NXP®
MIFARE Plus® EV2

Безшовное обновление уровня безопасности для бесконтактных инфраструктур

Новое поколение микросхем MIFARE Plus, обладает улучшенными параметрами производительности и безопасности, с поддержкой мобильных сервисов и беспроводных обновлений. Данный продукт является быстрым и экономичным способом обновления существующих бесконтактных инфраструктур до уровня AES безопасности. Также продукт позволяет с большим удобством пользоваться сервисами Smart City.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Бесконтактная работа

- Стандарты ISO/IEC 14443 A 1-4 и ISO/IEC 7816-4 для мобильных и носимых устройств
- Улучшенное время транзакции и RF-производительность
- Режим обратной совместимости с MIFARE Classic для бесшовной миграции

Миграция

- Программируемые пользователем параметры активации (SAK & ATQA) для предварительной миграции всех уровней безопасности (SL0, SL1 и SL3) в инфраструктурах MIFARE Classic
- Гибкий переход к безопасной аутентификации с шифрованием AES-128 и обмену сообщениями, как на уровне одного сектора, так и всего чипа в режиме SL1SL3MixMode

Безопасность

- Высокий уровень защиты благодаря сертификации по стандарту Common Criteria EAL5+
- Разделение прав доступа между уровнями SL1 и SL3 для ограничения операций по обновлению
- Онлайн- и офлайн-подтверждение транзакций с помощью генерируемого картой MAC-кода транзакций
- Проверка близости смарт-карты для обнаружения relay атак
- Таймер транзакций для борьбы с атаками man-in-the-middle

ПРЕДНАЗНАЧЕНИЕ

- Общественный транспорт
- СКУД
- Замкнутые системы микроплатежей
- Студенческие билеты и членские удостоверения
- Программы лояльности
- Электронный сбор платежей
- Парковки

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Бесшовная миграция существующих инфраструктур благодаря обратной совместимости с продуктами MIFARE Classic EV1 и MIFARE Plus
- Более высокий уровень безопасности благодаря миграции с Crypto1 до 128-битного AES-шифрования
- Безопасный канал для таких беспроводных услуг, как пополнение смарт-карт на мобильных устройствах и развертывание MIFARE 2GO (мобильные услуги) на уровне SL3

Микросхема MIFARE Plus EV2— это следующее поколение семейства продуктов MIFARE Plus от компании NXP. Они созданы не только для запуска новых проектов умных городов, но и для значительного обновления функций обеспечения безопасности текущих систем. MIFARE Plus EV2 предлагает более широкие возможности считывания и выполняет транзакции быстрее предыдущей версии. Это делает бесконтактные сервисы еще более удобными в использовании. Кроме того, MIFARE Plus EV2 имеет обратную совместимость с продуктами MIFARE Classic EV1 и MIFARE Plus, обеспечивая экономичное обновление безопасности в приложениях с использованием смарт-карт без необходимости в значительных предварительных вложениях для начала миграции.

НАДЕЖНАЯ ПОДДЕРЖКА СУЩЕСТВУЮЩИХ ИНФРАСТРУКТУР

В MIFARE Plus EV2 используется инновационная концепция безопасности Security Level (SL) для бесшовного обновления устаревших инфраструктур, помогающих повысить уровень безопасности. Микросхема позволяет переключаться с более низкого уровня безопасности (SL1) на более высокий (SL3) на основе 128-битного AES-шифрования для аутентификации и обеспечения целостности и защиты данных. Можно переключать уровни безопасности как для всей карты, так и для отдельных секторов. Специальная функция под названием SL1SL3MixMode дает возможность включать аутентификацию с шифрованием AES-128 по секторам на базе MIFARE Classic EV1. В сочетании с новой функцией ограничения обновлений уровня SL1 это дает возможность считывать хранящиеся в блоке данные, используя при этом аутентификацию уровня SL1, но обновлять данные можно только с помощью аутентификации с шифрованием AES-128. Блочная структура MIFARE Plus EV2 предусматривает технологическую логику, совместимую с приложениями Crypto1, имеющими структуру на основе блоков, поэтому системы на базе Crypto1 могут сохранять свою структурную логику. Это обеспечивает экономичные пути перехода с систем на базе технологий MIFARE Classic EV1 и Crypto1 на 128-битное AES-шифрование, гарантирующее более высокую безопасность. Поскольку микросхема одновременно поддерживает и новые, и текущие инфраструктуры, конечные пользователи могут продолжать использовать ту же смарт-карту, при этом обновляя систему до более высокого уровня безопасности.

РАСШИРЕННЫЙ НАБОР ВОЗМОЖНОСТЕЙ ДЛЯ БЕЗОПАСНЫХ БЕСКОНТАКТНЫХ СЕРВИСОВ УМНОГО ГОРОДА

Специальные функции соответствуют высоким требованиям стандартов умного города к безопасности и конфиденциальности. Например, Transaction MAC (TMAC) обеспечивает подлинность каждой транзакции, сводя к минимуму число случаев мошенничества и кражи личных данных. Для устранения атак man-in-the-middle представлена новая функция таймера транзакций, которая также доступна для карты NXP MIFARE DESFire EV3 IC, позволяющая устанавливать максимальное время проведения транзакции, чтобы злоумышленнику было труднее в нее вмешиваться. Поддержка EEPROM объемом до 4 килобайт помогает удовлетворить растущие требования к памяти системных приложений.

www.nxp.com, www.MIFARE.net

Дата выпуска: 23 июня 2020 г.
Номер документа: MFPLUSEV2LF REV0

ПОДДЕРЖКА ФУНКЦИЙ НА МОБИЛЬНЫХИ НОСИМЫХ УСТРОЙСТВАХ

Благодаря MIFARE Plus EV2 такие сервисы умного города, как мобильная система оплаты проезда и мобильный доступ, могут работать на смартфонах и носимых устройствах с поддержкой NFC. Использование MIFARE Plus EV2 с уровнем безопасности SL3 предусматривает поддержку облачной службы NXP MIFARE 2GO, позволяющая пользоваться цифровыми версиями на базе продуктов MIFARE и обеспечивающей работу таких функций, как бесконтактная оплата и мобильный доступ с устройств с поддержкой NFC. Используя защищенный сквозной канал связи (SL1SL3MixMode), предоставляемый MIFARE Plus EV2, операторы систем могут создавать дополнительные источники дохода, основанные на внедрении беспроводных служб, например пополнении мобильных телефонов, даже с устаревших приложений Crypto1.

СРАВНЕНИЕ ХАРАКТЕРИСТИК И ВОЗМОЖНОСТЕЙ MIFARE Plus EV2 и MIFARE Plus X

Память	MIFARE Plus EV2	MIFARE Plus X
Конфигурация памяти	Блочная/секторная структура	Блочная/секторная структура
Объем памяти	2 КБ/4 КБ	2 КБ/4 КБ
РЧ-интерфейс		
ISO/IEC	ISO/IEC 14443 A 1-4 ISO/IEC 7816	ISO/IEC 14443 A 1-4 ISO/IEC 7816
UID/ONUID	7B UID или 4B ONUID	7B UID или 4B ONUID
Скорость передачи данных	До 848 Кбит/с, ISO/IEC 14443-4	До 848 Кбит/с, ISO/IEC 14443-4
Безопасность		
Алгоритм	128-битное AES-шифрование, безопасный обмена сообщениями, устаревшая система Crypto1	128-битное AES-шифрование, безопасный обмена сообщениями, устаревшая система Crypto1
Концепция уровня безопасности	По секторам или для всей карты	Только для карты
SL1SL3MixMode	Доступ уровня SL3 к секторам уровня SL1	-
MAC-идентификатор транзакций (TMAC)	Безопасная проверка внутренних транзакций	-
Таймер транзакции	Защита от man-in-the-middle атак	-
Сертификация Common Criteria	EAL5+ для аппаратного и программного обеспечения IC	EAL4+ для аппаратного и программного обеспечения IC

ИНФОРМАЦИЯ ДЛЯ ЗАКАЗА

MIFARE Plus EV2	Форм фактор	17 пФ	12NC
MF1P4200DA8/00	Модуль MOA8	4 k	935404786118
MF1P4200DA4/00	Модуль MOA4	4 k	935399739118
MF1P4201DUD/00	Пластина 120 мкм, 12 дюймов	4 k	935405406045
MF1P2200DA8/00	Модуль MOA8	2 k	935387932118
MF1P2200DA4/00	Модуль MOA4	2 k	935404211118
MF1P2201DUD/00	Пластина 120 мкм, 12 дюймов	2 k	935405407045
MIFARE Plus EV2	**Форм фактор**	**70 пФ**	**12NC**
MF1PH4200DA8/00	Модуль MOA8	4 k	935383644118
MF1PH4200DA4/00	Модуль MOA4	4 k	935383641118
MF1PH4201DUD/00	Пластина 120 мкм, 12 дюймов	4 k	935405499045
MF1PH2200DA8/00	Модуль MOA8	2 k	935405195118
MF1PH2200DA4/00	Модуль MOA4	2 k	935405183118
MF1PH2201DUD/00	Пластина 120 мкм, 12 дюймов	2 k	935405497045