



恩智浦®
MIFARE® DESFire® EV3

为安全互联智慧城市服务的新时代奠定坚实基础

恩智浦久经验证的免接触式MIFARE DESFire产品组合迎来第三次演变, MIFARE DESFire EV3 IC凭借新一代性能、更高水平的安全特性以及移动服务的无缝集成, 引领智慧城市服务的新时代。

主要特性

- ▶ 兼容ISO/IEC 14443 A 1-4和ISO/IEC 7816-4标准
- ▶ IC硬件和软件经认证符合通用标准EAL5+
- ▶ 经认证符合NFC Forum 4类标签规格
- ▶ 通过SUN消息验证, 在标准NDEF读取操作中提供先进的数据保护。
- ▶ 具有灵活的文件架构, 实现真正的多应用操作
- ▶ 应用间文件共享, 使多个应用共用一个钱包
- ▶ 可灵活选择各种开放式DES/2K3DES/3K3DES/AES加密算法
- ▶ 每个应用都有多个密钥组, 实现签发后滚动应用密钥
- ▶ 利用基于卡片的MAC, 完成交易认证
- ▶ 具有交易定时器功能, 有效防御“中间人”攻击
- ▶ 采用虚拟卡架构, 确保隐私保护
- ▶ 配备近距离检验, 检测中继攻击

目标应用

- ▶ 公共交通
- ▶ 住宅楼宇园区门禁应用
- ▶ 闭环小额支付
- ▶ 校园和学生ID卡
- ▶ 会员卡管理

主要特性

- ▶ 在MIFARE DESFire EV3上运行的服务都能通过MIFARE 2GO轻松部署到NFC手机上
- ▶ 预加载了用于托管应用管理的密钥, 允许在已经部署的卡片中添加新的应用服务
- ▶ 功能向下兼容MIFARE DESFire EV2和MIFARE DESFire EV1, 提供无缝升级路径
- ▶ 与前代产品相比, 工作范围更大且交易速度更快, 改善了用户体验和安全性



更安全、更方便的MIFARE DESFire EV3 IC面向多种智慧城市服务(包括公共交通和门禁系统),为运营商和终端用户带来显著优势。

量身定制的安全与隐私支持

特别为了满足智慧城市服务对更高安全性和隐私性的需求。例如,基于片卡的MAC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。

恩智浦的NTAG 424 DNA IC上还配备新的“安全唯一NFC”(SUN)讯息功能,可以更安全地保护数据机密性和完整性。每次点击配备MIFARE DESFire EV3 IC的卡片或票据时,SUN讯息功能都会基于CMAC计算生成一条唯一的认证消息。随后,可将点击专用的URL及其安全加密SUN代码发送到服务器进行验证。在NDEF模式下运行时,SUN讯息功能与NFC手机和其他支持NFC的设备相兼容,因而在各种使用广泛的现成设备上,都能方便地完成标签和消息的安全验证。

非接触式性能

为了实现真正便利的“一碰就通过”的体验,MIFARE DESFire EV3 IC提供了比前几代版本更远的操作距离和更快的交易速度。70 pF选项有助于小尺寸天线的读取范围优化。与恩智浦的MIFARE DESFire EV1 IC相比,交易速度加快了1.5倍,因此运营商无需更新读卡器基础设施,就能提高系统效率并改善终端用户体验。

专注移动化

使用恩智浦的MIFARE 2GO云服务,在MIFARE DESFire EV3上运行的智慧城市服务便可部署到支持NFC的智能手机和可穿戴设备上。MIFARE 2GO管理基于MIFARE产品的数字化凭据,可启用设备上的无接触式支付或门禁管理功能。

为多个智慧城市应用打下基础

每个MIFARE DESFire EV3 IC都预先配置了密钥,便于托管应用管理,这支持无线更新已签发的智能卡片,从而更轻松地向现有用户部署更多服务。预先加载的密钥支持对每个IC进行个性化设置,而无需强制要求发卡机构管理和交付一组新的密钥。

特性

MIFARE DESFire EV3	
存储器	
非易失性(NV)大小[kB]	2/4/8
写入操作耐受程度[周期]	1,000,000
数据保持能力[年]	25
RF接口	
符合ISO/IEC 14443A	是 - 最高可4层
频率[MHz]	13.56
波特率[kbits/s]	106 ... 848
工作距离[mm]	最多100
安全性	
唯一序列号[字节]	7, 级联
访问密钥	每个应用14个密钥
多个密钥组	每个应用最多16组
访问条件	每个访问权限最多8个密钥
AES、2K3DES和3K3DES加密	MACing/加密
片上防修改支持	是
通用标准认证(硬件+软件)	EAL5+
特殊特性	
多应用	数量无限制,只要内存支持,托管应用管理
每个应用程序的文件数	32
钱包功能	值文件
应用间文件共享	是
交易MAC	每个应用都支持
SUN(安全唯一NFC消息)	是,兼容NTAG DNA

订购信息:MIFARE DESFIRE EV3

	2 kB	4 kB	8 kB
17 pF	器件分类		
晶圆	MF3D2301DUD/00	MF3D4301DUD/00	MF3D8301DUD/00
MOA4	MF3D2300DA4/00	MF3D4300DA4/00	MF3D8300DA4/00
MOA8	MF3D2300DA8/00	MF3D4300DA8/00	MF3D8300DA8/00
70 pF	器件分类		
晶圆	MF3DH2301DUD/00	MF3DH4301DUD/00	MF3DH8301DUD/00
MOA4	MF3DH2300DA4/00	MF3DH4300DA4/00	MF3DH8300DA4/00
MOA8	MF3DH2300DA8/00	MF3DH4300DA8/00	MF3DH8300DA8/00

www.nxp.com

恩智浦、恩智浦徽标、MIFARE、DESFire、MIFARE徽标和NTAG是NXP B.V.的注册商标。所有其他产品或服务名称均为其各自所有者的财产。© 2020 NXP B.V.

发布日期: 2020年5月19日
文档编号: MFDLFEV3 REV0



www.MIFARE.net