NXP®
MIFARE Plus® EV2

Implementação ininterrupta de atualizações de segurança para serviços sem contato

O CI (Circuito Integrado) MIFARE Plus de segunda geração, equipado com funcionalidades aprimoradas de desempenho e segurança, juntamente com suporte para serviços móveis e atualizações remotas (over-the-air), é uma maneira rápida e econômica de atualizar para a segurança da criptografia AES as infraestruturas sem contato existentes, além de oferecer melhor experiência e maior conveniência nos serviços das chamadas Smart Cities (Cidades Inteligentes).

PRINCIPAIS RECURSOS

Desempenho sem contato

- ISO/IEC 14443 A 1-4 e ISO/IEC 7816-4 para aceitação de dispositivos móveis e vestíveis
- Melhores tempos de transação e desempenho de RF
- Modo de retro compatibilidade com MIFARE Classic para a migração ininterrupta das infraestruturas existentes

Migração

- Parâmetros de ativação programados pelo usuário (SAK e ATQA) para migração preliminar de todos os níveis de segurança (SL0, SL1 e SL3) em infraestruturas baseadas no MIFARE Classic
- Migração flexível para garantir autenticação AES-128 e serviço de mensagens de texto a nível de setor ou de chip no SL1SL3MixMode

Segurança

- Nível de proteção de serviços bancários com certificação Common Criteria EAL5+
- Divisão dos direitos de acesso entre SL1 e SL3 para restringir as operações de atualização
- Comprovação de transação on-line e off-line através do Transaction MAC gerado por cartão
- Verificação de proximidade de cartão inteligente para detectar ataques de retransmissão
- Timer de transação para prevenir ataques man-in-the-middle (dispositivos NFC entre o cartão e a leitora)

APLICATIVOS ALVO

- Transporte público
- Gerenciamento de acesso
- Micro pagamento em closed-loop (transação não Bancária)
- Cartões de identificação de alunos em escolas e universidades
- Programas de fidelidade
- Cobrança eletrônica de pedágio
- Estacionamento

PRINCIPAIS BENEFÍCIOS

- Migração ininterrupta de infraestruturas existentes, com retro compatibilidade com os produtos MIFARE Classic EV1 e MIFARE Plus
- Proteção de nível superior com atualizações de segurança de Crypto1 para AES de 128 bits
- Canal de comunicação seguro de ponta a ponta para serviços sem fios (over-the-air), como recarga móvel de cartões inteligentes e implementação de MIFARE 2GO (serviços móveis) em SL3

Sendo a próxima geração de produtos da linha MIFARE Plus da NXP, o MIFARE Plus EV2 CI foi criado para ser uma porta de entrada para os novos aplicativos de Cidade Inteligente (Smart City) e uma atualização muito atrativa, em termos de segurança e de conectividade, para implementações existentes. O CI demonstra maior capacidade de alcance de leitura e tempos de transação mais rápidos em relação ao seu predecessor, facilitando a utilização de serviços sem contato, e é retro compatível com os produtos MIFARE Classic EV1 e MIFARE Plus, propiciando uma maneira econômica de atualizar as funcionalidades de segurança dos aplicativos de cartão inteligente implementadas, sem a necessidade de grandes investimentos antecipados para iniciar as migrações.

SUPORTE SÓLIDO DAS INFRAESTRUTURAS EXISTENTES

O MIFARE Plus EV2 CI utiliza um conceito inovador de níveis de segurança, (SL, Nível de Segurança em Inglês) para ajudar a criar atualizações ininterruptas passo a passo das infraestruturas existentes para níveis de segurança mais altos. O CI permite mudar o SL de segurança baixa (SL1) para segurança alta (SL3), com base na segurança da criptografia AES de 128 bits para autenticação, integridade de dados e proteção de dados. A mudança de SL pode ser aplicada a todo o CI ou apenas para setores individuais. Graças a uma funcionalidade especial, chamada SL1SL3MixMode, é possível ativar a autenticação de segurança AES-128 em setores baseados no MIFARE Classic EV1. Juntamente com as novas Restrições de Atualização em SL1, isso possibilita a leitura dos dados armazenados em um bloco com autenticação SL1, mas a atualização dos dados só é possível com autenticação AES-128 segura. A estrutura em bloco do MIFARE Plus EV2 utiliza uma lógica de tecnologia compatível com a estrutura baseada em bloco dos aplicativos com Crypto1, assim as implementações baseadas em Crypto1 podem manter a sua lógica estrutural. Isso possibilita criar caminhos econômicos de migração da segurança do MIFARE Classic EV1 e Crypto1 existentes para a segurança avançada do AES de 128 bits. Visto que o CI é compatível simultaneamente com infraestruturas novas e existentes, os usuários finais podem continuar utilizando o mesmo cartão inteligente enquanto o sistema é atualizado para um nível de segurança mais alto.

CONJUNTO DE FUNCIONALIDADES AVANÇADAS PARA SERVIÇOS SEGUROS E SEM CONTATO EM CIDADES INTELIGENTES (SMART CITY)

As funcionalidades especiais abordam a necessidade de maior segurança e privacidade para os serviços nas Cidades Inteligentes. Por exemplo, o Transaction MAC (TMAC) pode ajudar a garantir a autenticidade de cada transação para minimizar as fraudes e o roubo de identidade. Para ajudar a mitigar ataques man-in-the-middle (dispositivos NFC entre o cartão e a leitora), a nova funcionalidade de Timer de transação, também disponível no MIFARE DESFire EV3 CI da NXP, possibilita definir um tempo máximo por transação, dificultando que atacantes interfiram na transação. O suporte de EEPROM com tamanho de até 4 Kbytes ajuda a satisfazer os requisitos cada vez maiores de memória dos aplicativos do sistema.

www.nxp.com, www.MIFARE.net

Data de lançamento: 23 de junho de 2020
Número do documento: MFPLUSEV2LF REV0

SUPORTE PARA SERVIÇOS MÓVEIS E DE ATUALIZAÇÃO REMOTA SEM FIO (OVER-THE-AIR)

Com o MIFARE Plus EV2, os serviços das Cidades Inteligentes, como emissão de bilhetes para transportes e acesso usando dispositivos móveis, podem ser executados em smartphones e vestíveis, como pulseiras inteligentes, com NFC. A operação do MIFARE Plus EV2 em SL3 suporta a utilização do serviço na nuvem MIFARE 2GO da NXP, que gerencia credenciais digitalizadas baseadas no produto MIFARE e habilita funcionalidades como pagamentos sem contato e acesso móvel utilizando dispositivos NFC. Com o canal seguro de comunicação de ponta a ponta (SL1SL3MixMode) fornecido pelo MIFARE Plus EV2, os operadores do sistema podem criar novas fontes de rendimento baseadas na introdução de serviços sem fio, como recargas móveis, mesmo com os aplicativos Crypto1 existentes.

COMPARAÇÃO DE FUNCIONALIDADES: MIFARE Plus EV2 e MIFARE Plus X

Memória	MIFARE Plus EV2	MIFARE Plus X
Configuração da memória	Estrutura de blocos/ setores	Estrutura de blocos/ setores
Tamanho da memória	2 kB / 4 kB	2 kB / 4 kB
Interface RF		
ISO/IEC	ISO/IEC 14443 A 1-4 ISO/IEC 7816	ISO/IEC 14443 A 1-4 ISO/IEC 7816
UID/ONUID	7B UID ou 4B ONUID	7B UID ou 4B ONUID
Transferência de dados	Até 848 kbps, ISO/IEC 14443-4	Até 848 kbps, ISO/IEC 14443-4
Segurança		
Algoritmo	AES de 128 bits, mensagens de texto seguras, Crypto1 existente	AES de 128 bits, mensagens de texto seguras, Crypto1 existente
Conceito de nível de segurança	Setor a setor ou cartão	Apenas cartão
SL1SL3MixMode	Acesso SL3 nos setores SL1	-
Transação MAC (TMAC)	Validação segura de transações de processo interno (back-end)	-
Temporizador de transações	Mitigação de ataques man-in-the-middle (dispositivos NFC entre o cartão e a leitora)	-
Certificação Common Criteria	EAL5+ para CI HW e SW	EAL4+ para CI HW e SW

INFORMAÇÕES DE PEDIDOS

MIFARE Plus EV2	Formato de entrega	17 pF	12NC
MF1P4200DA8/00	Módulo MOA8	4 k	935404786118
MF1P4200DA4/00	Módulo MOA4	4 k	935399739118
MF1P4201DUD/00	Wafer 120 µm 12"	4 k	935405406045
MF1P2200DA8/00	Módulo MOA8	2 k	935387932118
MF1P2200DA4/00	Módulo MOA4	2 k	935404211118
MF1P2201DUD/00	Wafer 120 µm 12"	2 k	935405407045
MIFARE Plus EV2	**Formato de entrega**	**70 pF**	**12NC**
MF1PH4200DA8/00	Módulo MOA8	4 k	935383644118
MF1PH4200DA4/00	Módulo MOA4	4 k	935383641118
MF1PH4201DUD/00	Wafer 120 µm 12"	4 k	935405499045
MF1PH2200DA8/00	Módulo MOA8	2 k	935405195118
MF1PH2200DA4/00	Módulo MOA4	2 k	935405183118
MF1PH2201DUD/00	Wafer 120 µm 12"	2 k	935405497045