恩智浦®
MIFARE Plus® EV2

无缝部署免接触式服务的安全性升级

这是第二代MIFARE Plus IC，不仅提升了性能和安全功能，还支持移动服务和无线更新，能够以经济高效的方式快速升级现有免接触式基础设施，实现AES安全性，同时提升智慧城市服务的体验和便利性。

主要特性

非接触式性能

- 符合ISO/IEC 14443 A 1-4和ISO/IEC 7816-4标准，可通过移动和可穿戴设备验收
- 优化的交易时间和射频性能
- MIFARE Classic向后兼容模式，可无缝迁移基础设施

迁移

- 用户可编程的激活参数（SAK和ATQA），完成基于MIFARE Classic产品的基础设施中所有安全等级（SL0、SL1和SL3）的初步迁移
- 在SL1SL3MixMode中，灵活地迁移到AES-128安全验证以及扇区级或芯片级讯息

安全性

- 经过安全等级CC EAL5+认证，可提供银行级安全保护
- 访问权限在SL1和SL3之间分割，以限制更新操作
- 通过基于卡片的交易MAC，进行在线和离线交易认证
- 智能卡片近距离检验，可检测中继攻击
- 具有交易定时器功能，有效防御“中间人”攻击

目标应用

- 公共交通
- 门禁管理
- 内部小额支付
- 校园和学生ID卡
- 会员管理
- 电子收费
- 停车

主要优点

- 向下兼容MIFARE Classic EV1和MIFARE Plus产品，可无缝迁移现有基础设施
- 从Crypto1升级到128位AES安全，保护等级更上一层楼
- 适用于无线服务（例如，智能卡移动充值）的端到端安全通信通道，并且在SL3部署MIFARE 2GO（移动服务）

作为新一代恩智浦MIFARE Plus产品系列，MIFARE Plus EV2 IC的设计用途不仅是充当新智慧城市应用的网关，更是对现有部署的安全性和连接性的一次卓越升级。与前代产品相比，IC能提供更长的读取范围功能和更快的交易时间，因此可以更方便地使用免接触式服务；另一方面，IC向下兼容MIFARE Classic EV1和MIFARE Plus产品，因而不需要大量的前期投资来启动迁移，就能以经济高效的方式升级本地智能卡应用的安全功能。

为现有基础设施提供有力支持

MIFARE Plus EV2 IC采用创新性的安全等级(SL)概念，有助于通过无缝式分步升级提高传统基础设施的安全性。IC基于128位AES安全功能进行验证并确保数据完整性和数据保护，实现从较低安全性(SL1)切换到较高安全性(SL3)的SL切换。SL切换可以整体应用于IC，也可以分别应用于单独扇区。通过名为SL1SL3MixMode的特殊特性，可对基于MIFARE Classic EV1的扇区进行AES-128安全验证。这样结合新的SL1更新限制，即可通过SL1验证读取模块中存储的数据，但必须通过AES-128安全验证才能更新数据。MIFARE Plus EV2的模块结构采用与Crypto1应用的模块结构相兼容的技术逻辑，因此基于Crypto1的部署都可以维持原有的结构逻辑。这就实现了经济高效的迁移路径，从传统MIFARE Classic EV1和Crypto1升级到高级别128位AES安全性。IC同时支持传统和新型基础设施，因此终端用户可以在继续使用相同智能卡的基础上，将系统升级到更高安全性，十分便捷。

扩展功能集实现了安全的非接触式智慧城市服务

特殊特性满足了智慧城市服务对更高安全性和隐私性的需求。例如，交易MAC (TMAC)有助于确保每笔交易的真实性，从而最大限度减少欺诈和身份盗用。为了帮助抵御“中间人”攻击，新的交易定时器功能（恩智浦MIFARE DESFire EV3 IC上也有提供）可以设置每笔交易的最长时间，从而增加攻击者干扰交易的难度。支持最大4 KB的EEPROM，有助于满足系统应用不断增长的内存要求。

支持手机和云服务

凭借MIFARE Plus EV2，移动交通票务和移动接入等智慧城市服务都能在支持NFC的智能手机和可穿戴设备上运行。以SL3等级运行MIFARE Plus EV2支持使用恩智浦MIFARE 2GO云服务，此服务可管理基于MIFARE产品的数字化凭据，并在支持NFC的设备上实现免接触式支付和移动接入等功能。通过使用MIFARE Plus EV2提供的端到端安全通信通道(SL1SL3MixMode)，系统运营商即使只有传统Crypto1应用，也能在引入无线服务（例如，移动充值）的基础上设计其他收入流。

功能比较：MIFARE Plus EV2与MIFARE Plus X

存储器	MIFARE Plus EV2	MIFARE Plus X
内存配置	模块/扇区结构	模块/扇区结构
存储器容量	2 kB / 4 kB	2 kB / 4 kB
RF接口		
ISO/IEC	ISO/IEC 14443 A 1-4 ISO/IEC 7816	ISO/IEC 14443 A 1-4 ISO/IEC 7816
UID/ONUID	7B UID或4B ONUID	7B UID或4B ONUID
数据传输速率	高达848 kbps, ISO/IEC 14443-4	高达848 kbps, ISO/IEC 14443-4
安全性		
算法	AES 128位，安全传送信息，传统Crypto1	AES 128位，安全传送信息，传统Crypto1
安全等级概念	逐个扇区或卡片	仅限卡片
SL1SL3MixMode	SL3访问SL1扇区	-
交易MAC (TMAC)	后端交易的安全验证	-
交易定时器	抵御“中间人”攻击	-
安全标准认证	EAL5+针对IC硬件和软件	EAL4+针对IC硬件和软件

订购信息

MIFARE Plus EV2	交付形式	17 pF	12NC
MF1P4200DA8/00	MOA8模块	4 k	935404786118
MF1P4200DA4/00	MOA4模块	4 k	935399739118
MF1P4201DUD/00	晶圆120 µm 12”	4 k	935405406045
MF1P2200DA8/00	MOA8模块	2 k	935387932118
MF1P2200DA4/00	MOA4模块	2 k	935404211118
MF1P2201DUD/00	晶圆120 µm 12”	2 k	935405407045
MIFARE Plus EV2	**交付形式**	**70 pF**	**12NC**
MF1PH4200DA8/00	MOA8模块	4 k	935383644118
MF1PH4200DA4/00	MOA4模块	4 k	935383641118
MF1PH4201DUD/00	晶圆120 µm 12”	4 k	935405499045
MF1PH2200DA8/00	MOA8模块	2 k	935405195118
MF1PH2200DA4/00	MOA4模块	2 k	935405183118
MF1PH2201DUD/00	晶圆120 µm 12”	2 k	935405497045

发布日期：2020年6月23日
文档编号：MFPLUSEV2LF REV0