FTF2016
TECHNOLOGY FORUM CHINA

MIFARE® DESFire ® EV2

新一代非接触式智能安全芯片

FTF-CIT-N1924

JOO MING CHUA (蔡裕铭)
产品经理

主题

- 介绍 MIFARE 和 MIFARE DESFire
- MIFARE DESFire 的革新
- 目标应用领域
- 创新功能介绍
- 未来蓝图

1994

MIFARE ® 的历史

革命性的开创了非接触式芯片技术的里程碑

2016

MIFARE ® 是非接触式安全芯片世界的领先者

MIFARE® DESFire® 的数据

超过
5亿 张
销量

> 65%
平均增长率
最近10年平均增长率

实用性证明
> 30
个应用场景

可用在
银行卡和
移动支付
多应用平台
多服务提供商

授权给
> 10
家公司

NFC
TagType4
兼容

系统集成商推荐的IC卡系统
公交卡,
门禁,
小额支付&
会员卡

在
> 90 城市
公交卡应用

> 10
个区域性和
全国性系统

兼容
> 10
国际和工业
标准

不断在创新的
MIFARE DESFire EVx平台
- 提供领先的
高安全,
隐私保护,
高性能&
多应用

可扩展性
- 小额金融支付
- 电子政务
- NFC手机,智能穿戴

MIFARE® DESFire® 的众多应用领域

小额支付系统

出租车卡

住宅门禁

交通票务

赛事活动门票

租车

楼宇门禁

校园卡

邮轮卡

酒店门禁

自行车租赁

图书卡

高速收费

音乐馆卡

城市一卡通

旅游卡

零售业会员卡

文件授权

游乐园

场馆

智能家居

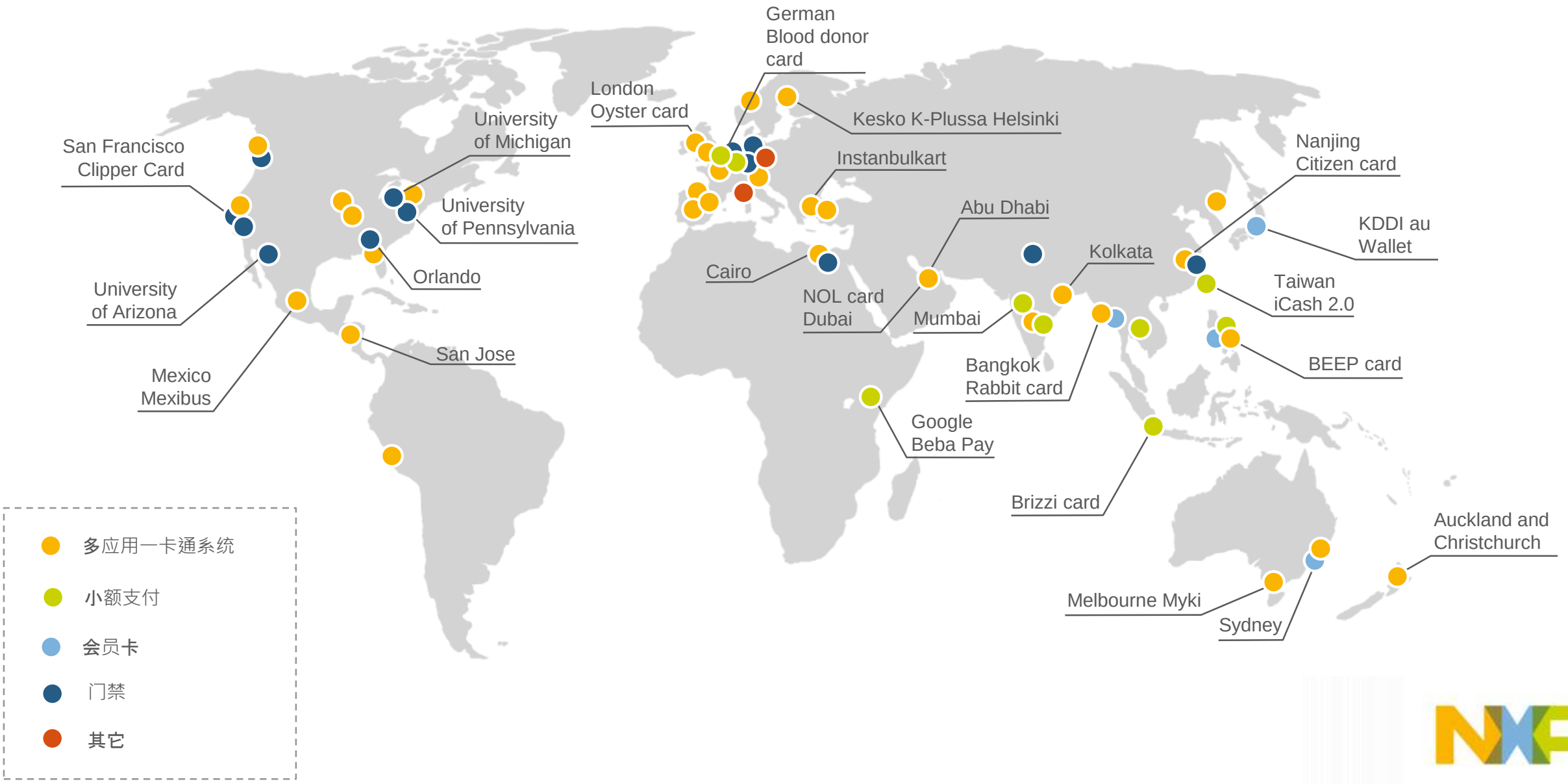
健身会员卡

停车

学生卡

加油卡

MIFARE® DESFire® 全球参考项目



MIFARE® DESFire® EV2 的发展历程

MIFARE DESFire EV2

2016

MIFARE DESFire EV1

2008

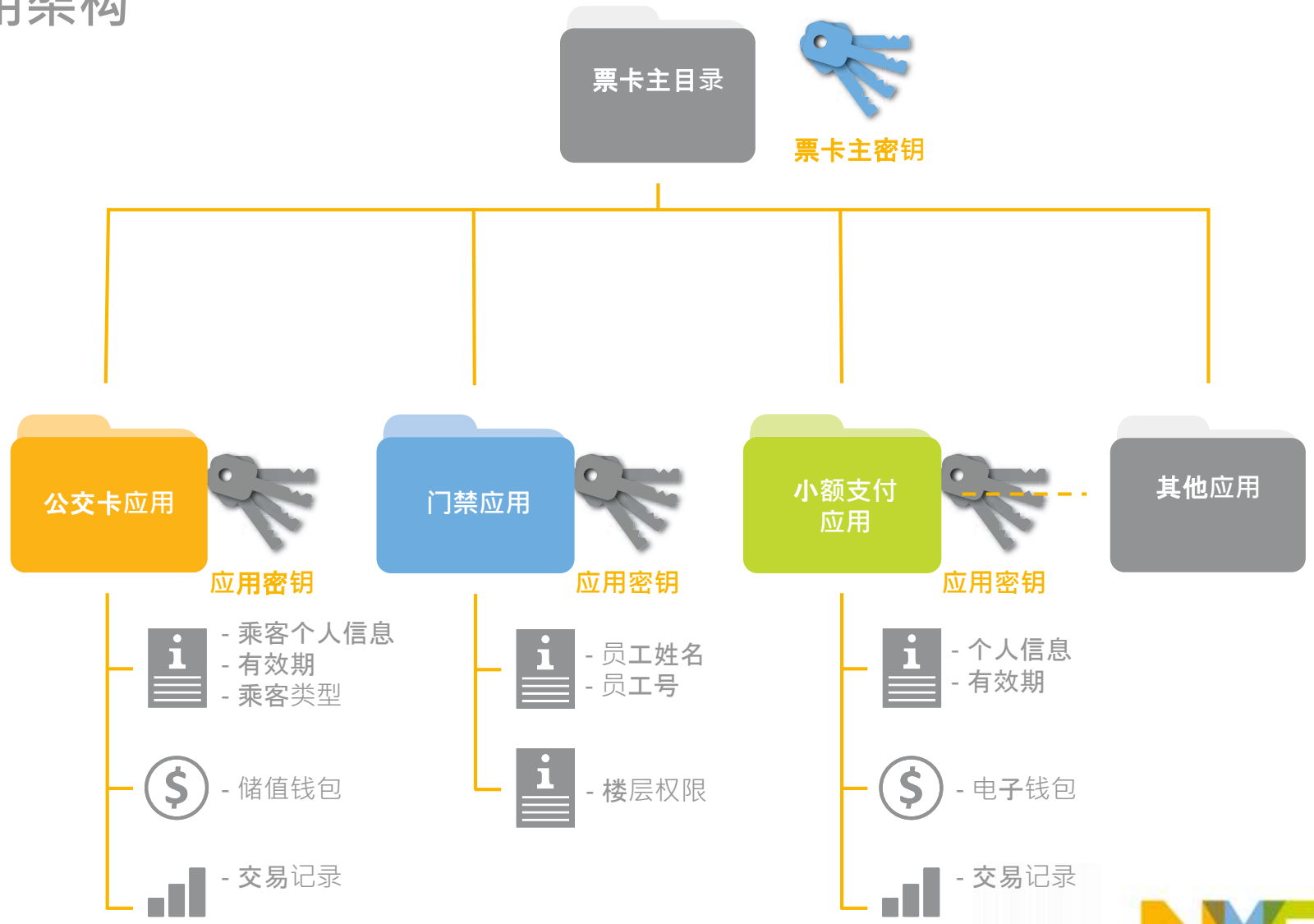
MIFARE DESFire

2002

	MIFARE DESFire EV1	MIFARE DESFire EV2
ISO/IEC 14443 A 1-4	✓	✓
ISO/IEC 7816-4 support	extended	extended
EEPROM data memory	2/4/8KB	2/4/8KB
Flexible file structure	✓	✓
NFC Forum Tag Type 4	✓	✓
Secure, high-speed cmd	✓	✓
Unique ID	7BUID or 4B RID	7BUID or 4B RID
Number of applications	28	unlimited
Number of files per app	32	32
High data rates support	up to 848 Kbit/s	up to 848 Kbit/s
Crypto algorithms support	DES/2K3DES/ 3K3DES/AES	DES/2K3DES/ 3K3DES/AES
CC certification (HW + SW)	EAL 4+	EAL 5+
MIsmartApp feature	-	✓
Transaction MAC per app	-	✓
Multiple keysets per app	-	Up to 16 keysets
Multiple file access rights	-	Up to 8 keys
Inter-app files sharing	-	✓
Virtual Card Architecture	-	✓
Proximity Check	-	✓
Delivery types	Wafer, MOA4 & MOA8	Wafer, MOA4 & MOB6

MIFARE® DESFire®
基于高安全级别的一卡多应用架构

- 可灵活定义的多应用文件系统
- 每一个应用都象一个文件夹一样易创建，生命周期管理同Windows系统
- 支持创建自定义的应用以及与应用相关的数据文件的创建
- 每一个应用支持独立密钥
- 卡发行商拥有票卡的主密钥



MIFARE® DESFire® EV2

MIFARE DESFire EV2 – 2k

MIFARE DESFire EV2 – 4k

MIFARE DESFire EV2 – 8k

- MIFARE® DESFire® 产品线的第三代产品
- 向下兼容MIFARE® DESFire® EV1 和 DESFire® D40
- 支持多应用，高扩展性
- 高性能的交易处理速度以及高效的读写距离
- 高安全性，获得CC EAL 5+（硬件＋软件）国际安全认证

支持标准卡
17pF versions

支持异型卡
70pF versions

MIFARE® DESFire® EV2 – 主要功能介绍

1 多应用场景

- **功能上向下兼容DESFire®**
  - 新老产品完美替代
- **支持OTA空发的功能，通过MIsmartApp实现**
  - 覆盖多应用的线上和线下场景
- **基于安全要素的多应用间的数据文件共享**
  - 应用于多应用交叉场景

2 高安全要求

- **独立应用管理下的密钥集设计**
  - 在线密钥更新，无需收回票卡
- **芯片层产生的交易MAC**
  - 交易合法性认证
- **世界级领先的芯片安全设计**
  - 最高安全保证

3 高性能指标

- **最优化的安全交易处理速度**
  - 快速且安全
- **良好的射频性能**
  - 优化读写距离
- **最优化的交易防撕裂特性**
  - 提高交易处理的完整性

性能特点

无缝向下兼容

- 现有的MIFARE® DESFire® 系统可以无缝迁移至最新产品EV2
- 无缝对接可以让用户直接体验最新产品带来的高性能和高扩展性

读写距离提升

- 更加友好的touch n' go用户体验
- 提升原有系统的用户体验
- 更快更可靠的交易处理性能

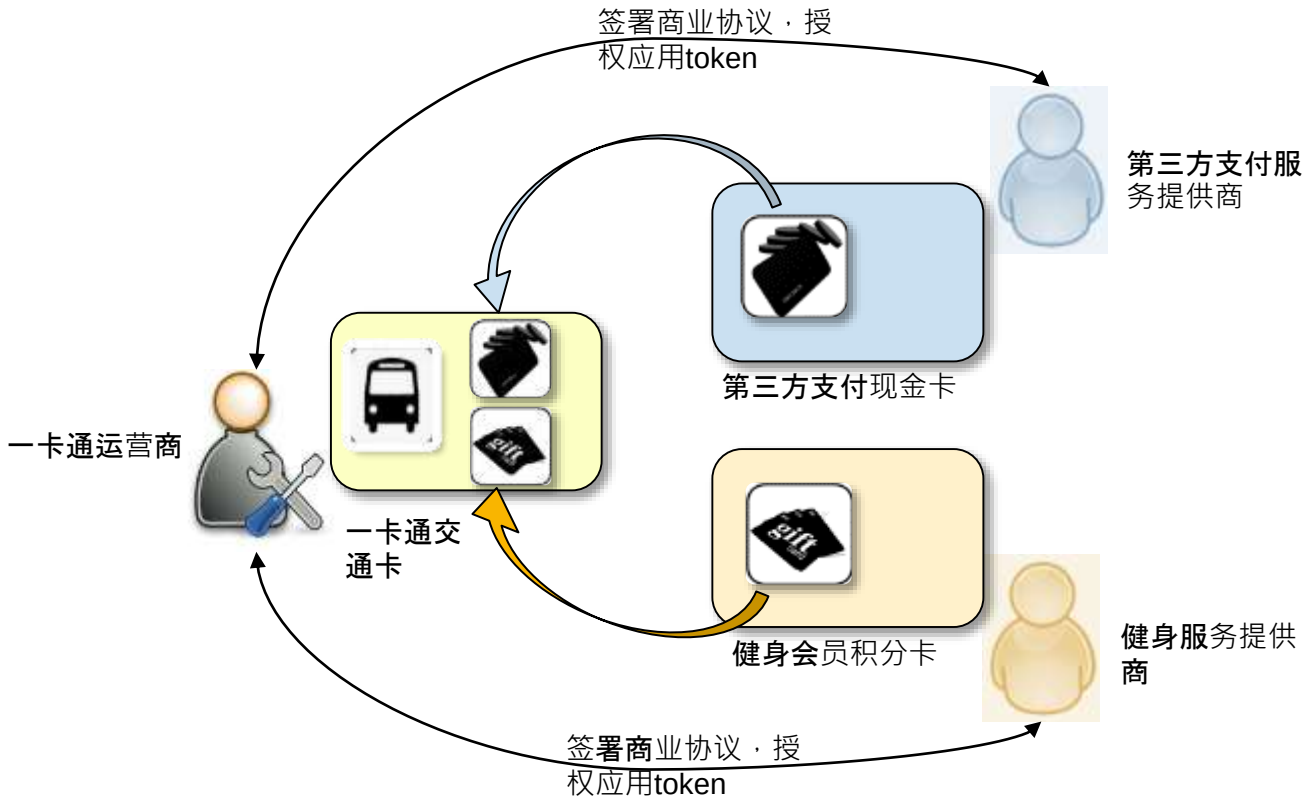
CC EAL 5+认证

- 提供与金融和电子护照同等安全级别的芯片解决方案
- 为客户和系统集成商提供可信赖的国际上广泛认可的最高安全认证证书

我们带来的创新

MIsmartApp

- MIsmartApp 功能可以提供新型的“线上与线下无缝对接的”商业模式。
- 空中发行(OTA)新应用 – 无需收回已发行的票卡。票卡发行商可以通过云端系统向已发行的票卡增加新的应用。
- 完美实现一卡多应用场景的互联互通。



我们带来的创新

芯片级别的交易MAC (TMAC)

- **芯片**层生成的交易MAC**从底**层保证了每一笔交易的真实可靠性。
  TMAC**采用的数字**签名技术提供了高可靠的交易防篡改性，**保**证了后台数据处理系统的有效验证
- **是适用于多运**营商，**多商**户应用场景下的一卡互联互通的完美解决方案。
- TMAC **有效的保**证了后台数据处理系统检测到:
  - **被**篡改的交易
  - **重复交易**
  - **非法机具**产生的交易
- 为离线交易提供了高可靠的应用场景

合法的离线交易

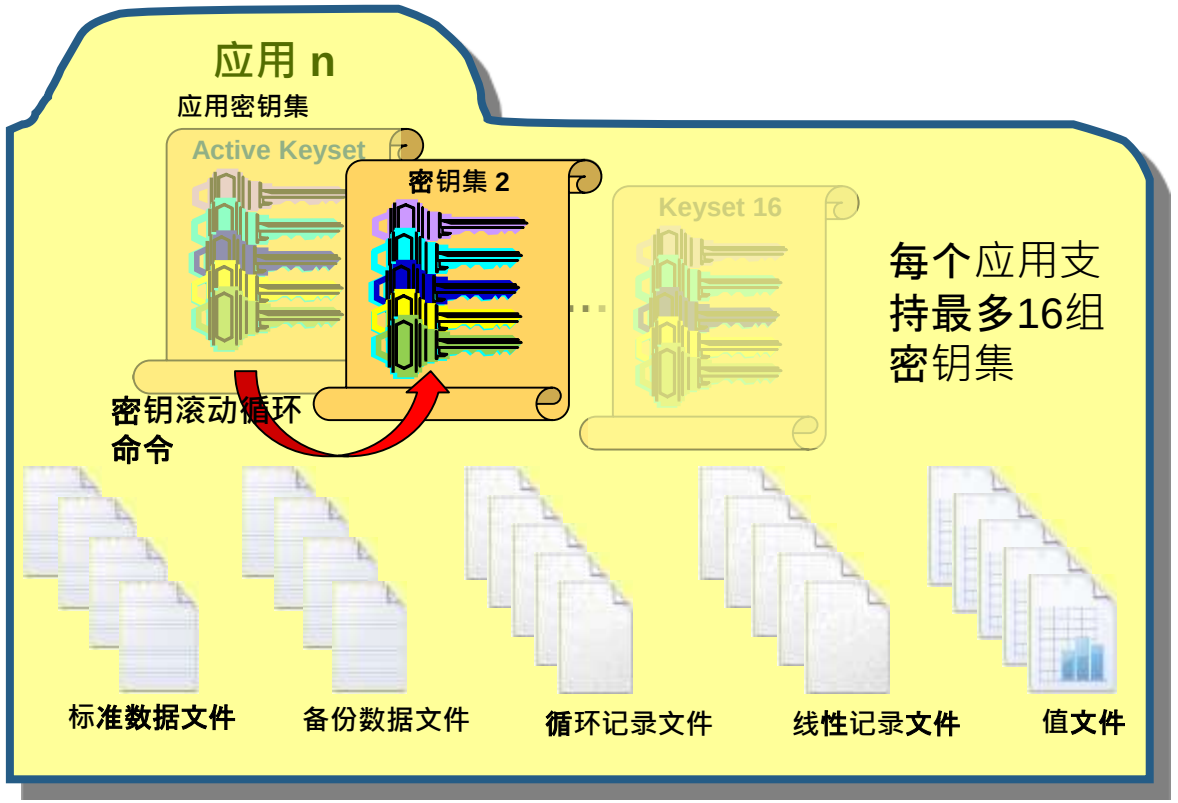
带TMAC**的交易数据**传至**任何**连线的设备

连接云端服务上传所有带**TMAC的交易数据至后台数据**处理系统验证。

我们带来的创新

滚动式密钥集设计

- 对于已发行的票卡支持在线密钥更新
- 通过密钥集内多密钥的循环滚动实现安全可信赖的密钥更新
- 定期密钥循环滚动可提高系统的防御能力，降低系统可被攻击的风险。
- 当正在使用的密钥被攻破时，自我修复机制会自动激活。
- 支持逐步从3DES系统架构升级至AES或3K3DES更高安全级别的加密机制。



MIFARE DESFire EV2 – 目标应用展望

小额支付

- MIsmartApp
- Transaction MAC

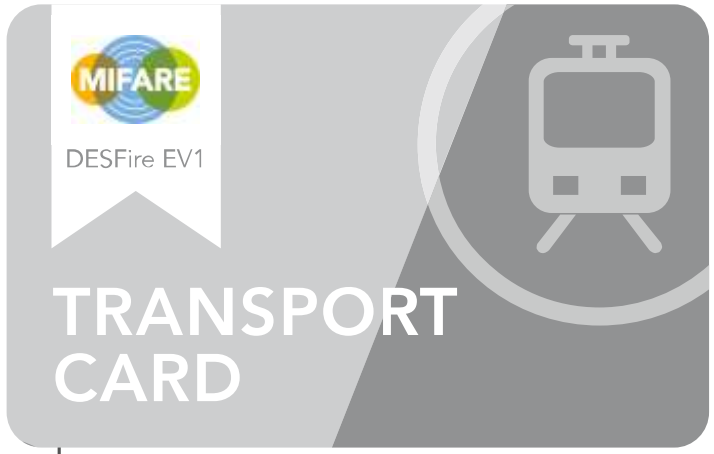
多应用场景互联互通

- MIsmartApp
- 向下兼容
- Transaction MAC
- 密钥集

楼宇门禁

- MIsmartApp
- 向下兼容
- 密钥集
- Transaction MAC

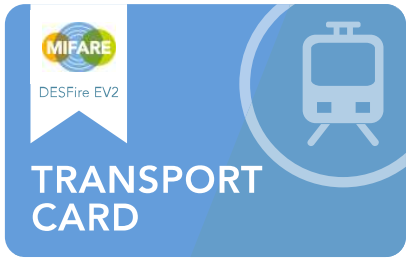
多应用场景定义



现有的一卡通交通卡

升级为

在以下应用中选择想要添加的新应用场景至现有的交通卡中




有轨电车


停车收费


自行车租赁


戏院门票


体育馆门票


大型活动门票


旅游景点门票


展览馆门票

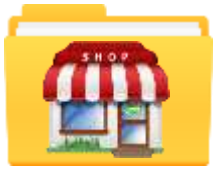

酒店门禁


公路收费


出租车付费


加油卡


宠物店消费


零售店消费

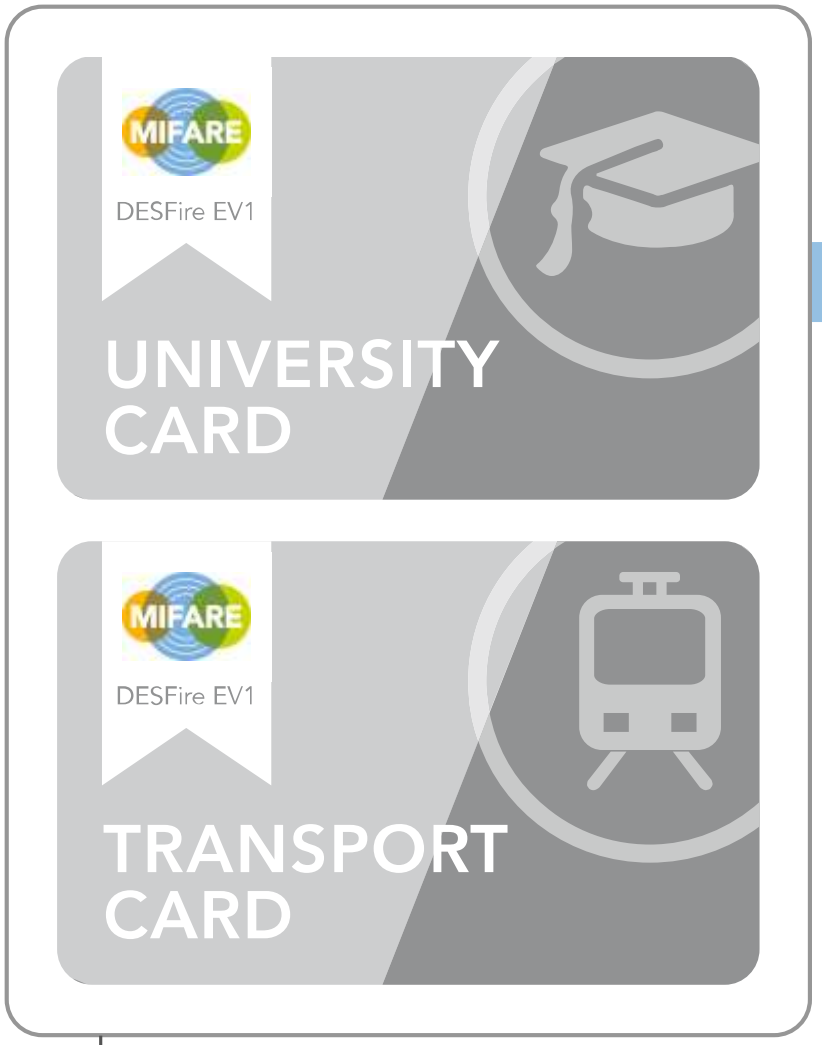

咖啡馆消费


餐饮消费


药店消费

NXP

多应用场景案例– 校园卡



出租车付费　自行车租赁

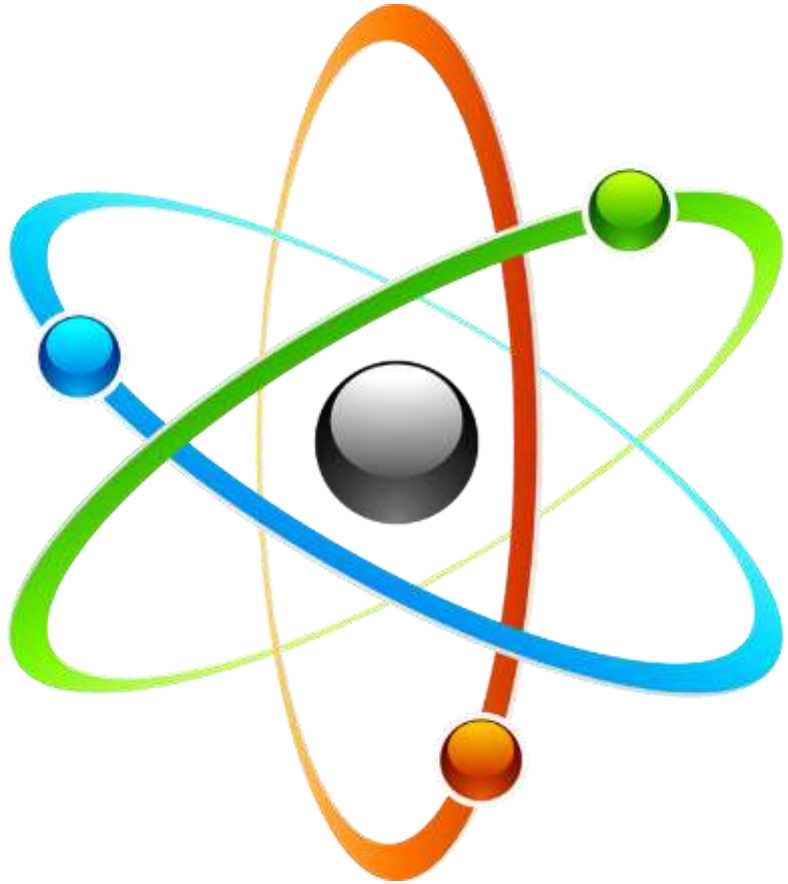
在以下应用中选择想要添加的新应用场景至现有的校园卡中

健身会员卡　音乐会门票　电影门票　剧院门票　运动会门票

零售商店　咖啡馆　餐馆　书店

MIFARE® DESFire® EV2 生态体系规划

- **APP Store**
  利用MIsmartApp提供多应用管理平台
- MIFARE® DESFire® EV2 **Applet**
  支持应用于手机，移动设备的环境
- **SmartMX平台的加载**
  支持高安全平台（如金融卡，政务系统等）上移植MIFARE® DESFire® EV2应用



- **提供安卓环境下的SDK**
  简化安卓环境下基于MIFARE® DESFire® EV2的软件开发
- **UL MIFARE® Certification**
  建立MIFARE® DESFire® EV2的授权认证体系

MIFARE® DESFire® EV2 的发布

产品发布状态:
MIFARE® DESFire® EV2 已开放订购

样品:
可通过NXP销售获取样品。

产品技术手册:
Datasheets, Application Notes, Software Tool and Reader Sample Code

技术文档获取：
https://www.docstore.nxp.com/flex/DocStoreApp.html

FOLLOW US:

https://twitter.com/nxp_mifare

http://blog.nxp.com/

www.youtube.com/user/nxpsemiconductors

https://at.linkedin.com/in/nxpmifare

https://www.facebook.com/nxpsemi

VISIT US AT: http://MIFARE.net

THANK YOU

Q&A

SECURE CONNECTIONS
FOR A SMARTER WORLD