RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

从无畏到不畏，互联时代如何“锁”住您的安全

陈达

飞天诚信科技股份有限

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012

演讲提纲

- 传统互联网安全新应用
- 移动互联网安全新应用

传统互联网安全新应用

- 2011年底中国网民达到5.13亿
- 2011上半年遭受木马和病毒攻击网民达2.17亿
- 2011上半年帐号或密码被盗网民达1.21亿
- 攻击手段不断翻新，针对特定手段的被动防范难以长期有效，主动的帐户防护成为趋势

传统互联网安全新应用

消费者想要什么？——身份保护居首

身份盗窃保护是消费者第一安全需求

传统互联网安全新应用

为什么大多数网民没有受到有效的安全保护？

- 高安全性产品是否足够易用和方便

  …..从而让用户愿意接纳

- 高安全性产品的综合成本是否足够低

  …..从而产品和技术能够普及应用

传统互联网安全新应用

极度纤薄

厚度小于21毫米，堪比一本杂志

极其快捷

从休眠状态下返回小于7 秒！

(2012)

增强安全性

英特尔® 身份保护技术

极长电力

至少5小时连续使用，数周待机时间

极炫体验

性能一样出色，智能视觉体验

同时具备平板的特性与PC的性能!

传统互联网安全新应用

2011

动态口令(OTP)

保障用户身份认证

IPT™ with OTP

2012

受保护交易内容显示(PTD)

保护交易内容及用户输入，确保OS/第三方应用不能截取或更改内容

IIPT™ with PTD

2012

PKI

公钥基础设施方案

IPT™ with PKI

2013

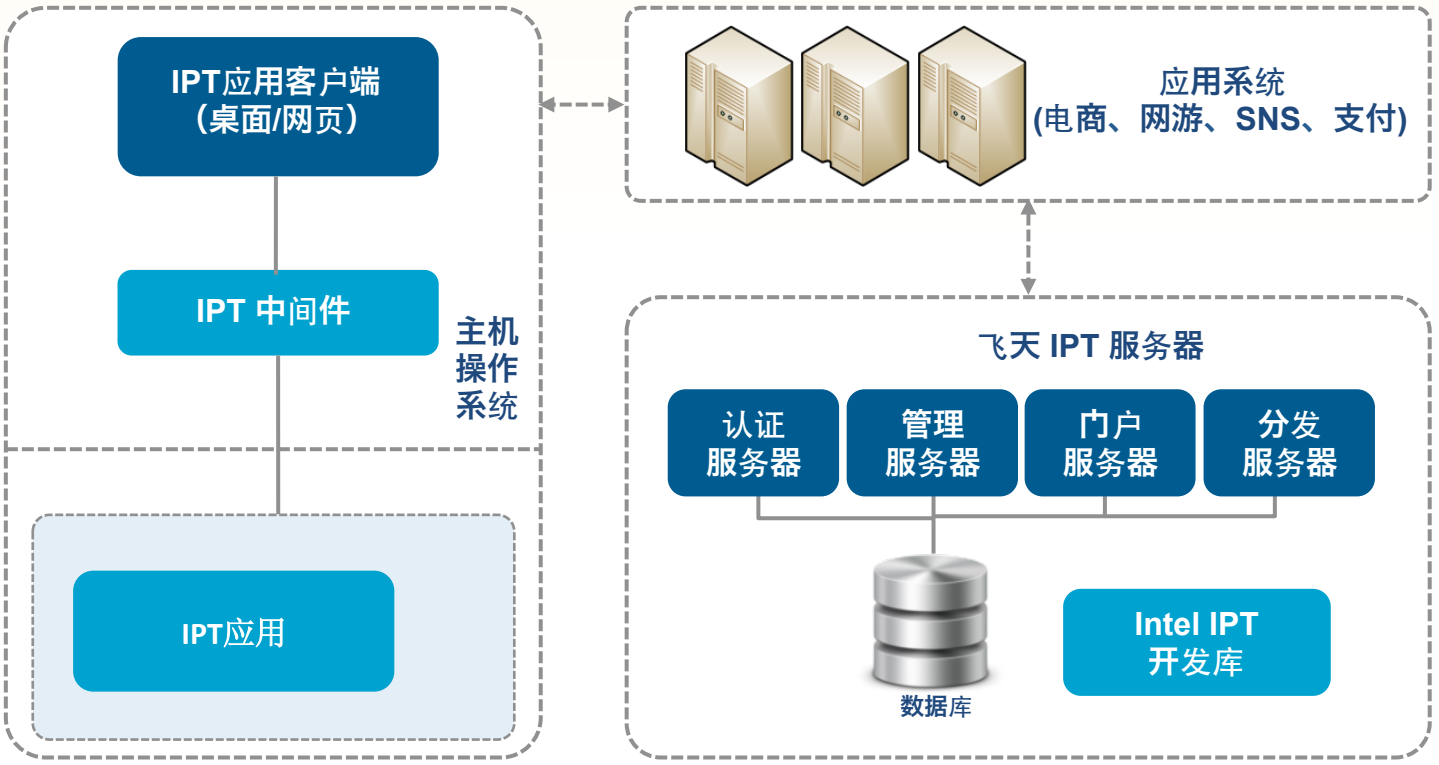
近场通讯（NFC）

安全的电子商务支付

IPT™ with NFC

传统互联网安全新应用

- 飞天诚信基于英特尔® 身份保护技术的解决方案是为互联网应用提供的一个全新的双因素高性价比、强身份认证解决方案。

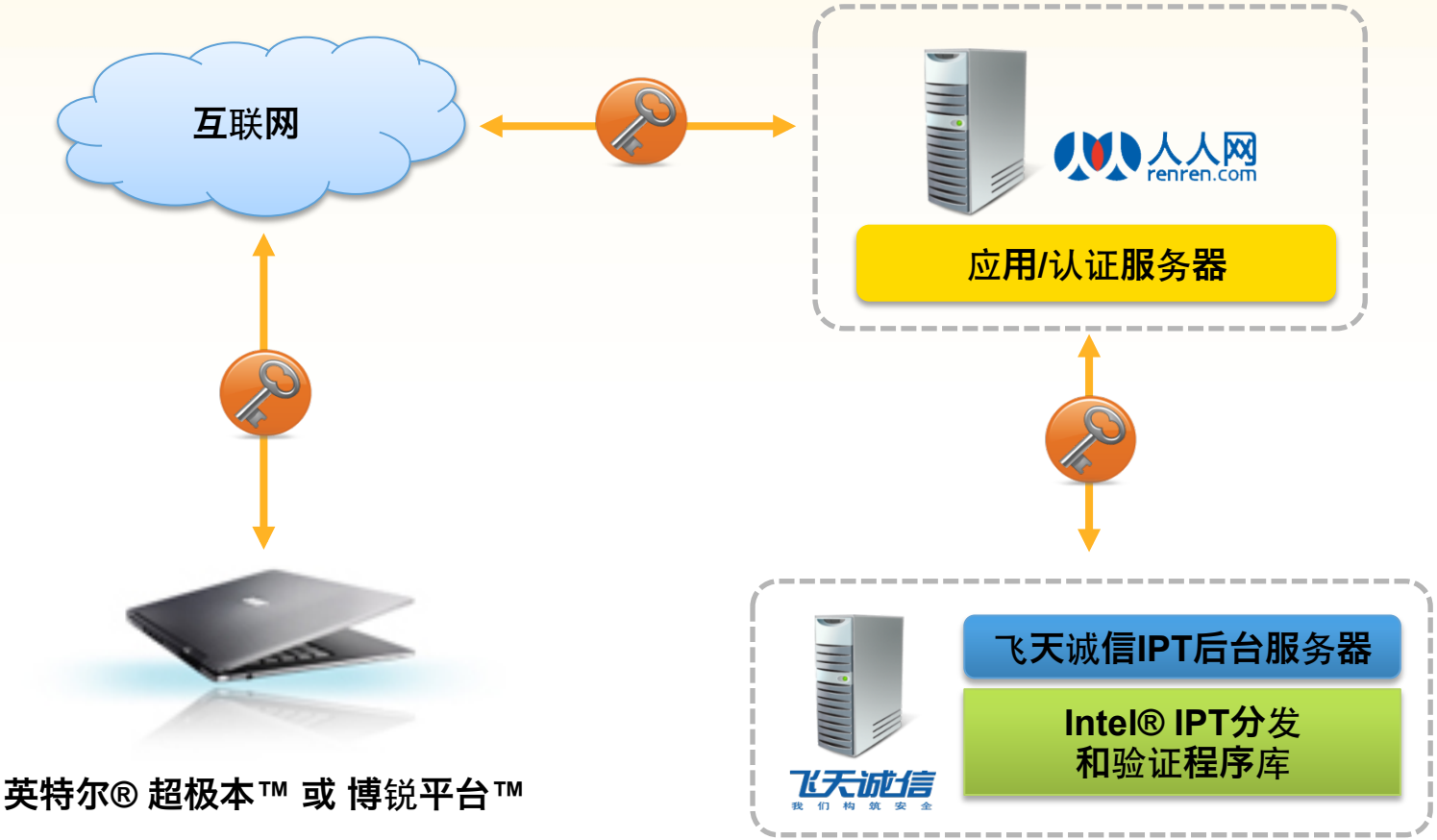


传统互联网安全新应用

飞天诚信IPT解决方案

- 提供全方位、多层次的安全保护
- 为用户使提供安全、方便、快捷的使用体验
- 最佳投入产出比
- 应用于所有互联网系统

传统互联网安全新应用

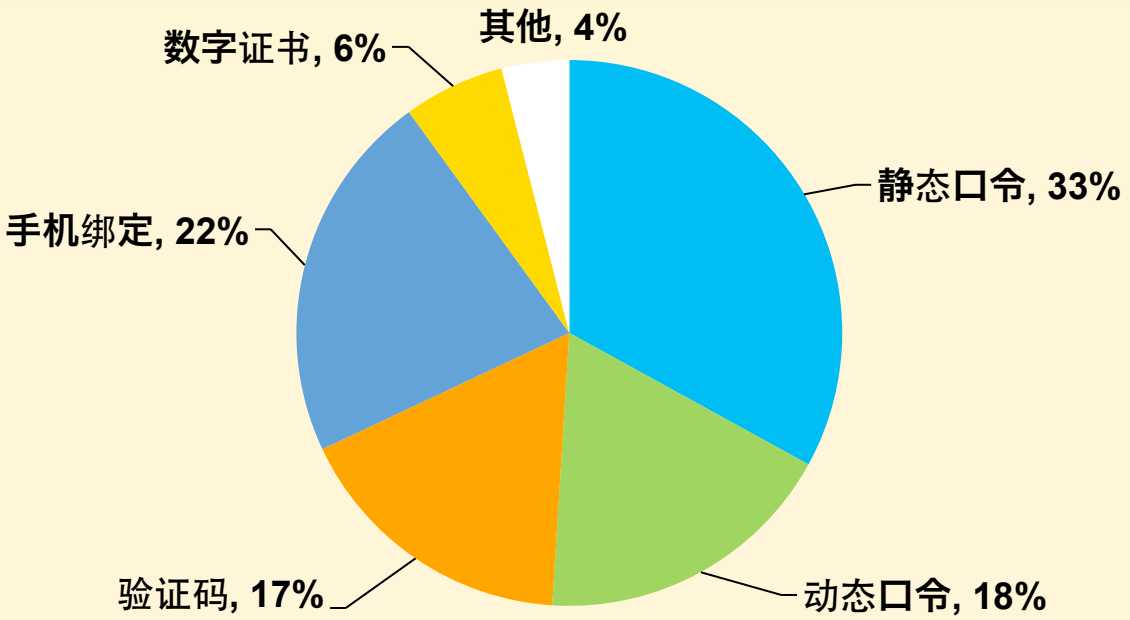

互联网
人人网
renren.com
应用/认证服务器
飞天诚信IPT后台服务器
Intel® IPT分发
和验证程序库
飞天诚信
我们构筑安全
英特尔® 超极本™ 或 博锐平台™

移动互联网安全支付

- 移动支付多以非对公业务为主
- 移动支付多以小额支付为主
- 移动支付关注更多的是“快捷性”

一、国内移动支付安全工具调研

移动支付的安全认证方式



* 数据来源：CFCA

二、移动支付安全交易设备与实现

- 1、移动平台的可用通讯接口：
  - 1）双向接口：适合基于PKI体系的Key产品
    - SIM卡：手机内置Key
    - SD卡：手机内置Key
    - 耳机接口：外置Key
    - 专用接口：苹果的iDock、HTC的USB等，外置Key
    - 蓝牙等：外置Key
    - Wifi：外置Key
  - 2）单向接口，适合光感令牌产品
    - 光感扫描屏幕
  - 3）人工操作，适合普通令牌产品

二、移动支付安全交易设备与实现

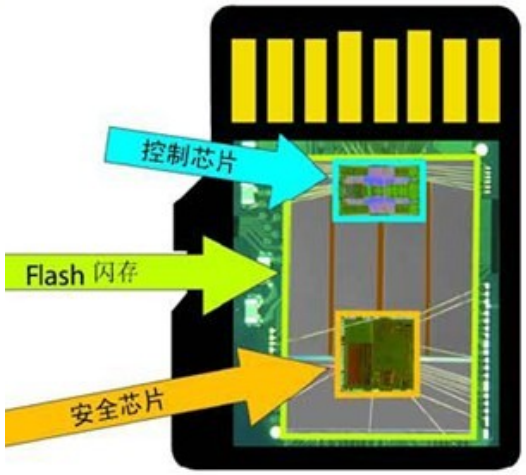
- 2、双向通讯的PKI：
  - 1）SWP体系

    * 将“卡”和“Key”的概念统一、将“Key”移入移动平台

    * 三种模式

      - SWP-SIM卡：中国联通
      - SWP-SD卡：中国银联、欧贝特
      - SWP-手机：诺基亚、 Gemalto（芯片）

二、移动支付安全交易设备与实现



二、移动支付安全交易设备与实现

- 2、双向通讯的PKI：
  - 1）通用耳机接口

    * 代表厂商： Square， 飞天诚信

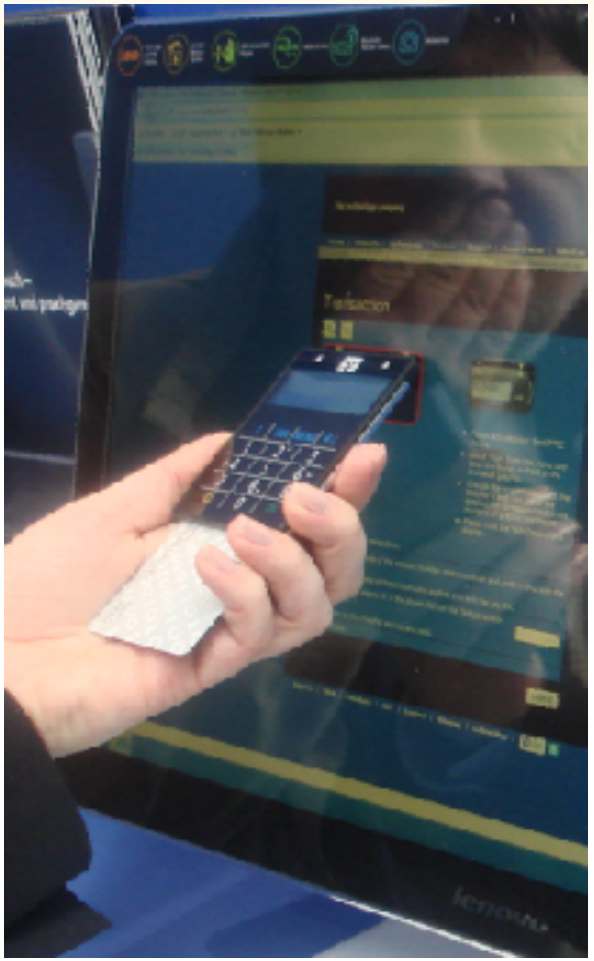
- 适合智能手机

二、移动支付安全交易设备与实现

- 2、双向通讯的PKI:
  - 2）通用蓝牙接口：适合所有智能手机
  - 3）专用苹果接口：适合所有苹果产品， 如iPad、iPhone、iTouch

二、移动支付安全交易设备与实现

- 3、单向通讯的令牌体系：
  - 光传输：可以实现挑战应答、交易签名功能



二、移动支付安全交易设备与实现

- 4、人工操作的令牌体系：
  - 1）基于时间、时间令牌
  - 2）挑战应答

二、移动支付安全交易设备与实现

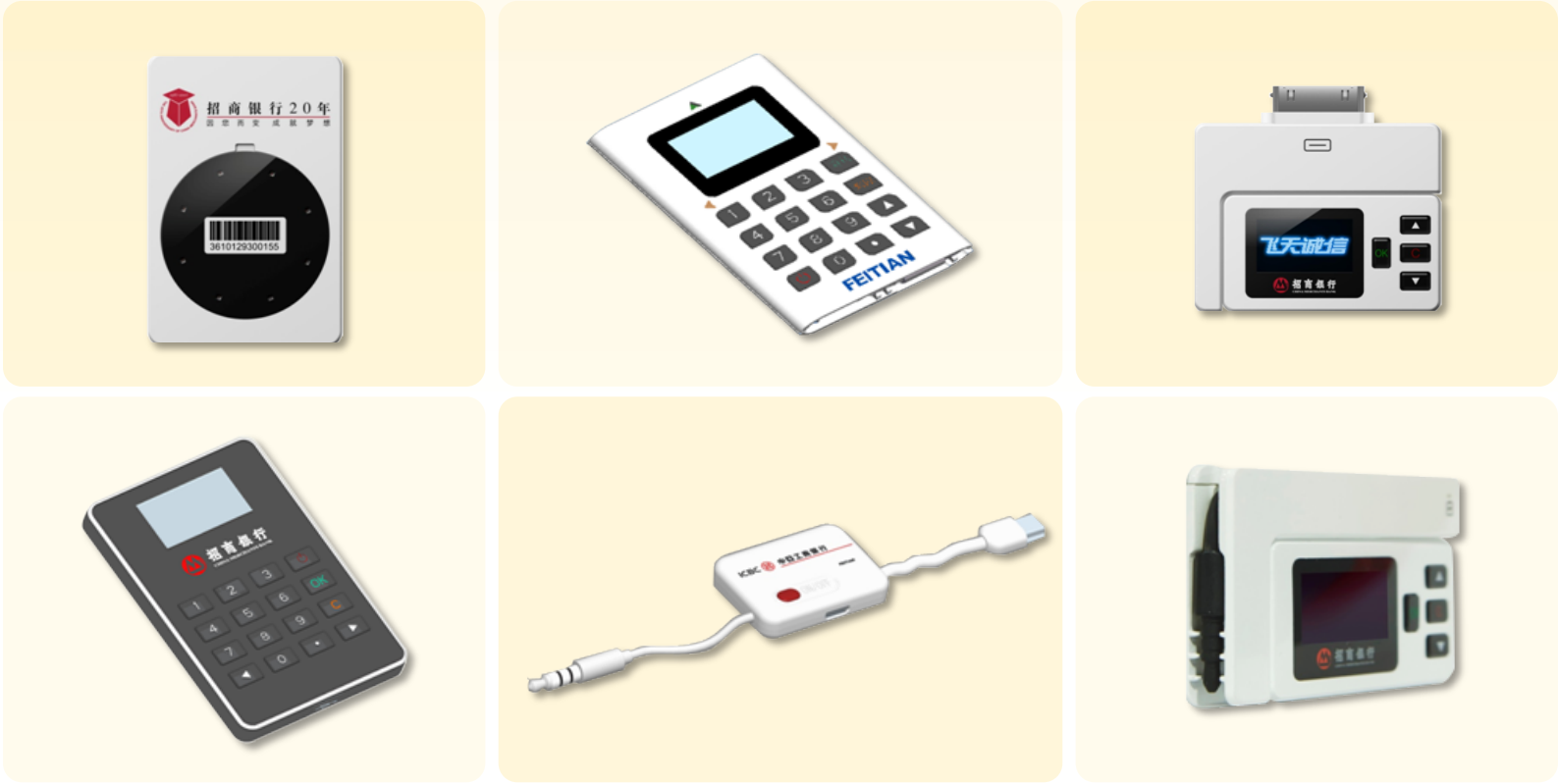
symbian iOS BlackBerry

Android Java

越好的认证方案支持越多的移动平台

——Anywhere

二、移动支付安全交易设备与实现



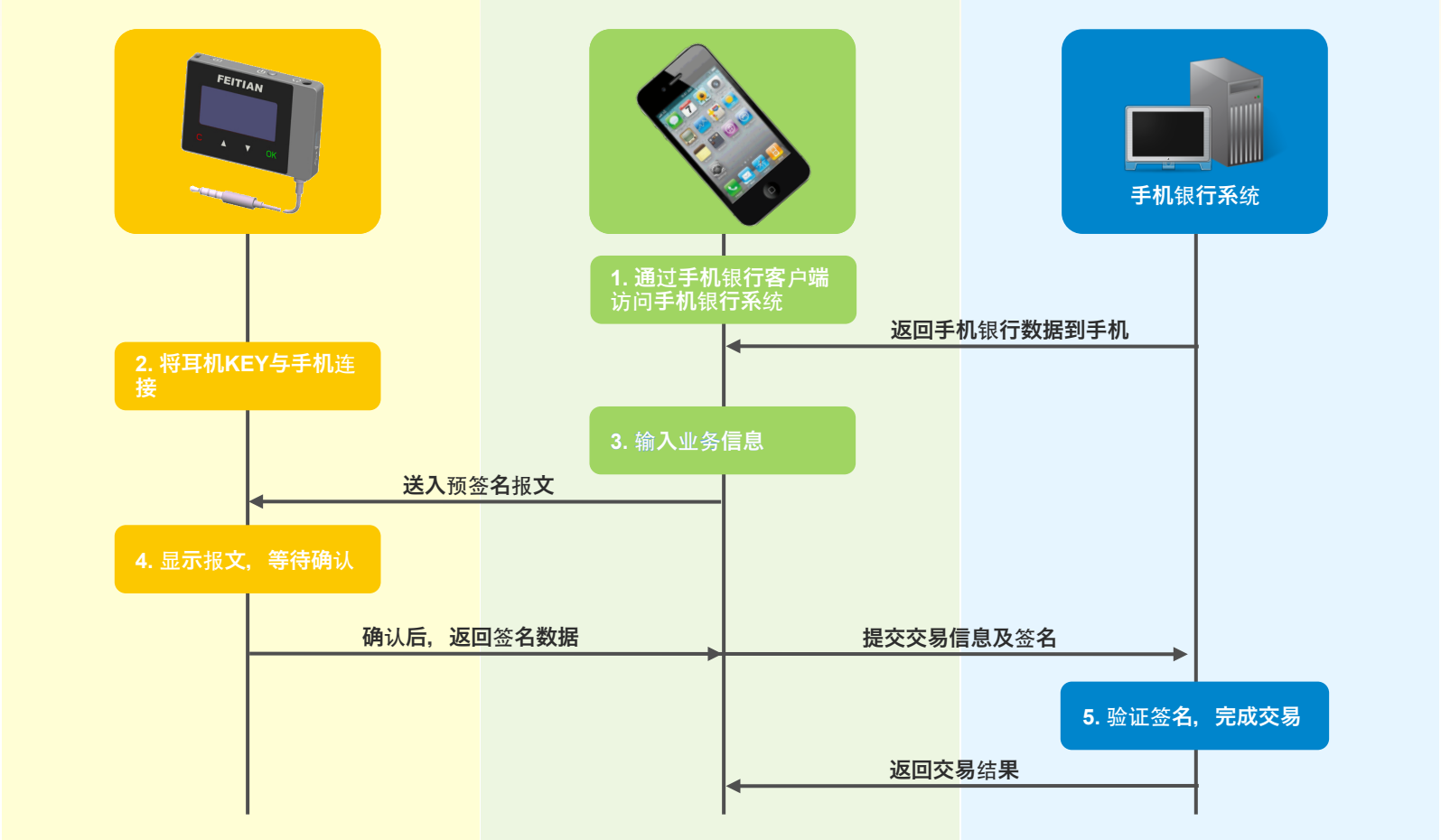
和桌面平台兼容　　——Anytime

二、移动支付安全交易设备与实现

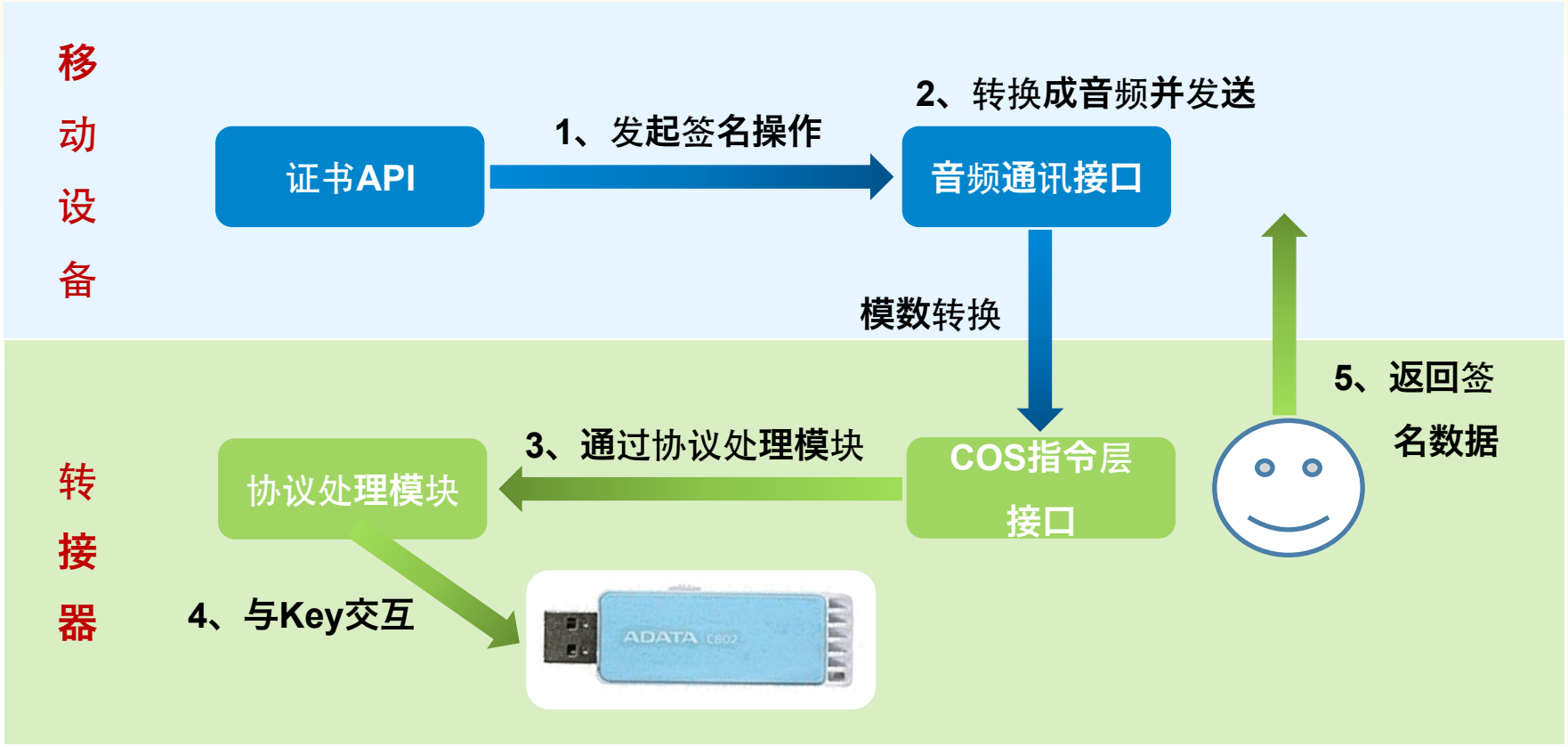
摘自-“中国移动支付网”

三、移动支付的安全交易流程

业务流程



三、移动支付的安全交易流程



技术原理

三、移动支付的安全交易流程

耳机设备要解决的潜在风险

四、移动支付安全交易的观点

- 1、保障
  - 在认为网络通道不安全的基础上，通过个人终端设备的合理利用，移动平台的交易可以是安全的。
- 2、现状
  - 个人终端认证设备的种类完备，已经为移动平台的交易安全做好了准备。

四、移动支付安全交易的观点

- 3、发展
  - 便携：既然为移动平台所利用，设备的便携是保证。小型化、功耗低的产品是其发展方向。
- 4、多应用结合与组合
  - 1）与个人银行卡片结合的技术，CAP体系、银联动态密码体系。
  - 2）动态口令智能密码钥匙。



谢谢

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012