



国家金融IC卡安全检测中心
National Financial IC Card Security Test Center

银行卡检测中心
Bank Card Test Center



生物识别： 打开潘多拉魔盒的钥匙？

银行卡检测中心 杨波

Friday, October 26, 2018

目录

CONTENTS

1

生物识别技术的应用

2

打开潘多拉魔盒

3

标准与检测

第一部分

生物识别技术的应用

技术背景与应用情况

1.1 | 名词解析

生物特征



生物特征包含生理特征和行为特征。
生理特征如人脸、指纹、虹膜、指静脉等；**行为特征**如步态、声音、笔迹。

生物特征检测



生物特征检测指从复杂环境中定位、标识生物特征。

生物认证



生物认证指利用检测到的生理或行为特征进行身份鉴定。

1.2 生物认证应用概览

生物特征



具体应用



刷脸取款



刷脸吃饭



指纹刑侦



指纹支付



说话人辨识



应用解锁



身份鉴权



安防刑侦



指静脉开锁



刷脸转账



刷脸买保险



考勤、门禁

1.3 生物认证应用于金融支付



支付方式演变过程

1.4 生物识别分类

生物识别

行为特征

生物特征

击键

情感

心跳

手部

声纹

DNA

头

坐姿

指静脉

人脸

人耳

眼部

步态

掌静脉

2D人脸

巩膜

签名

指纹

3D人脸

虹膜

眨眼

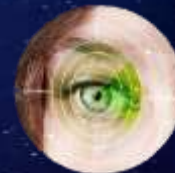
掌形

红外人脸

视网膜

摇头

掌纹



1.5 | 生物识别技术—元素与组件

生物特征样本

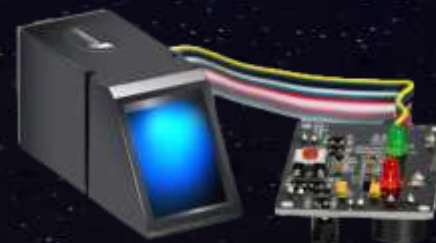
生物特征项

生物特征探针

生物特征模板

生物特征参考

生物特征认证器



1.7 | 采用指纹识别技术的EMV卡

※ 首发

- 金雅拓在2018年1月于塞浦路斯银行发布全球首款接触式与非接触式的EMV生物识别双界面支付卡

※ 产品特点

- 只需轻触，无需在POS终端上输入PIN码即可进行付款交易
- 非接支付交易不再受额度限制
- 生物识别技术验证仅在卡体执行
- POS机无需升级
- 无需充电
- 交易次数不受限制



1.8 | 人脸识别技术

※ 识别形式

- 3D结构光人脸识别
- 2D人脸识别+活体检测（红外、动作、唇语）
- 2D人脸识别

※ 当前移动终端产品

- 3D：Apple iPhone X Face ID、OPPO Find X FaceKey 3D、华为 nova 3
- 2D：其他使用人脸识别的Android设备和应用

※ 金融产品及配套方案

- 柜台人证合一身份认证系统
- 远程开户
- VIP识别与精准营销
- 刷脸支付



1.9 | 生物识别技术—应用案例



人脸识别超级柜台



ATM刷脸取款



人脸识别智能柜台

1.10 | 生物识别技术—农行重庆分行：无感支付



入口处系统检测客户人脸



刷脸支付结账

1.11 | 2018中国国际金融展代表性成果



农行科技银行



云从人脸识别服务



工行刷脸支付



民生银行智能机器人

第二部分

打开潘多拉魔盒

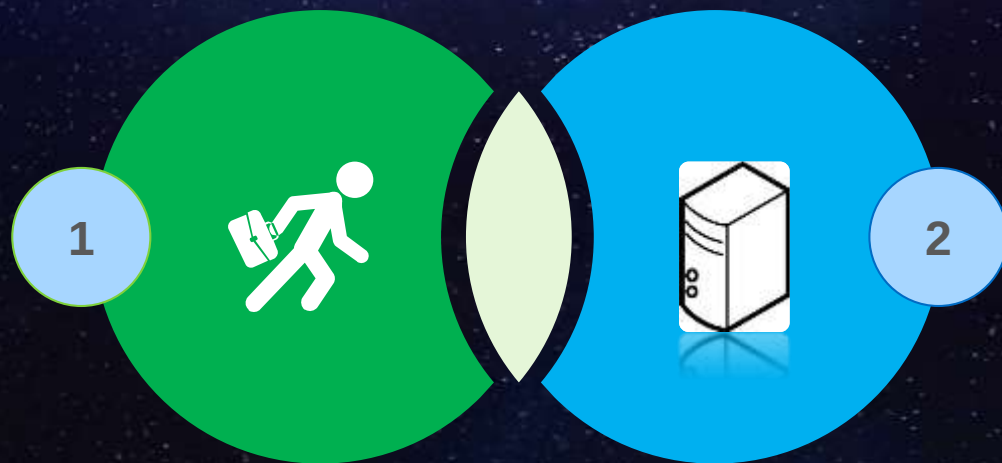
生物识别技术的安全问题

2.1 | 生物认证应用面临的问题

后端安全性弱

认证能力差异大

不同机构技术水平不同，生物认证能力差异大，而且生物特征信息无法修改，使用户隐私面临较大被泄露风险。



存储及维护差异大

机构各自存储生物特征，不仅需较高存储技术还需对生物特征后期维护。差异较大的存储及维护能力使生物特征面临安全风险。

2.2 生物识别技术的安全问题

※ 设备、算法与样本的可靠程度

- 指纹识别模块的种类与灵敏度、摄像头像素
- 机器学习方法与数据库



※ 风险分析

- 不具备活体检测功能或3D人脸检测功能——可实施**呈现攻击**
- 使用伪装、复制或修改的生物特征信息并呈现给生物特征识别系统以达到欺骗生物特征识别系统的目的
- 使用市面上售卖的工具即可有效复制出能够通过认证的指纹套
- 身份认证整体方案的安全性问题（生物特征数据的采集、传输、处理、存储、更新）



高仿真硅胶面具

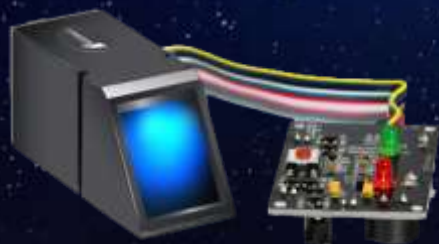


半导体指纹模



光学指纹模

指纹学习机制的陷阱



攻击原理

- 1、目前市场上的指纹模组为了提升用户的使用体验，提高指纹的识别率，使用过程中加入了指纹学习机制，指纹模组会记录指纹在使用过程中的变化点
- 2、通过指纹学习机制把假指纹学习到内部指纹数据库中达到开锁的目的。



2.3 移动支付的安全问题

※ 手机终端涉及厂商和型号众多

- 安全设计各家都有不同，重视程度不同
- 安全问题的重灾区

※ 风险分析

- 当前移动支付（扫码、非接、手机银行）交易量激增
- 便利优先，安全防护与标准规范滞后



终端软件层

APP

通信协议

OS/COS

TEE OS

生物识别算法

Firmware

终端硬件层

CPU/AP

通信模块

存储模块

传感器模块

生物识别模块

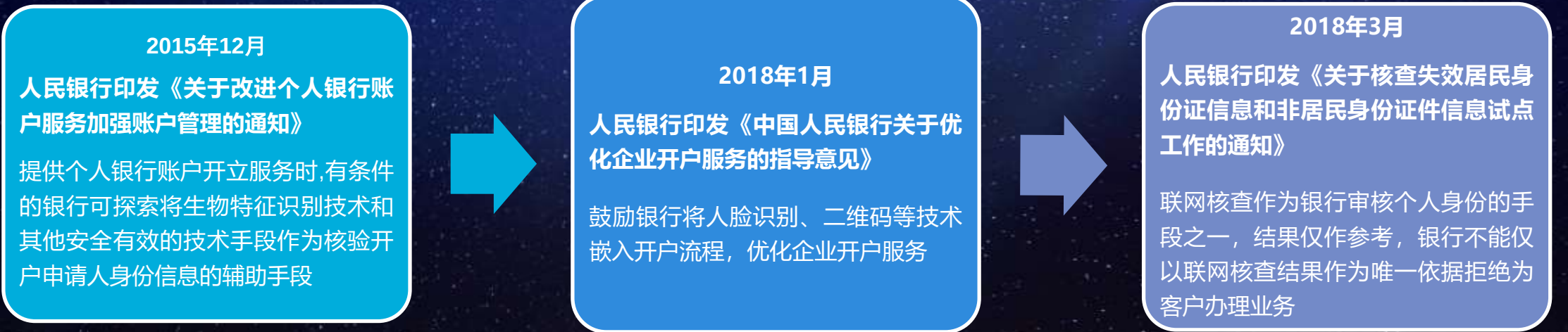
安全芯片

第三部分

标准与检测

相关标准要求及安全防护技术

3.1 | 生物认证相关标准及政策



序号	标准/规范名称	归口部门
1	《中国银联生物认证技术指引》	中国银联
2	《GB/T 35735-2017公共安全指纹识别应用采集设备通用技术要求》	全国安防标委会
3	《GB/T 35736-2017 公共安全指纹识别应用图像技术要求》	全国安防标委会
4	《GB/T 35742-2017 公共安全指静脉识别应用图像技术要求》	全国安防标委会
5	《GB/T 35678-2017 公共安全人脸识别应用图像技术要求》	全国安防标委会
6	《GB/T 27912-2011 金融服务 生物特征识别 安全框架》 (ISO 19092-1:2006 翻译修改)	金标委
7	《GB/T26237 信息技术 生物特征识别数据交换格式》	信标委

3.3 | SE (安全单元)

※ 起源

- IC卡 (CPU卡) 芯片

※ 已广泛用于传统支付终端

- 目前UPTS和PCI PTS要求智能POS必须具备SE (SP/安全芯片)

※ 智能手机开始推广应用SE

- eSE (苹果)
- inSE (华为)
- SIM等其他形式的SE

※ 芯片安全

- 基于完全物理隔离的安全区域
- 处理和存储安全敏感信息，密码学运算，具备一定tamper-proof功能



3.4 TEE (可信执行环境)

※ 起源

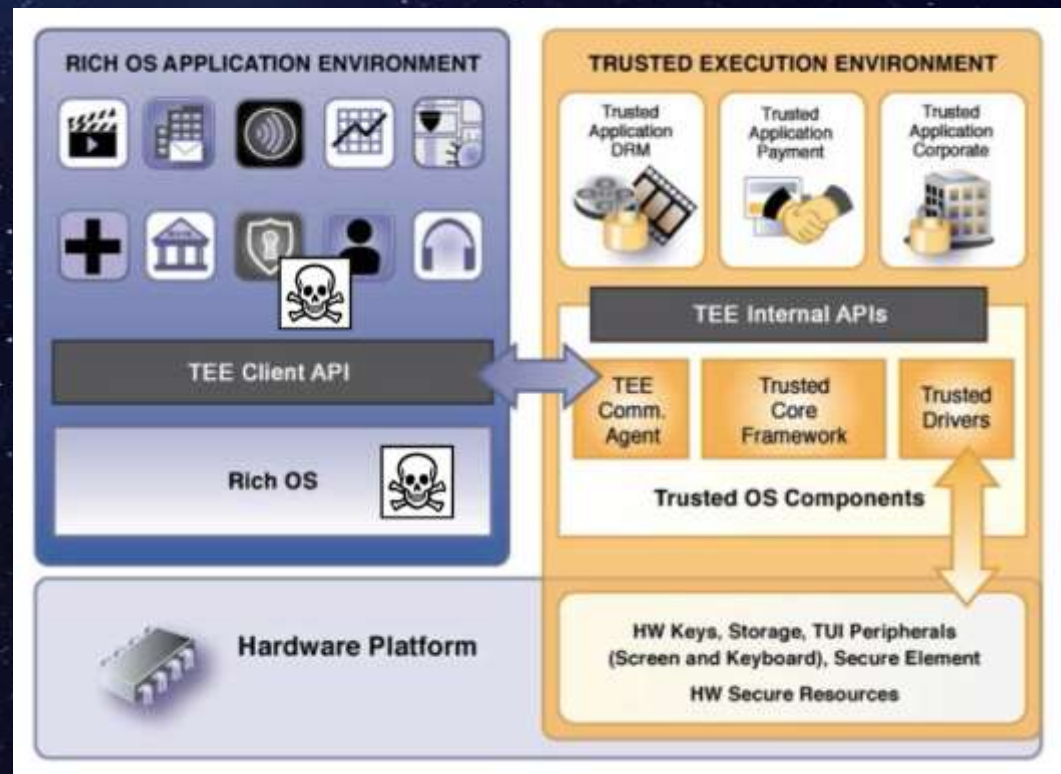
- 可信计算

※ 已广泛用于手机终端

- 保护终端安全
- 基本带指纹的手机都使用TEE技术
- 基于ARM TrustZone技术实现
- JRT 0156-2017 移动终端支付可信环境技术规范

※ 技术实质

- 提供基于硬件的隔离执行环境
- 能够保护敏感程序的执行和数据存储
- 可实现可信启动、完整性保护等功能
- 安全强度低于SE
- 近年来出现TEE+SE的解决方案：手机盾、手机POS、生物认证、手机非接支付



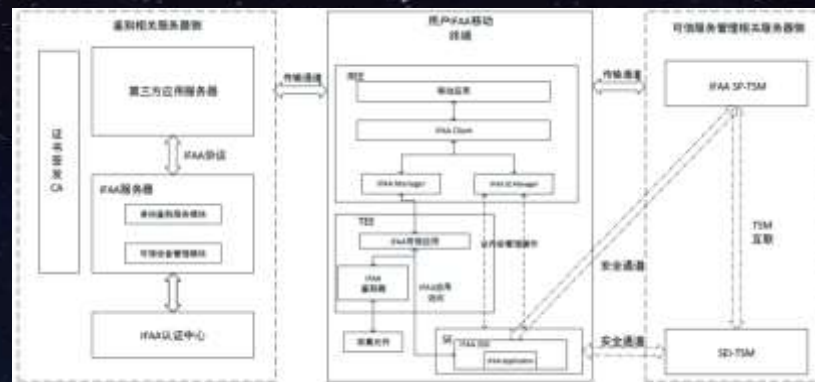
3.5 | 可信身份认证协议与方案

※ 硬件隔离结合可信身份认证协议的方案

- UKey (SE & CA证书协议)
- 手机盾 (TEE & CA证书协议)
- TUSI (SE & TUSI协议)
- FIDO (TEE & UAF、SE & UAF、SE & U2F)
- IFAA (TEE & IFAA标准)

※ 身份认证组织

- FIDO联盟 (线上快速身份验证联盟)
- IFAA联盟 (互联网金融身份认证联盟)
- BCTC是FIDO授权的安全检测实验室
- BCTC是IFAA测试认证组副组长, IoT安全工作组组长



本地免密2.1规范



国家金融IC卡安全检测中心

National Financial IC Card Security Test Center

银行卡检测中心

Bank Card Test Center

感谢聆听！



yangbo@bctest.com