

# 中国网络安全大会

## 2015. 07.01

### 新移动时代信用云平台和信息云平台的分合

谢涛令 博士，中组部国家千人

董事长，苏州海博智能系统有限公司  
首席科学家，中城建物业集团总公司

[www.hierstar.com](http://www.hierstar.com)

# 什么是工业4.0? 多少版本?

- ❖ 工业1.0, 2.0, 3.0, 4.0 工业4.0已经开始了几年!
- ❖ 金融仍然是核心, 而金融的核心是货币载体:
  - 工业4.0开打: 个性化定制生产的大趋势把互联网金融推到了新经济新常态创新的核心战略位置, 各巨头势在必得
  - 移动支付手段和技术是互联网金融的核心
  - 支付的各方都把安全看作是最迫切需要解决的问题
  - O2O打通是困扰众多产业拥抱网络技术的最大障碍
  - 网络安全、信息安全和金融支付安全已经是国家首脑亲自管理布局的核心国家利益问题

# 信息载体的发展与与时俱进

1844

1876

1946

1964

1974

2000

电 报

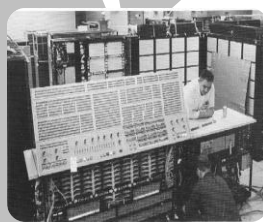
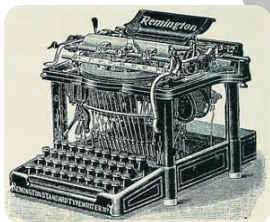
电 话

ENIAC计算机

集成电路  
主机系统

个人电脑

智能移动终端



# 信任载体是最顶尖技术的完美展现

BC200

BC100

1985

2003

2005

2013

汉朝虎符  
印章

身份文书

第一代身份证  
磁条卡

网银  
防伪印刷护照

二代身份证  
金融IC卡

可视金融IC卡  
可视身份证



# 互联网广播特性：绝大痛点

## ❖ 互联网的本质是互联的广播

- 查号台概念
- 电话系统
- 互联网根服务器
- 美国控制

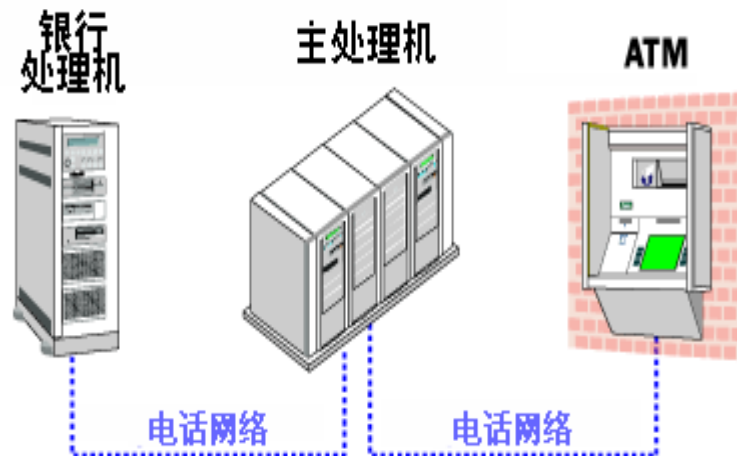
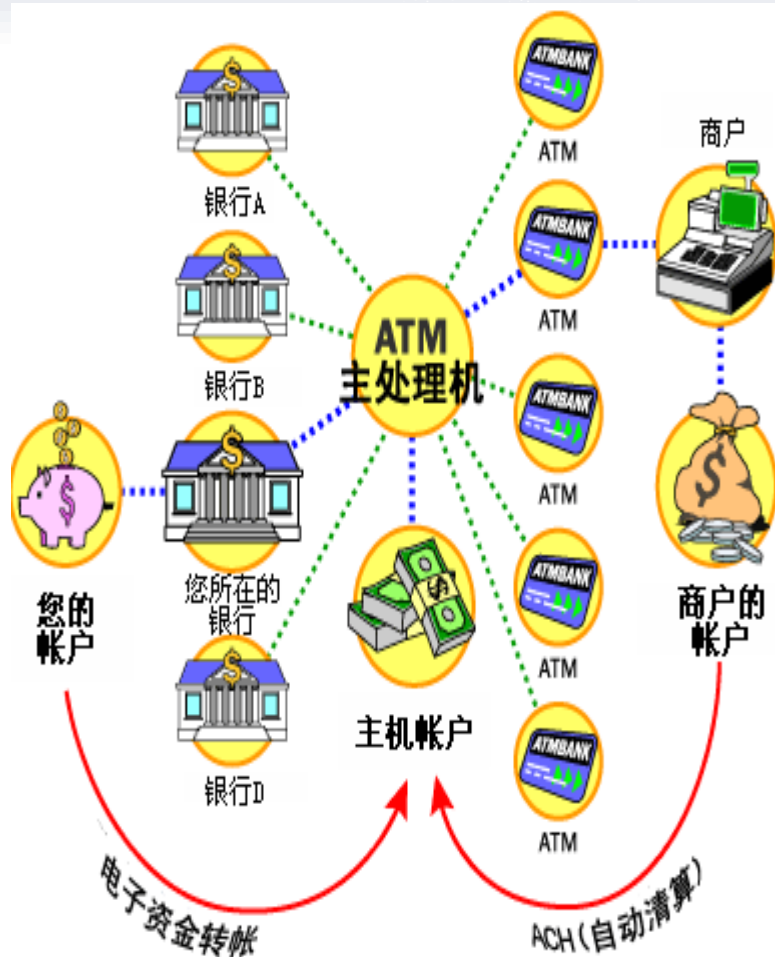
## ❖ 类似电报系统！

## ❖ 微信，淘宝，无加密通道！

## ❖ 裸奔兮，风险自担！

# 银行金融1.0——ATM, POS, 银行分支

## 加密专网 延伸到用户附近



银行通过专网专线将后台数据连接到ATM终端，最大程度保障用户操作安全。



# 网络银行2.0

加密通道 延伸到 PC

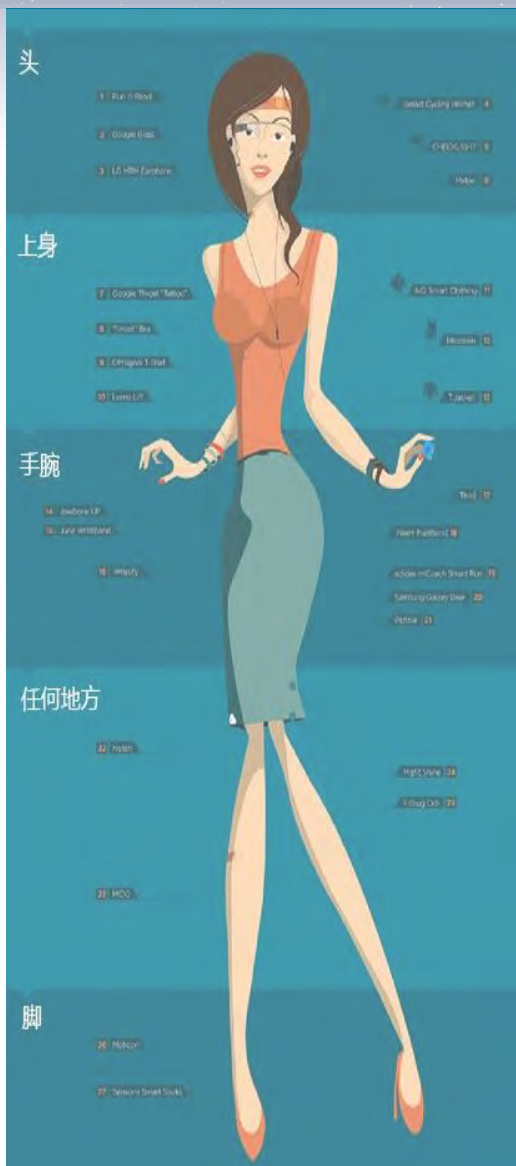
用户的PC端，将用户数据纳入了互联网，数据环境更加开放，安全风险也更大：

- 数据传输系统可能被攻破，威胁用户资金安全。
- 计算机病毒可越过网络防护入侵用户账户造成严重损失。



# 网络银行3.0 – 移动

金融  
加密通道 延伸到 身体





# 央行一锤定音 – 移动支付必须绑定硬件载体

## 短信验证码作废

《指导意见》还对移动金融服务的交易可靠性提出了要求：采取手机等移动终端直接与后台系统远程交互的方式提供移动金融服务时，各商业银行和银行卡清算机构应使用可靠的多因素身份认证方式，并采用手机安全单元（SE）、智能密码钥匙（Key）等基于安全芯片的电子设备作为必要的认证因素、以确保资金类、重要信息变更类、重要业务变更类等高风险交易的安全。

“过去PC端的网上银行要求使用U盾，手机银行其实也是网上银行。这次的要求就是要提升手机银行的安全保障能力，” 监管层专家称，“过去病毒、木马主要针对PC端，以后移动端用户多了，可能会存在风险隐患。”

按照《指导意见》要求，手机需具备SE或Key等基于安全芯片的电子设备。目前方案分两类，包括Key（类似网银U盾），或手机内置SE安全芯片。

监管层专家表示，目前包括三星、华为等部分支持非接触支付的智能手机已内嵌了SE元件，电信运营商也在部分SIM卡里增加了SE元件；如果不具有SE，也可以通过网银Key的形式。Key类似PC端网上银行的U盾，但由于手机没有USB接口，因此可以通过蓝牙等方

2015年1月13日人民银行颁发的《关于推动移动金融技术创新健康发展的指导意见》充分强调了移动支付**必须**绑定硬件安全载体。

央行政策否定了纯软件作为支付载体的实现方式，进一步巩固了海博的信心，是对海博过去10年辛勤投入的重要肯定！



# 人民币国际化对于货币载体的需求明确

## 中国将启动自己的SWIFT – CIPS

财经 19:15 2015年03月11日 (更新 17:35 2015年03月12日)

1025 8 0

中国在提升人民币国际地位上又向前迈了一大步。今年9-10月有望启动类似SWIFT的中国国际支付系统(CIPS)。它将大大简化人民币跨境结算流程,让人民币更加接近储备货币的身份。

目前人民币的国际跨境结算主要通过香港、新加坡和伦敦银行的参与来实现。这些金融中心占人民币全部结算量的95%。启动CIPS后,将在统一的国家平台进行人民币结算,摆脱中间链,使境外公司直接同中国的分支机构打交道。结果,金融通信速度将加快,结算成本将降低。实际上这将使人民币上升到世界主要货币的水平,并将从美元那里夺到国际结算业务市场的相当一部分份额。

发展中国家早就选择了逐渐放弃利用美元结算的策略。因为目前全球绝大多数银行使用的SWIFT(环球同业银行金融电讯协会),就像国际信用评级体系一样,威信日渐丧失。虽然SWIFT的总部位于布鲁塞尔,但是它却受美国控制。在世界媒体报道制裁俄罗斯时,越来越经常提到该体系。一些欧洲领导人不久前宣称,禁止俄罗斯使用SWIFT。现在西方政客的语气有所缓和,称这只有在非常情况下才有可能。



© SPUTNIK ALEXANDER YURIEV

中国人民币跨境支付系统(CIPS)可能在2015年下半年启动

0314/1014092480.html

美国SWIFT跟海博的合作探讨,必将被中国自己同类系统跟海博合作探讨所取代。

在人民币国际化大背景下需要有一个强大、安全且便捷的货币载体方式帮助人民币交易与消费走出国门,实现在全球的快速安全支付。目前只有海博技术满足这一需求。



# 安全三要素：认证，加密，电子签名

## ❖ 认证

- 身份确定
- 授权
- 个性化

## ❖ 加密

- 保密
- 防止信息泄露
- 隐私保护

## ❖ 电子签名

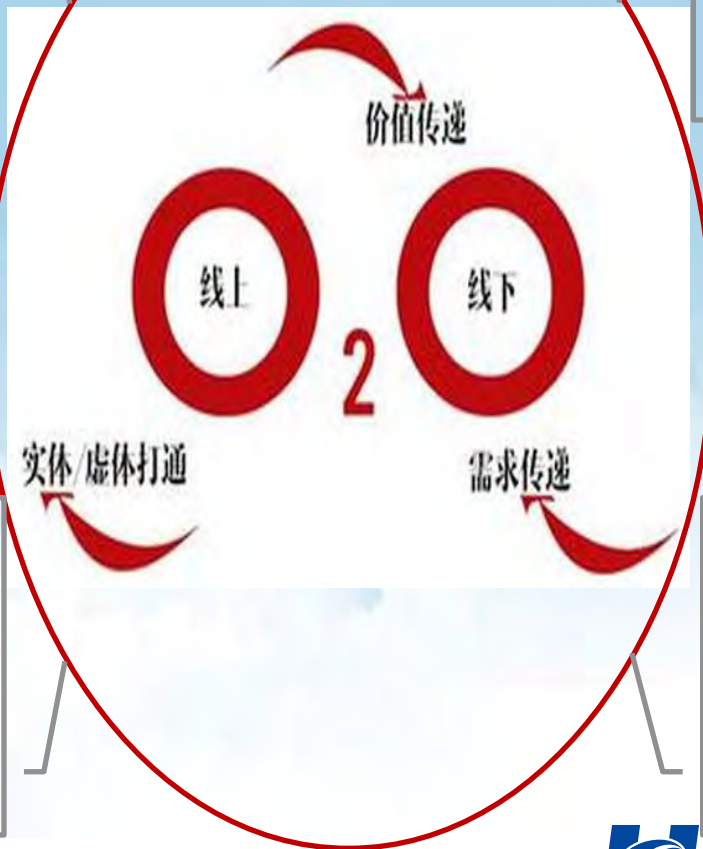
- 防止抵赖
- 信任的基础
- 法律的基础



通道&云端  
数据加密



线上线下身  
份  
唯一且真实



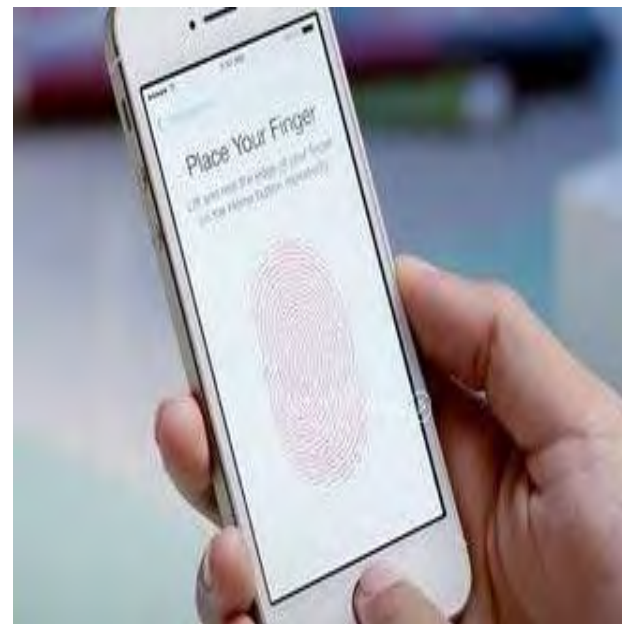
安全&便捷  
随时支付



对所作所为  
担负责任



# 生物识别无法解决远程认证等诸多问题



## 不能解决远程认证

不能通过网络传输

只能解决人和机器、人和卡片的本地认证

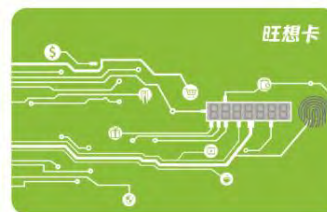
不符合电子签名法要求

不能解决通道加密

# 手机外硬体是金融行业的硬需求；国外开始觉醒

❖ 安全三要素：认证防假冒，加密防泄露，电子签名防抵赖

- 手机和其他移动软体受制于病毒和木马等恶意软件
- 需要硬件作为密钥载体



最近国外趋势明确，  
都是海博可视卡为基础的公

- Coin
- Swyp
- Plastic Card
- Dynamic
- Final





# O2O货币安全载体设计和工艺

技术和工艺掌握极其困难和耗时；**2006**年开始研发至今；  
**100**多项专利，**2015**年底**200**项，**75%**发明专利



柔性显示

集成

压扁



集成



薄卡中料 (3x6)



成品卡

内嵌模组



超薄柔性电池

# 最可能的新货币主要载体：O2O可视IC卡

- 集成了身份证卡，银行卡，磁条卡，动态密码OTP令牌，PKI Key（U盾）等功能，一卡打通多维通道
- 线下能力：线下身份认证、POS消费、ATM取款
- 线上能力：PKI Key(U盾)或者OTP
- 功能：线上身份认证和支付，即线上认证防假冒，加密防泄漏、电子签名防抵赖
- 支持NFC 近场支付保护，与移动终端互动
- 支持蓝牙BLE中距离支付保护，与移动终端互动
- 支持完整远程人证绑定功能，这是互联网金融关键**





虚拟卡



标准IC卡



可视IC卡

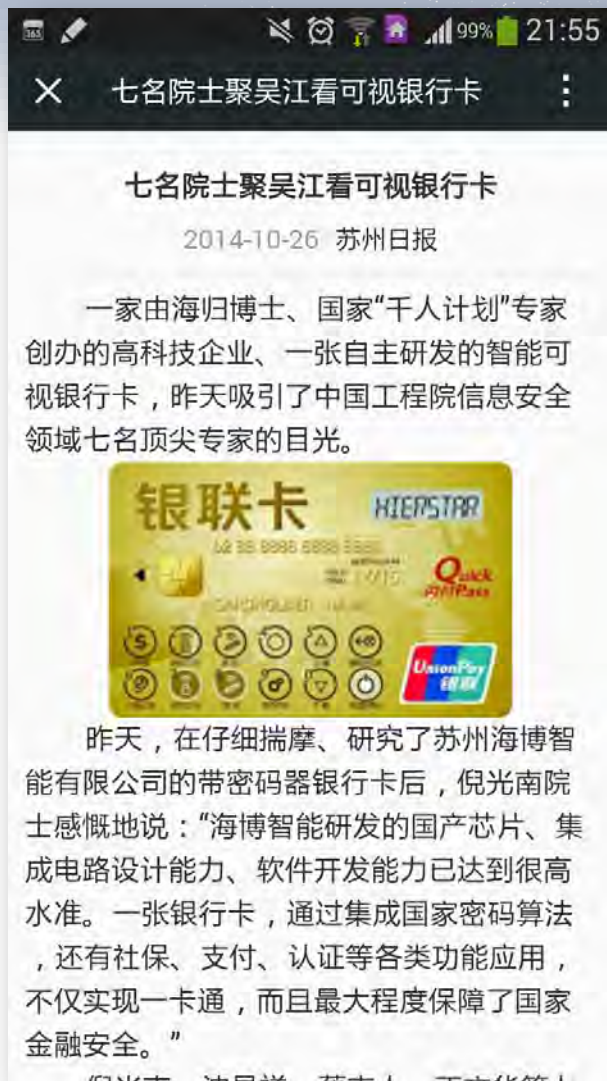


智能穿戴

以人为中心  
高度耦合的  
安全介质  
不同类型



# 技术风险和市场风险极小



海博可视金融IC卡已经等到了倪光南等院士的论证和赞扬。

同时海博的产品在建行、交行等国有商业银行发行，能够得到向来保守的商业银行特别是国有五大行的认可，说明海博的产品已充分获得了市场的认可。



# 用户与信息载体、云端之间的点对点绑定凭证





# 服务云平台的应用市场

金融

Hierstar +



企业

Hierstar +



其他行业市场



更多应用市场待开发……

## 应用场景—认证，电子签名、加密

Before



一份文件多人手签，甚至跨国专递，兴师动众

Now



全部流程线上完成，PKI电子签名极速、安全、简便



PKI对文件加密

"妈妈再也不用担心我的\*\*门"

# 部分其他成功案例卡面集锦 – 身份金融和应用

## ● 中国银联



## ● VISA / MasterCard



## ● 智慧城市 & 智慧社区



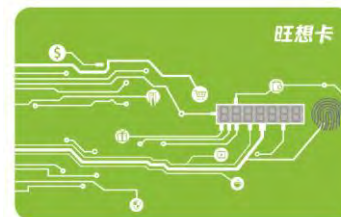
## ● 交通卡



## ● 企业一卡通卡



## ● 移动支付



**感谢各位**  
**祝身体健康万事如意**

