



NXP®
MIFARE Plus® EV2

Implementación sencilla de actualizaciones de seguridad para servicios sin contacto

Esta segunda generación de MIFARE Plus IC, con características mejoradas de rendimiento y seguridad, es compatible con los servicios móviles y las actualizaciones inalámbricas, y representa una manera rápida y rentable de implementar la seguridad AES en las infraestructuras sin contacto existentes, así como ofrecer mejores experiencias y mayor comodidad en servicios de Smart City.

PRINCIPALES CARACTERÍSTICAS

Rendimiento sin contacto

- ▶ Compatibilidad con las normas ISO/IEC 14443 A 1-4 e ISO/IEC 7816-4 para móviles y dispositivos portátiles
- ▶ Tiempos de transacción mejorados y mayor rendimiento RF
- ▶ Modo de compatibilidad con MIFARE Classic para una migración sencilla de la infraestructura

Migración

- ▶ Parámetros de activación programables por el usuario (SAK y ATQA) para migraciones preliminares de todos los niveles de seguridad (SL0, SL1 y SL3) en infraestructuras basadas en MIFARE Classic
- ▶ Migración flexible para garantizar la autenticación AES-128 y la mensajería a nivel de sector o de chip con la característica SL1SL3MixMode

Seguridad

- ▶ Protección a nivel bancario con la certificación Common Criteria EAL5+
- ▶ División de permisos de acceso entre SL1 y SL3 para restringir operaciones de actualización
- ▶ Prueba de transacción en línea y sin conexión con MAC de transacción generado por la tarjeta
- ▶ Comprobación de proximidad de la tarjeta inteligente para detectar ataques de transmisiones
- ▶ Temporizador de transacciones para combatir ataques intermediarios

APLICACIONES ESPECÍFICAS

- ▶ Transporte público
- ▶ Gestión de acceso
- ▶ Micropago de bucle cerrado
- ▶ Tarjetas de identificación de campus y estudiantes
- ▶ Programas de fidelidad
- ▶ Cobro electrónico de peaje
- ▶ Estacionamiento de vehículos

BENEFICIOS CLAVE

- ▶ Migración sencilla de infraestructuras existentes, con compatibilidad con los productos MIFARE Classic EV1 y MIFARE Plus
- ▶ Protección de nivel superior, con actualizaciones desde Crypto1 hasta seguridad AES de 128 bits
- ▶ Canal de comunicación integral seguro para servicios inalámbricos, como recarga de tarjetas inteligentes con el móvil e implementación de MIFARE 2GO (servicios móviles) en SL3



Como la siguiente generación de la gama de productos MIFARE Plus de NXP, MIFARE Plus EV2 IC ha sido diseñado para ser tanto una vía de acceso de las nuevas aplicaciones Smart City como una actualización convincente en términos de seguridad y conectividad de implementaciones existentes. El IC cuenta con capacidades de lectura más largas y tiempos de transacción más rápidos que su predecesor, de manera que los servicios sin contacto son más cómodos de usar y es compatible con los productos MIFARE Classic EV1 y MIFARE Plus. Así, ofrece una manera rentable de actualizar las características de seguridad in situ de las aplicaciones de tarjetas inteligentes, sin la necesidad de realizar grandes inversiones por adelantado en migraciones de lanzamiento.

COMPATIBILIDAD SÓLIDA CON INFRAESTRUCTURAS EXISTENTES

MIFARE Plus EV2 IC utiliza un concepto de nivel de seguridad (SL) innovador que ayuda a implementar paso a paso una seguridad superior en las infraestructuras existentes. El IC permite efectuar cambios de SL que abarcan desde baja seguridad (SL1) hasta alta seguridad (SL3), empleando la seguridad AES de 128 bits para la autenticación, la integridad y la protección de los datos. El cambio de SL puede aplicarse en el IC por completo o en sectores individuales. Una característica especial, llamada SL1SL3MixMode, permite habilitar la autenticación segura AES-128 en sectores basados en MIFARE Classic EV1. Esto permite, en combinación con las nuevas restricciones de actualización SL1, leer datos almacenados en un bloque con autenticación SL1, pero la actualización de datos solo funciona con la autenticación segura AES-128. La estructura basada en bloques de MIFARE Plus EV2 utiliza una tecnología de lógica compatible con la estructura basada en bloques de las aplicaciones Crypto1, de manera que las implementaciones basadas en Crypto1 puedan mantener su lógica estructural. Esto permite rutas de migración rentables, desde MIFARE Classic EV1 y Crypto1 tradicionales hasta seguridad AES de alto nivel de 128 bits. Dado que el IC es compatible con las infraestructuras nuevas y existentes, los usuarios finales pueden continuar utilizando la misma tarjeta inteligente mientras el sistema adopta una seguridad superior.

CONJUNTO DE CARACTERÍSTICAS EXPANDIDAS PARA SERVICIOS SIN CONTACTO DE SMART CITY

Las características especiales cumplen con la necesidad de contar con una seguridad y privacidad mejoradas en los servicios de Smart City. Por ejemplo, el MAC de transacción (TMAC) puede ayudar a garantizar la autenticidad de cada transacción para minimizar el fraude y el robo de identidad. Para ayudar a mitigar los ataques intermediarios, la nueva característica Temporizador de transacciones, que también está disponible en MIFARE DESFire EV3 IC de NXP, permite establecer un tiempo máximo por transacción para dificultar que un atacante pueda interferir con la transacción. La compatibilidad con tamaños de EEPROM de hasta 4 Kbytes ayuda a cumplir los requisitos de memoria cada vez más rigurosos de las aplicaciones de sistemas.

www.nxp.com

NXP, el logotipo de NXP, MIFARE, el logotipo de MIFARE, MIFARE Classic y MIFARE Plus son marcas comerciales registradas de NXP B.V. Todos los demás productos o nombres de servicios pertenecen a sus respectivos propietarios. © 2020 NXP B.V.

Fecha de lanzamiento: 23 de junio de 2020
Número de documento: MFPLUSV2LF REV0

COMPATIBILIDAD CON MÓVILES Y SERVICIOS INALÁMBRICOS

Con MIFARE Plus EV2, los servicios de Smart City, como la emisión móvil de billetes de transporte y el acceso móvil, pueden ejecutarse en teléfonos inteligentes y dispositivos portátiles compatibles con NFC. La utilización de MIFARE Plus EV2 en SL3 admite el uso del servicio de nube MIFARE 2GO de NXP, que administra las credenciales digitalizadas MIFARE basadas en productos y permite determinadas características, como pagos sin contacto y acceso móvil mediante dispositivos compatibles con NFC. A través del canal de comunicación integral seguro (SL1SL3MixMode) proporcionado por MIFARE Plus EV2, los operadores de sistemas pueden desarrollar fuentes de ingresos adicionales basadas en la introducción de servicios inalámbricos, como recargas móviles, incluso con aplicaciones Crypto1 tradicionales.

COMPARACIÓN DE CARACTERÍSTICAS: MIFARE Plus EV2 y MIFARE Plus X

Memoria	MIFARE Plus EV2	MIFARE Plus X
Configuración de la memoria	Estructura de bloque/sector	Estructura de bloque/sector
Tamaño de la memoria	2 kB / 4 kB	2 kB / 4 kB
Interfaz 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 o 4B ONUID	7B UID o 4B ONUID
Tasas de datos	Hasta 848 kbps, ISO/IEC 14443-4	Hasta 848 kbps, ISO/IEC 14443-4
Seguridad		
Algoritmo	AES 128 bits, mensajería segura, Crypto1 tradicional	AES 128 bits, mensajería segura, Crypto1 tradicional
Concepto de nivel de seguridad	Sector por sector o tarjeta	Solo tarjeta
SL1SL3MixMode	Acceso SL3 en sectores SL1	-
MAC de transacción (TMAC)	Validación segura de transacciones "back- end"	-
Temporizador de transacción	Mitigación de ataques intermediarios	-
Certificación Common Criteria	EAL5+ para HW y SW de IC	EAL4+ para HW y SW de IC

INFORMACIÓN DE PEDIDO

MIFARE Plus EV2	Formulario 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	Formulario 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

www.MIFARE.net