围观 发现 7 个不明物体 漏洞 资讯



火眼（FireEye）安全研究人员在三星Galaxy S5中发现了一个新漏洞。尽管Galaxy手机对指纹进行了加密，但黑客仍然可以克隆手机中的用户指纹数据，进而还原指纹图像，冒充受害者身份。

为什么选择智能穿戴设备？



VS



- 应用与认证模块集成度高，用户体验好；
- 应用受攻击面大；
- 产业链复杂，上下游协调困难；
- 产品生命周期短，与安全认证设备生命周期矛盾
- 盈利模式不清晰

- 应用与认证分离，用户体验较好；
- 认证设备独立于应用，风险控制难度小；
- 产品生命周期独立于终端应用设备
- 盈利模式清晰

为什么选择智能穿戴设备？

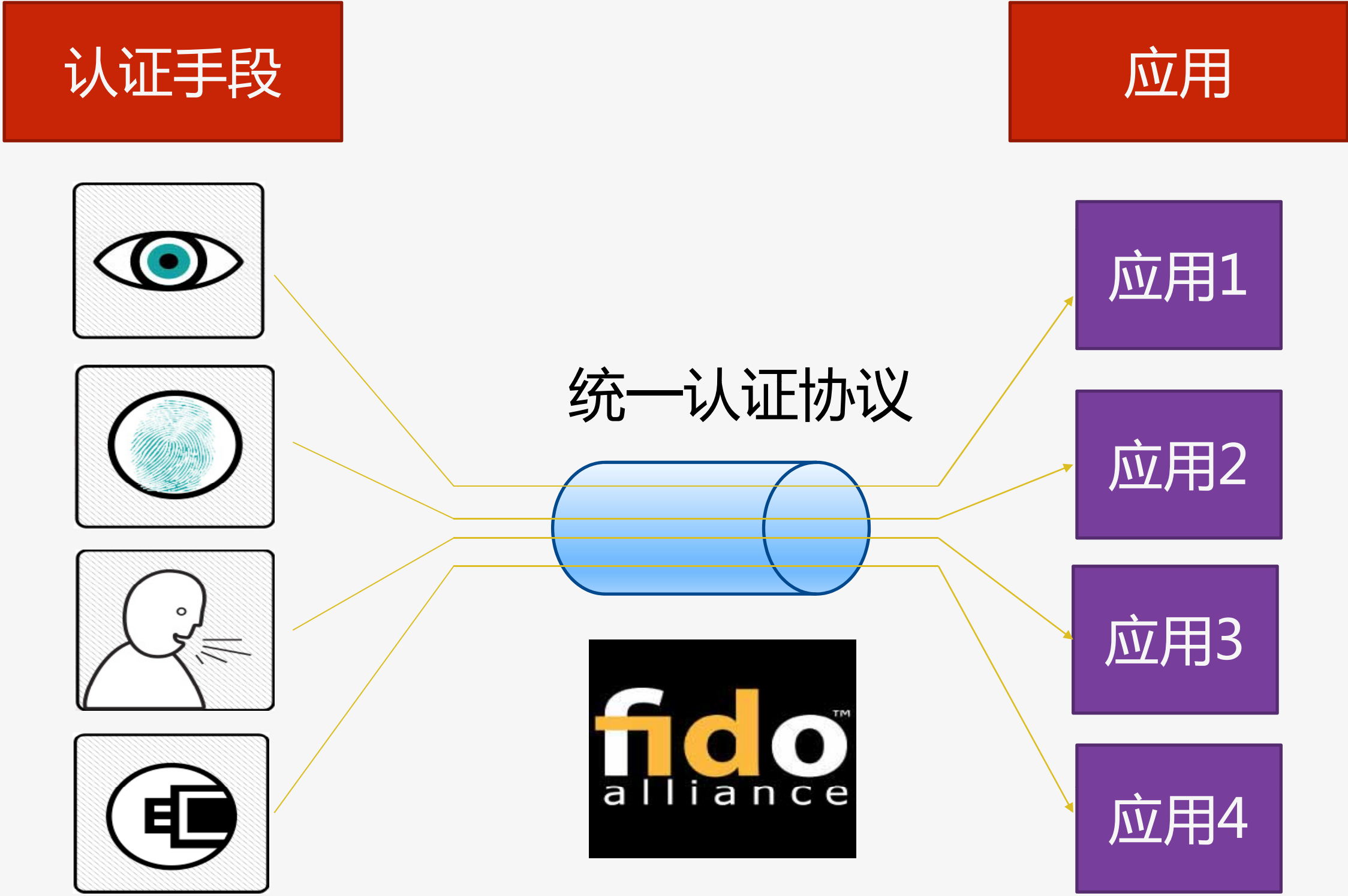
- ◆ 智能穿戴设备是继手机之后的另一个安全平台和多应用平台
- ◆ 可作为独立的认证和支付设备，具有更高的安全性
- ◆ 用户对智能穿戴产品功能预期：认证与支付功能位居第二
- ◆ 认证与支付功能是一种强用户黏性的应用，可作为穿戴设备的杀手级应用

智能穿戴设备的认证和支付应用是业内关注热点



智能穿戴设备的认证和支付应用是业内关注热点

FIDO——一种轻量级身份认证和安全支付解决方案



- 将认证方式与认证协议分离
- 支持尽可能多的认证方式，充分利用现用硬件设备内嵌的安全能力
- 支持不同的安全级别，使得网络服务提供商能够了解设备具有的认证方式和能力并设置认证策略
- 保护用户隐私，使得用户信息不被泄漏且无法被追踪
- 在所有用户的所有设备上对所有应用支持多样化的认证方式

智能穿戴设备的认证和支付应用是业内关注热点

FIDO——一种轻量级身份认证和安全支付解决方案

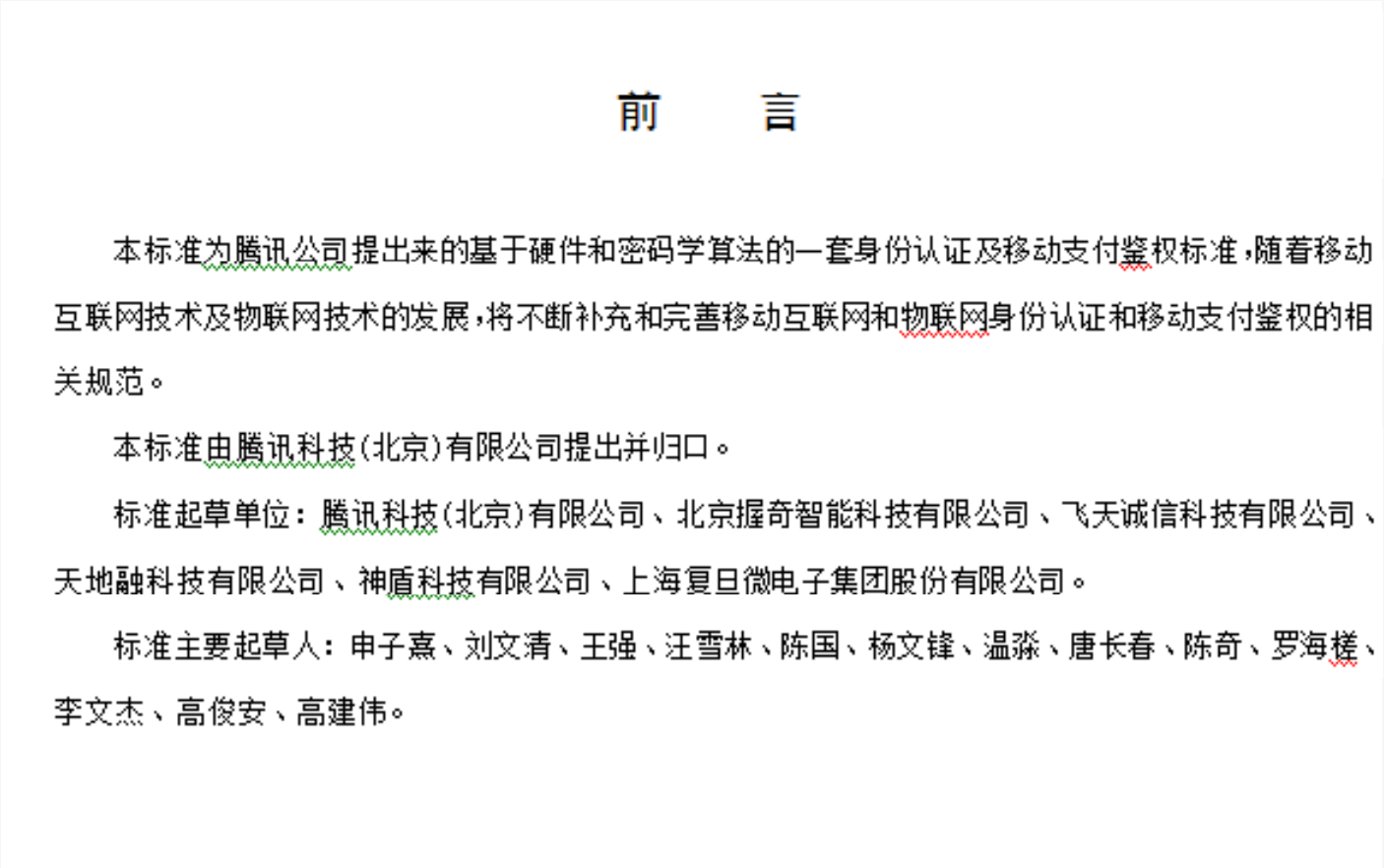


本地身份认证方式举例：

- 移动设备内置的指纹传感器
- PIN认证器，PIN验证在SE中
- 手机作为其它设备的认证器
- USB令牌内置用户存在验证技术
- 设备中内置声音或面部验证技术

智能穿戴设备的认证和支付应用是业内关注热点

腾讯及其领域守护计划



为了安全，总是握奇

智能穿戴设备的认证和支付应用是业内关注热点

QKey关注的应用场景



为了安全，总是握哥

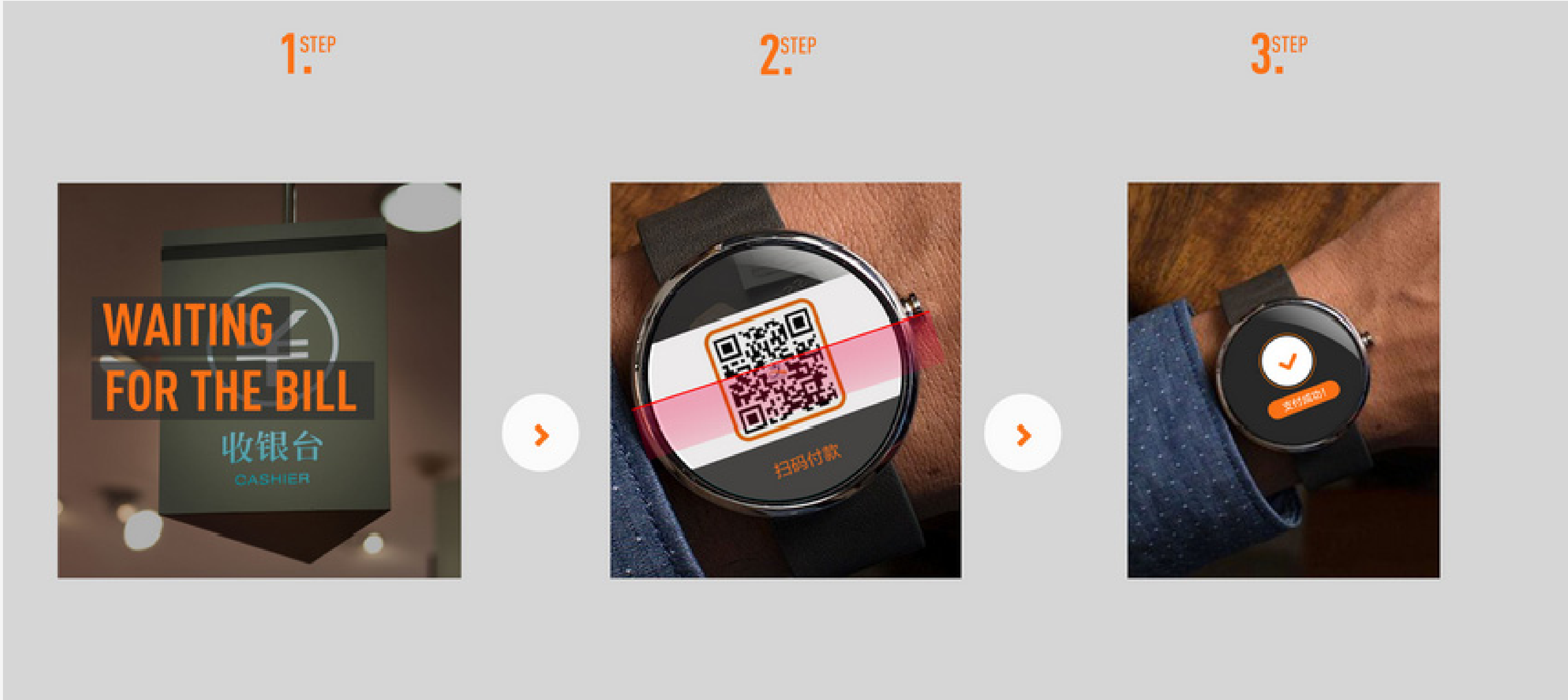
智能穿戴设备的认证和支付应用是业内关注热点

IFAA及其近场认证标准



智能穿戴设备的认证和支付应用是业内关注热点

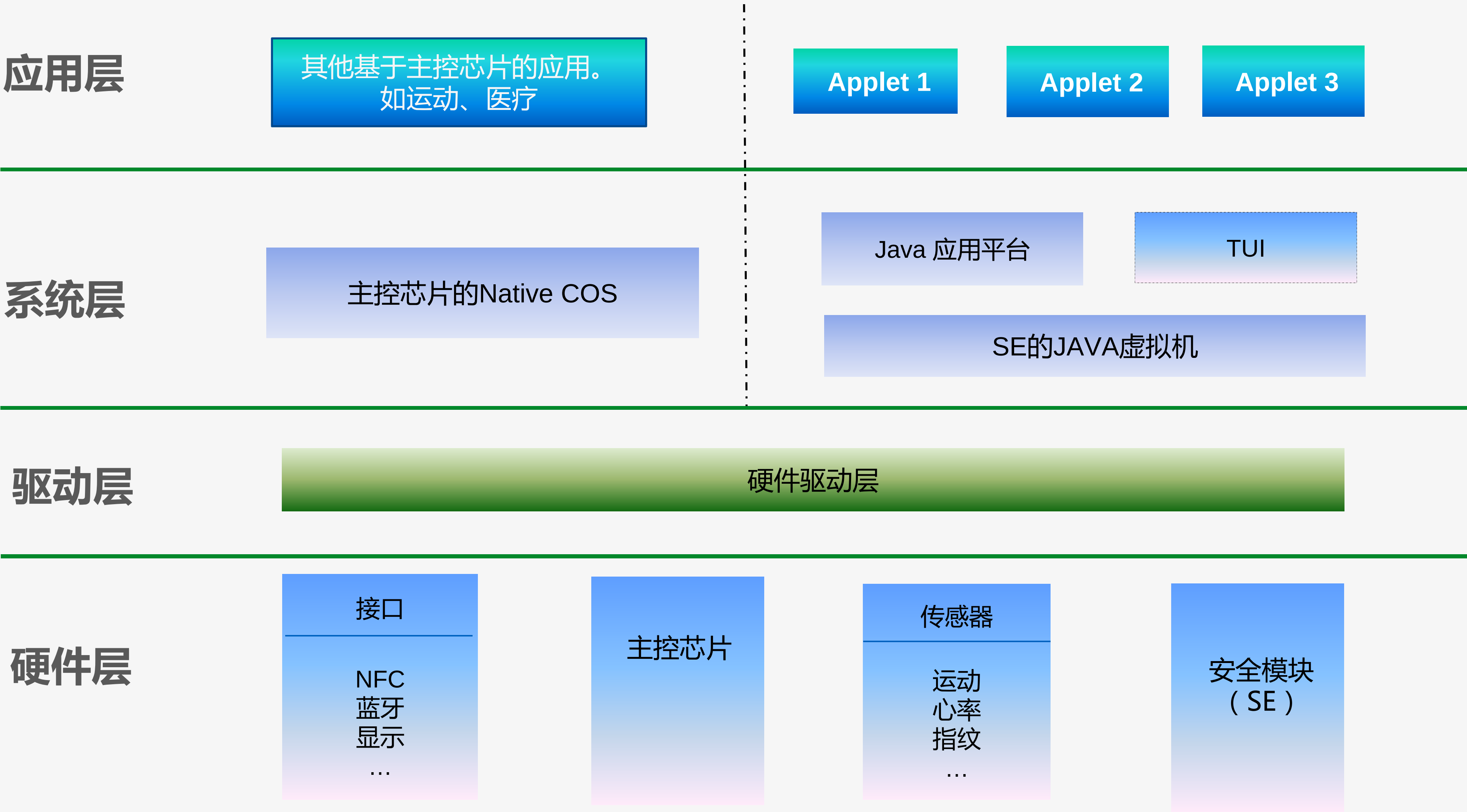
IFAA近场认证应用场景



基于智能穿戴设备的认证和支付应用



认证与支付智能穿戴设备的平台化技术

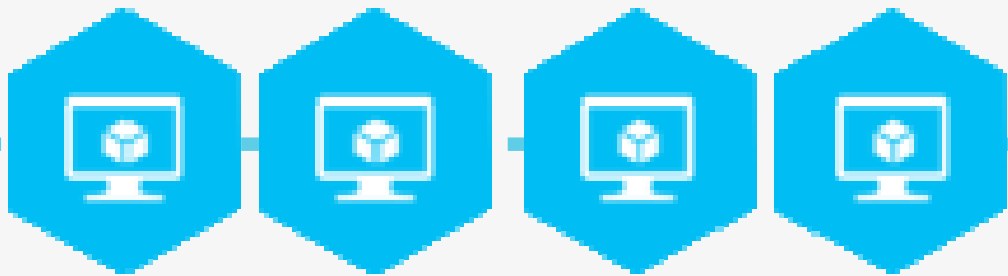
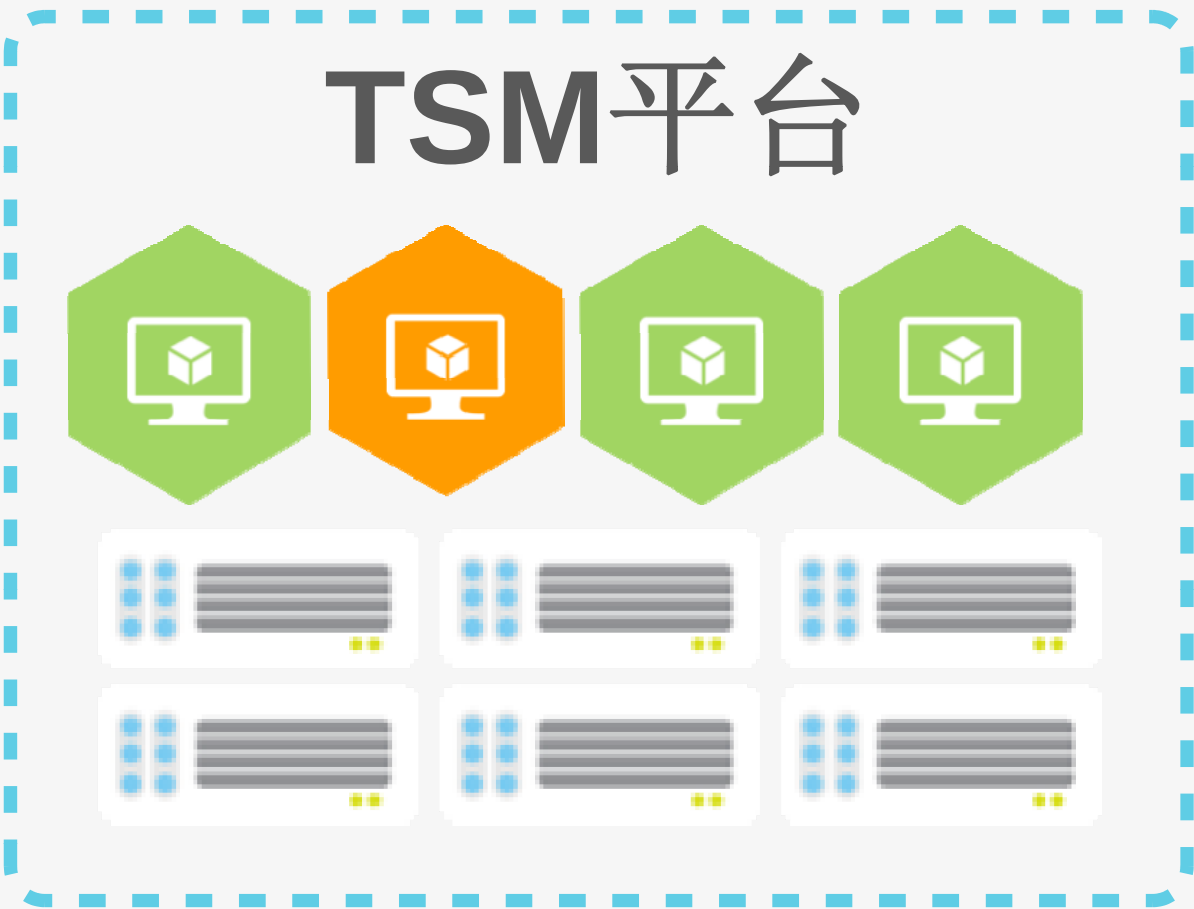
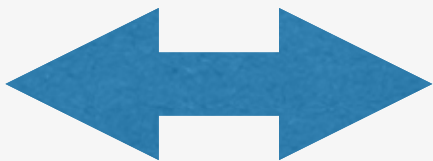


认证和支付智能穿戴设备的平台化技术



认证和支付智能穿戴设备的平台化技术

支持动态空中下载
支持多应用加载
支持发行后管理



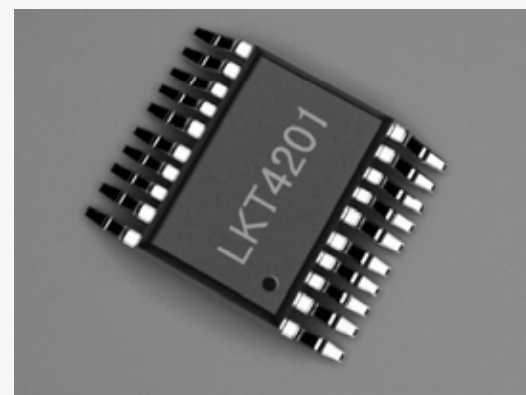
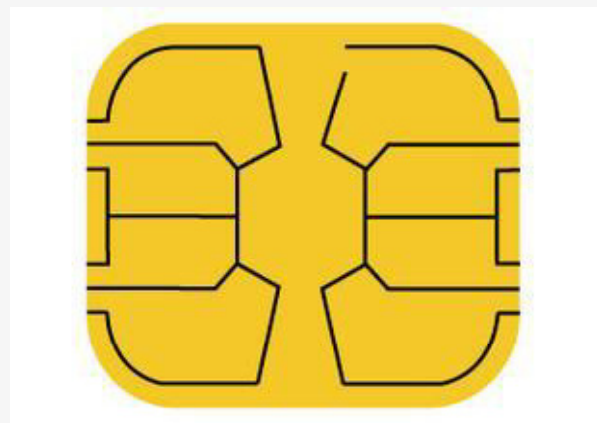
Java多应用平台



随时增加更多可能！

智能穿戴设备平台化的关键技术需求

SE



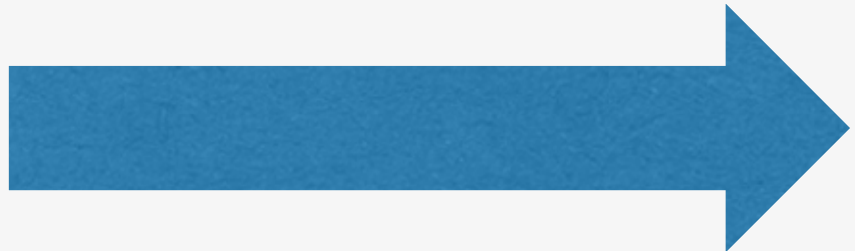
更大容量、更多接口、
更高性能、国密算法



系统平台

Javacard Platform

人机交互、异步处理



Javacard Platform + TUI

目 录



1 认证与支付技术发展趋势概述

2 基于智能穿戴设备的认证与支付解决方案

3 握奇实践分享

4 未来展望

握奇智能穿戴认证与支付产品



握奇第一代智能穿戴设备

握奇智能穿戴产品关键技术

有源射频技术

- RF感应距离、性能良好

应用功能

- PBOC3.0/MasterCard/Visa
- FIDO/TUSI/IFAA/网银U盾
- 住建部规范/交通部规范/各地规范

适配不同的手机操作系统



- Android
- iOS

COS统一平台

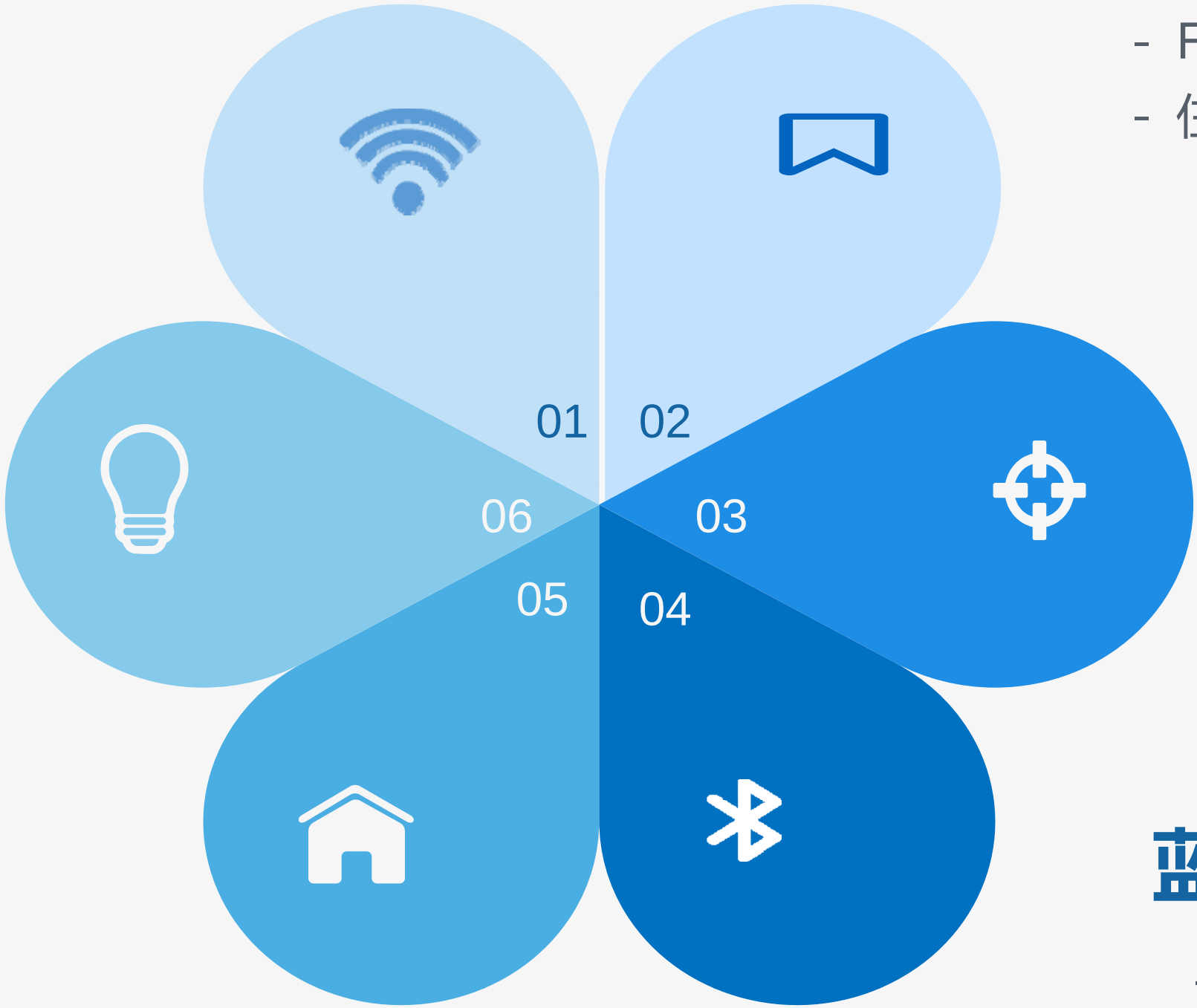
- 同一COS平台支持认证、交通、金融多应用
- 同一平台支持TypeA/TypeB/ISO18092协议规范

SDK标准接口

- 输出Android和iOS两套接口

蓝牙技术

- 支持金电MTPS蓝牙协议规范
- 支持银联蓝牙协议规范
- 支持FIDO U2F/UAF协议
- 支持TUSI蓝牙协议



握奇智能穿戴产品的高安全性

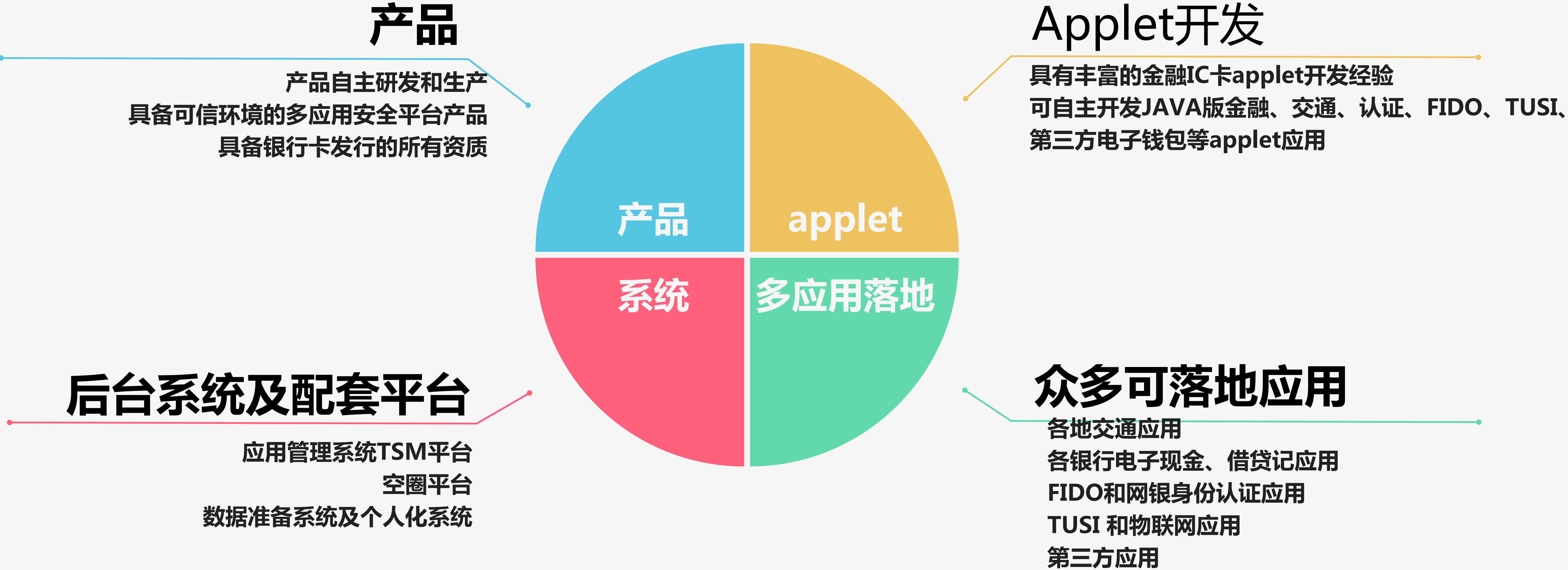


满足金融级别的多应用安全平台

握奇智能穿戴产品应用框架

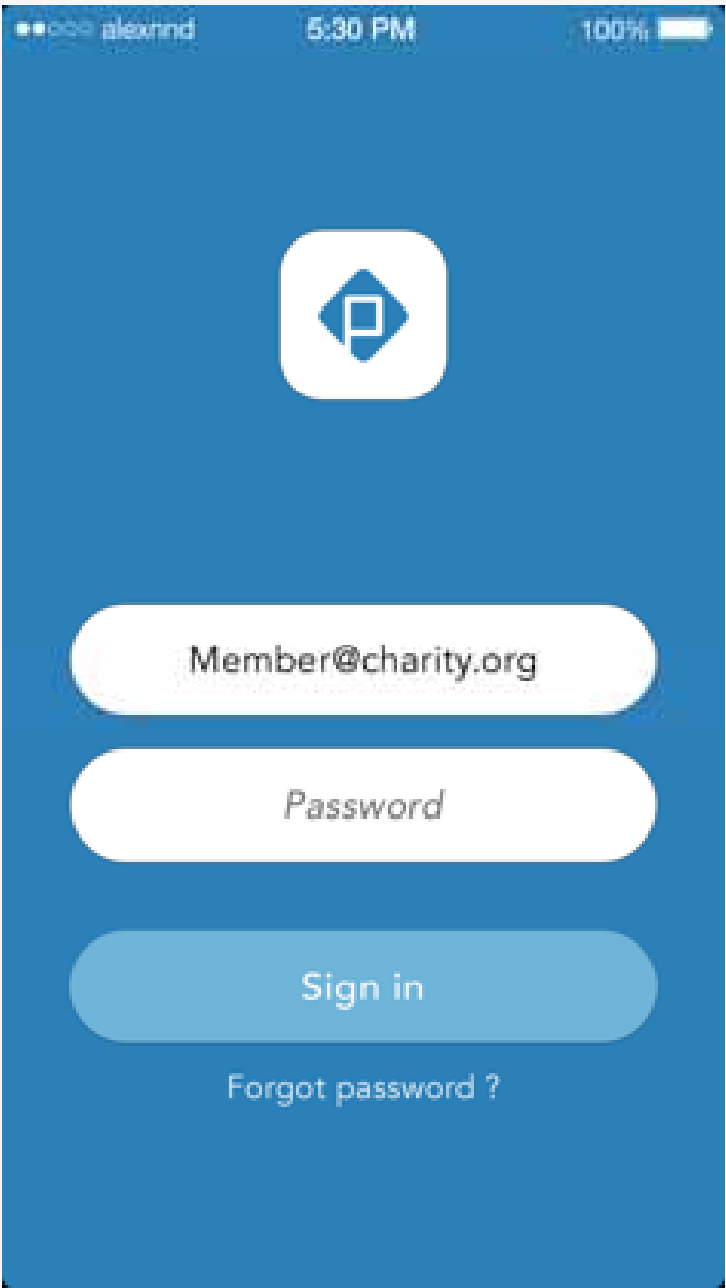


握奇智能穿戴一体化解决方案

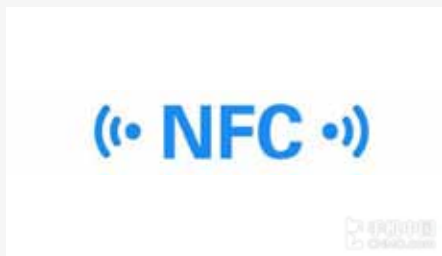


握奇可以提供整套解决方案

应用场景：线上身份认证



认证信息
→
←
认证签名



线上身份认证

通过蓝牙或NFC接口完成应用登录过程中后台与设备之间的认证过程

2

支持NFC或蓝牙接口

3

支持FIDO/TUSI/U盾
等各种规范

应用场景：线上支付安全



1 线上大额支付

对交易信息进行显示并反馈交易签名
相当于蓝牙型二代USBKEY的安全级别

2 线上小额快捷支付

对移动终端接收到的短信进行加解密处理
防止木马软件截取短信验证码明文

3 应用安全认证

做为身份识别载体提供第三方应用登陆认证或身份认证等功能

4 支持FIDO/TUSI/U盾等各种规范

应用场景：交通出行



快速刷公交地铁

比公交卡更灵敏，无需触屏刷卡
国内领先有源技术，主动发射信号
响应距离长达5cm



在线充值、掌控余额

连接手机APP充值，无需排队
公交、地铁等网点亦可充值

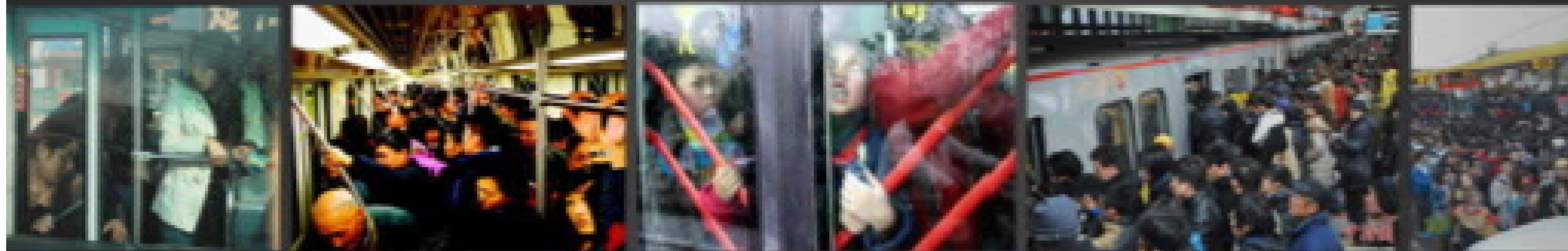
* 在线充值功能开通时间因各地交通运营商差异有所不同

应用场景-线下有卡支付

你有几张银行卡？



找卡+掏卡+刷卡+放卡 = 人均 **1分18秒**



戴在腕上的银行卡



0.3秒极速支付

应用场景：线下条码支付



生成并显示二维码



支付过程与手机终端无关

应用场景：物联网应用

物联网面临的安全问题

黑客谈智能硬件：脆弱到没朋友

李儒超 | 08月27日 18:58

除了无人机，很多智能硬件都比我们想象中要脆弱很多；同时，资金相对紧张的智能硬件初创厂商，在安全上下功夫的并不多。



文/技术白李儒超（微信公众号：techcc）

曾破解过公交卡，如今，杨卿又将目标转到了无人机上。坏消息是，他成功了，被破解后的无人机，可以无视厂商设下的安全限制，轻松在北京六环内起飞。当然，由于没有了限制，你可以在无人机上放上你想放任何东西，飞到你想飞到的任何地方。

好消息是，搞了这个“破坏”的杨卿，是一个“白帽”黑客。

“经过三四个月的尝试，我们发现，不仅仅是汽车，在政策上颇为敏感的无人机，也并非无懈可击”，杨卿说，除了无人机，很多智能硬件都比我们想象中要脆弱很多；同时，资金相对紧张的智能硬件初创厂商，在安全上下功夫的并不多。

杨卿没有对智能硬件全盘否定。他给出的建议是，在购买前，想下智能硬件被黑的后果，比如智能的豆浆机，大不了半夜响起来吓人一跳；但智能的热水器、燃气等，一旦被破解，就可能要了人的命。

也许，并非所有东西都需要变“智能”。

为了安全，总是握奇

搜狐科技 > 智能硬件 > 物联网



智能硬件安全形同虚设 万物互联保障路在何方

搜狐科技 2016-08-24 07:09:19 物联网 智能 企业  阅读(174342)  评论(3)



搜狐科技 文/丁丁

智能保管箱、储物柜、快递柜已经可以在酒店、浴室、学校、公司等公共场所见到。绝大多数人认为把自己的物品放到里面会很安全。但正如有句话所说的，世界上没有打不开的锁。现在不少所谓的智能保管箱，其实存在安全隐患。当有一天你看到一个人站在一排保管箱墙前面，拿着像U盘一样的东西和一部手机折腾几分钟，一整面墙的保管箱就全部打开，这样的场景是何其壮观！

为了讽刺某款保管箱产品强调的智能安全徒有虚名，“黑客叔叔”（姚威）将其改成了一台闹钟。早上一起床时间，保管箱就会响起铃声，并且门就会自动打开。据称，这款智能保管箱已经被一些部门采购，有些物流公司甚至真的将其大量用于户外保管箱或快递柜。

在自动化控制基础上发展起来的物联网行业，如今处于爆发的前夜。近几年来，智能硬件的数量也在飞速增长。IDC的数据显示，仅可穿戴设备，2016年第一季度全球出货量就达1970万台，相比2015年第一季度的1180万台，同比增长67.2%。IDC家居物联网的最新调研结果显示，中国家居物联网在未来5年还将保持高速增长稳定的增长，到2020年，市场规模有望达到194亿美元左右，其中，家庭安防、智能家电、个人健康将成为最主要的使用场景。

美国遭遇史上最严重DDoS攻击，物联网安全引发关注

正文

手机网浏览财经资讯

广告:您有10万元体验金未领取!

来源：中国证券网 作者：佚名 2016-10-26 21:40:23  

中金在线  微博  加关注 微信  加关注  中金部落 关注  在线咨询

美国最大的域名解析(DNS)服务商Dyn 的服务器遭遇大规模分布式拒绝服务攻击(DDoS)Twitter、Tumblr、Netflix、亚马逊、Shopify、Reddit、Airbnb、PayPal 和Yelp 等诸多人气网站无一幸免。

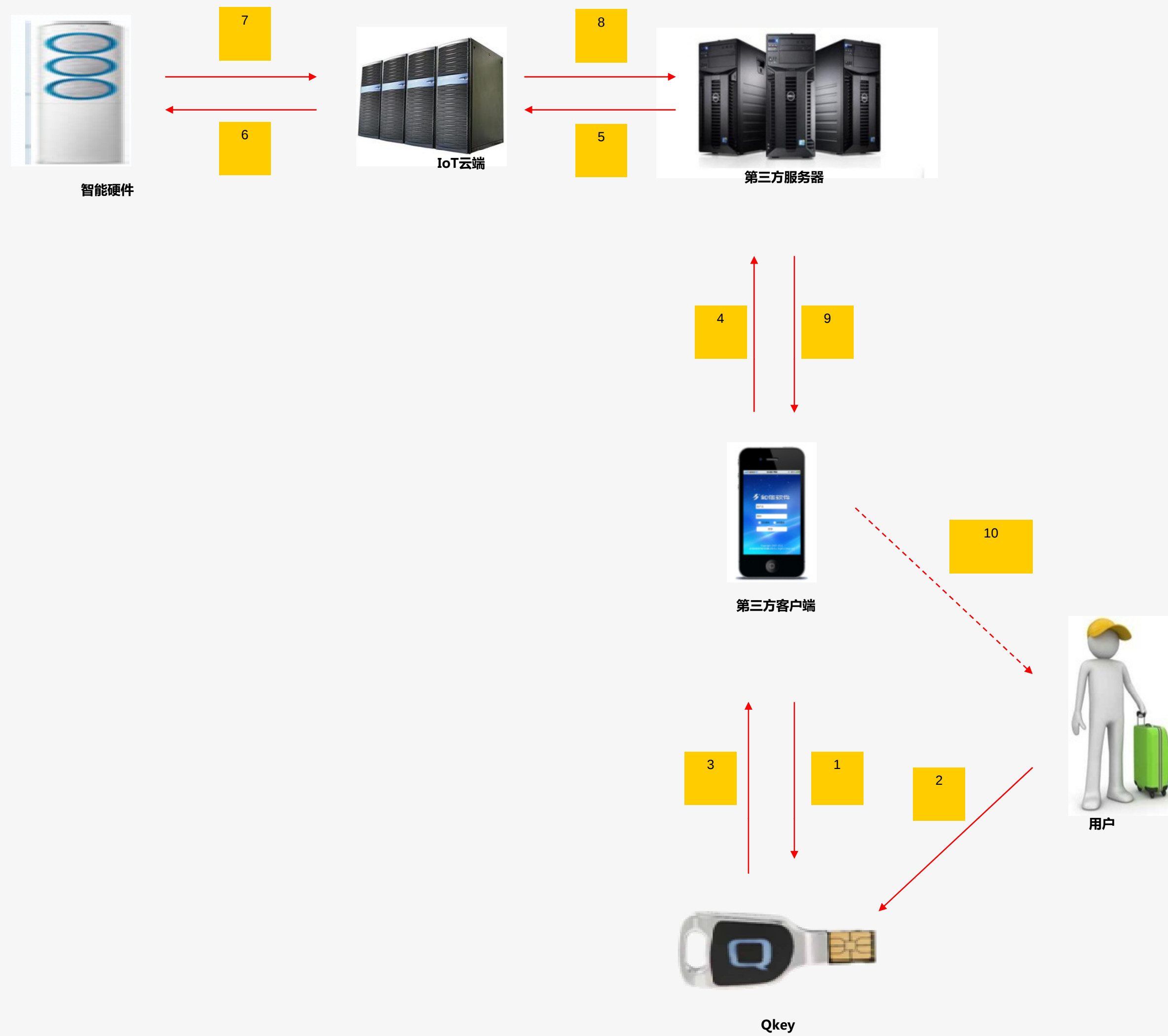
简评

物联网智能设备是元凶

根据相关研究机构分析，一共有超过百万台物联网设备参与了此次 DDoS 攻击。主要包括 DVR 和网络摄像头，这些智能产品由于受到恶意代码的攻击成为僵尸机，进而受到操纵对Dyn 的服务发起大规模DDoS 攻击，导致了DNS 服务的瘫痪。



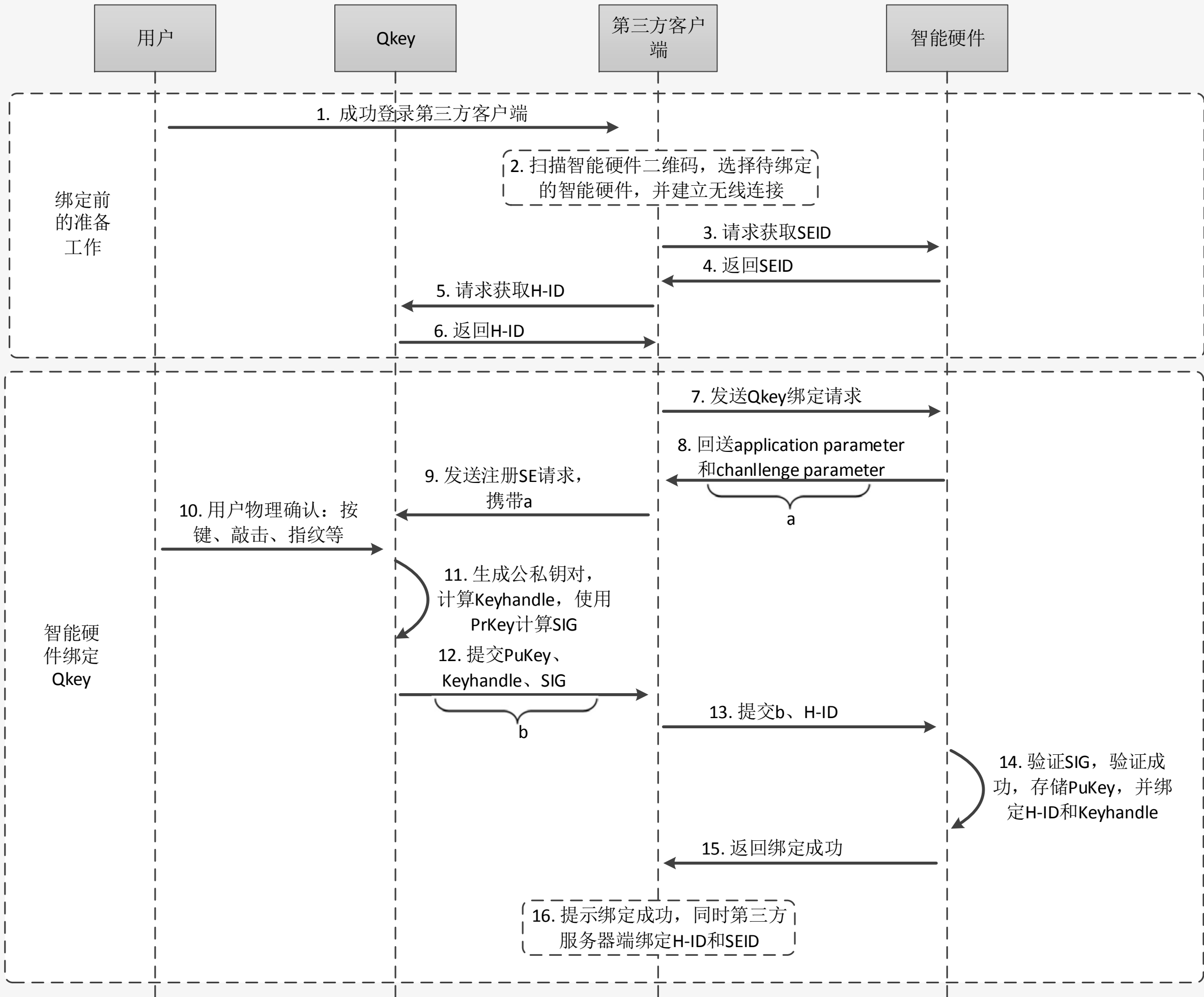
应用场景：物联网应用



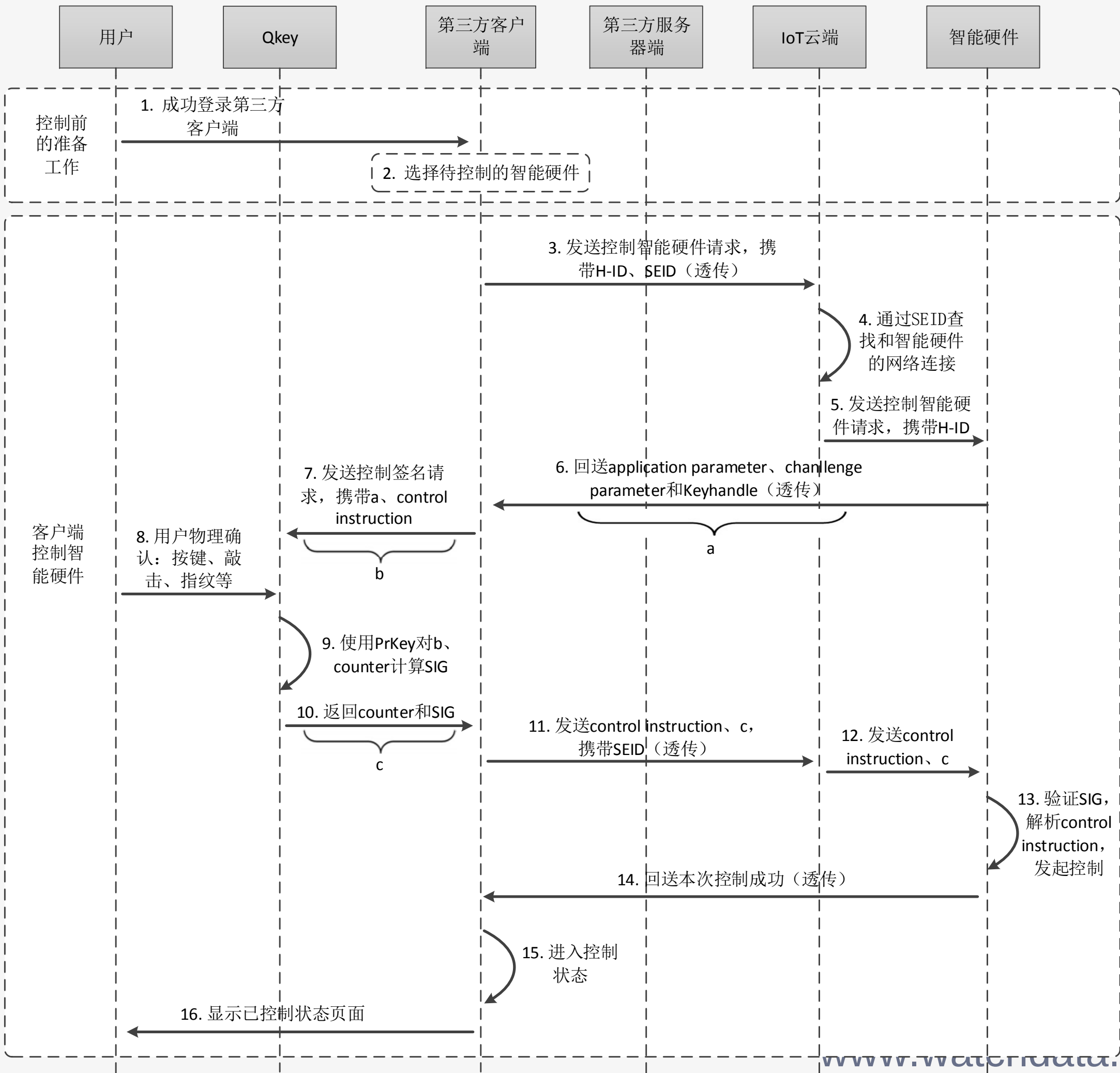
- IoT身份安全流程包括
 - 智能硬件连接家庭网关流程
 - 智能硬件注册IoT云端流程
 - 智能硬件登录IoT云端流程
 - 智能硬件绑定Qkey流程
 - 控制智能硬件流程
 - 智能硬件解绑Qkey流程
- 当智能硬件注册到IoT云端，且绑定了Qkey，用户即可以通过第三方客户端控制智能硬件。

应用场景：物联网应用

智能硬件绑定Qkey流程



客户端控制智能硬件流程

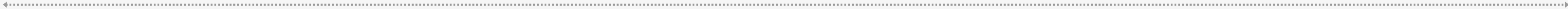


万物互联时代的认证和支付载体



为了安全，总是握奇

应用案例——公交一卡通



北京
一卡通

公交、地铁、超市、加油站

深圳通

深圳

公交、地铁

上海

公交、地铁、超市、加油站

羊城通

公交、地铁、超市



应用案例——金融



广东建行



中国银行&北京一卡通



广东农信



为了安全，总是握奇

应用案例——身份认证/线上支付

FIDO U2F/UAF

TUSI



目 录



1 认证与支付技术发展趋势概述

2 基于智能穿戴设备的认证与支付解决方案

3 握奇实践分享

4 未来展望

未来展望



炫酷外观/ 产品形态

- 外观，材质
- 时尚，品质高
- 环保

- 手表，手环
- 戒指，手链
- 项链



认证支付应用

多应用方向

- 金融
- 交通
- 认证
- 线上线下交易

其它行业应用方向

- 物联网应用
- 校园应用
- 门禁应用
- ID身份识别应用



基础功能

- 更低功耗、更高性能、更多接口
- 更大容量存储
- 更友好的多应用平台
- 屏幕，touch
- 心率监控
- 记步睡眠监控
- GPS定位
- 电话功能

未来展望

握奇将在2016年4季度发布第二代智能穿戴设备

敬请关注.....

中国领先的数据安全解决方案提供商

一直以来不断致力于数字世界的融合与创新，成功服务于电信、金融、交通、政府、企业等领域的行业客户，为数亿用户的身份认证与安全交易保驾护航。

1994年成立于北京，下设握奇数据系统有限公司、握奇智能科技有限公司

2015年销售额达17亿元人民币

超过30亿握奇产品，服务于人们生活每一刻

来自全球10个国家的分支机构，为同一个使命而奋斗

为全球63个国家提供最可信赖的数据安全产品及服务

1200多项专利技术源自握奇的贡献

1000名员工兢兢业业，为客户创造超越期待的价值



结束

Watchdata

谢谢!



关注握奇 了解更多