Hoja de datos del producto utilizado que evidencia el cumplimiento con la norma ISO/IEC 14443

TOPPAN SECURITY SAS

Familia SmartMX3 P71D320

Descripción general, fijación y características eléctricas

Rev. 3.0 — 15 de junio de 2017
295730

Ficha técnica breve del producto
EMPRESA PÚBLICA

1. Introducción

SmartMX3 P71D320 es un microprocesador seguro con capacidad de cifrado de interfaz dual. Forma parte de la familia de productos SmartMX de NXP. El dispositivo está construido sobre un núcleo RISC seguro, probado y potente. Estos productos son ideales para aplicaciones de pago y administración electrónica que requieren una solución económica pero también a prueba de manipulaciones, capaz de soportar los escenarios de ataques actuales y futuros.

El P71D320 ofrece la flexibilidad de la memoria Flash para códigos y datos. Al mismo tiempo, la ROM sigue estando disponible para los clientes que quieran utilizarla. Se mantiene el alto rendimiento sin contacto conocido por los microprocesadores seguros de NXP. La memoria es administrada por el firmware del dispositivo, lo que da como resultado una resistencia y retención muy sólidas a nivel de aplicación.

El cifrado de datos y códigos de extremo a extremo y la protección de la integridad garantizan que los datos del usuario y el código de la aplicación no puedan recuperarse del dispositivo ni corromperse durante la ejecución. Un mecanismo de copia seguro basado en hardware permite la ejecución segura y rápida de rutinas de software que se ocupan de la copia de datos.

Los coprocesadores criptográficos dedicados para criptografía simétrica y asimétrica ofrecen una eficiencia energética y una flexibilidad excepcionales. El motor DES/AES está protegido por contramedidas comprobadas matemáticamente. El coprocesador criptográfico asimétrico ofrece resistencia a DPA y ofrece algoritmos criptográficos asimétricos con una longitud de clave RSA flexible de hasta 4096 bits y hasta 544 bits para criptografía de curva elíptica.

La arquitectura de seguridad SmartMX3 P71 de NXP se basa en más de 15 años de experiencia. La plataforma proporciona un firmware integrado y una capa de abstracción de hardware que ofrece soluciones estándar para tareas rutinarias.

El producto SmartMX3 P71 admite la fácil implementación de sistemas operativos nativos en segmentos de mercado como banca, gobierno electrónico, tarjetas de identificación, tarjetas de salud, acceso seguro y módulos de plataforma confiable (TPM).

Tabla 1. Tabla de características

Tipo de producto	Usuario Flash [KB]	ROM de usuario [KB]	RAM [KB]	Coprocesador criptográfico asimétrico	Coprocesador criptográfico DES/AES	Opción de interfaz
P71D320	hasta 336	hasta 192	10	Sí	Sí	ISO/IEC 7816, ISO/IEC 14443
P71D240	256	hasta 108	10	Sí	Sí	

2. Descripción general

P71D320 es un microprocesador seguro para aplicaciones similares a las tarjetas inteligentes. Representa la novena generación de microprocesadores seguros de NXP Semiconductors y constituye la esencia de más de quince años de experiencia, pero también de muchos cientos de años de investigación y desarrollo dedicados a la excelencia en la arquitectura y el diseño de chips.

Con su concepto FlexMem, P71D320 ofrece características de flexibilidad únicas en términos de uso de memoria y soporte para la gestión del ciclo de vida de producción. Cada elemento de código se puede colocar en la ROM para una ejecución de máxima velocidad y con el menor consumo de energía, o se puede cargar en Flash para lograr flexibilidad y posibilidad de actualización.

El software integrado proporcionado por NXP que viene con P71D320 proporciona bibliotecas de SO compartidas de NXP, lo que hace que el diseño del sistema operativo sea más eficaz. Un concepto innovador de firewall administra los derechos entre instancias de software independientes de una manera novedosa y mucho más flexible que la conocida hasta ahora. Se pueden ejecutar dos instancias de software de forma independiente. El firewall P71D320 garantiza que una no pueda comprometer la seguridad de la otra.

Se ofrece una biblioteca criptográfica modular para P71D320 que proporciona funciones criptográficas probadas y con certificación de seguridad para los desarrolladores de sistemas operativos.

El P71D320 comparte el mismo núcleo de CPU y la misma arquitectura básica que se utilizan en los productos SmartMX2 P40 de NXP. Sin embargo, las capacidades y el rendimiento del sistema se han mejorado considerablemente.

El conjunto de herramientas de desarrollo para P71D320 se basa en un entorno de desarrollo integrado bien establecido. Hay disponible un dispositivo de enmascaramiento suave con capacidades de depuración para el desarrollo en el sistema y la verificación de código.

3. Características y beneficios

3.1 Características específicas del producto

Microprocesador seguro de interfaz dual de alto rendimiento

- CPU RISC (computación con conjunto de instrucciones reducido) MRK3-SC de 16/32 bits para alta Rendimiento de transacciones, bajo consumo de energía y nivel de seguridad de clase mundial
- La firma de código garantiza la integridad de la ejecución de las instrucciones.

Motores de criptografía de alto nivel con soporte de "longitud de clave completa"

- Unidad funcional de criptografía dedicada para algoritmos DES y AES simétricos
- Clave de longitud de 56 bits DES, 2DES de 112 bits, triple DES de 168 bits (TDES o 3DES), en varias configuraciones
- AES con longitud de clave de 128, 192 y 256 bits
- Unidad aceleradora de criptografía asimétrica, compatible con RSA, ECC y relacionados algoritmos
- Criptografía RSA con longitud de clave arbitraria de hasta 4096 bits
- Criptografía de curva elíptica (ECC) con una longitud de clave de hasta 571 bits

Generador de números aleatorios verdaderos, compatible con AIS31

Generador de números aleatorios deterministas para una ejecución más rápida en casos donde los valores son inferiores.

La entropía del RNG es suficiente

Unidad funcional de verificación de redundancia cíclica (CRC) para operaciones de 16 y 32 bits

Gran memoria para flexibilidad en el diseño del sistema operativo:

- Memoria de solo lectura (ROM) para el almacenamiento de elementos de código fijo o para un rendimiento máximo con un suministro de energía mínimo; ROM de 0...192 K disponible para uso del cliente, según la configuración lógica y las opciones seleccionadas
- Memoria Flash para máxima flexibilidad; partes menores de esta memoria pueden reservarse para NXP, según la configuración lógica y las opciones seleccionadas; hasta 336 K Flash están disponibles para uso del cliente, según la configuración lógica y las opciones seleccionadas

10 K de RAM

Enfoque NXP FlexMem:

- Área de direccionamiento de memoria lógica única y contigua en ROM y Flash recuerdos
- Flexibilidad para cargar código y datos en ROM o Flash según sea necesario (ROM: ejecución más rápida; Flash: carga de posproducción, actualización)
- Flexibilidad total para particionar la memoria Flash entre código y datos de personalización

Cargador de arranque seguro para carga inicial o actualizaciones de memoria Flash; adecuado para uso en Tanto en sitios de fabricación seguros como en entornos generales. Existen varias opciones de configuración para gestionar y delegar derechos de acceso y escritura.

Tecnología de firewall vertical

- Separación total de instancias de SW, no se requiere confianza entre instancias de SW, es decir, el software no confiable no puede comprometer el software con certificación de seguridad
- Mecanismo de intercambio/entrega con certificación de seguridad para administrar recursos de HW entre instancias de SW

Soporte de interfaz dual con amplio rango de configuración

- Interfaz de contacto ISO/IEC 7816; velocidades de datos estándar hasta TA1 = 97 h
- Interfaz sin contacto ISO/IEC 14443

Interfaz tipo A para velocidades de datos de hasta 848 kbit/s, configuraciones de velocidad de datos simétrica y asimétrica

Compatibilidad con configuración de interfaz sin contacto con tasa de bits muy alta (VHBR) para minimizar el tiempo de transacción (3,4 Mbit/s en la dirección del chip al lector)

Amplia gama de opciones de embalaje con certificación de seguridad disponibles directamente desde NXP - Módulos de chip de contacto, de interfaz dual y sin contacto, varias opciones de suministro de obleas

Función físicamente no clonable basada en hardware (PUF) disponible para configuración a través del firmware NXP

3.2 Características de seguridad

La tecnología CMOS de 90 nm ofrece una fuerte protección inherente contra ataques invasivos a la lógica y las memorias.

El concepto NXP Glue Logic descorrelaciona eficazmente la función y la ubicación de los circuitos en el dispositivo: no se reconocen bloques funcionales en ninguna capa física del dispositivo, lo que agrega otro nivel de protección contra ataques invasivos activos y pasivos.

No se utilizan bloques macro lógicos; toda la lógica en el dispositivo, incluida la CPU, Los coprocesadores y todas las demás funciones se sintetizan en una única área lógica.

NXP PUF (función físicamente no clonable) para protección adicional de secretos estáticos contra incluso los ataques de ingeniería inversa más sofisticados

4. Aplicaciones

Pasaportes electrónicos (ePP) y permisos de residencia (eRP)

documentos nacionales de identidad

Tarjetas sanitarias

Banca de contacto y doble interfaz

Licencias de conducir electrónicas

Tarjetas de firma digital

Gestión de acceso de alta seguridad

Autenticación de máquina a máquina

Módulos de plataforma confiables

Tarjetas multiaplicación

5. Datos de referencia rápida

Tabla 1. Datos de referencia rápida

Símbolo	Parámetro	Condiciones	Mínimo	Tipo	Máximo	Unidad
VDD	Tensión de alimentación[1]	Clase A: rango de 5 V	4.5	5.0	5.5	V
		Clase B: rango de 3 V	2.7	3.0	3.3	V
		Clase C: rango de 1,8 V	1.62	1.8	1,98	V
yo	Intensidad del campo	Operación de interfaz sin contacto	1.5		7.5	Soy
Tambor	Temperatura ambiente de funcionamiento[2]		-25		+85	°C

[1] Observación: Se admite funcionamiento continuo desde 1,62 V hasta 5,5 V.

[2] Todas las propiedades y valores del producto especificados en esta hoja de datos solo son válidos dentro del rango de temperatura ambiente de funcionamiento.

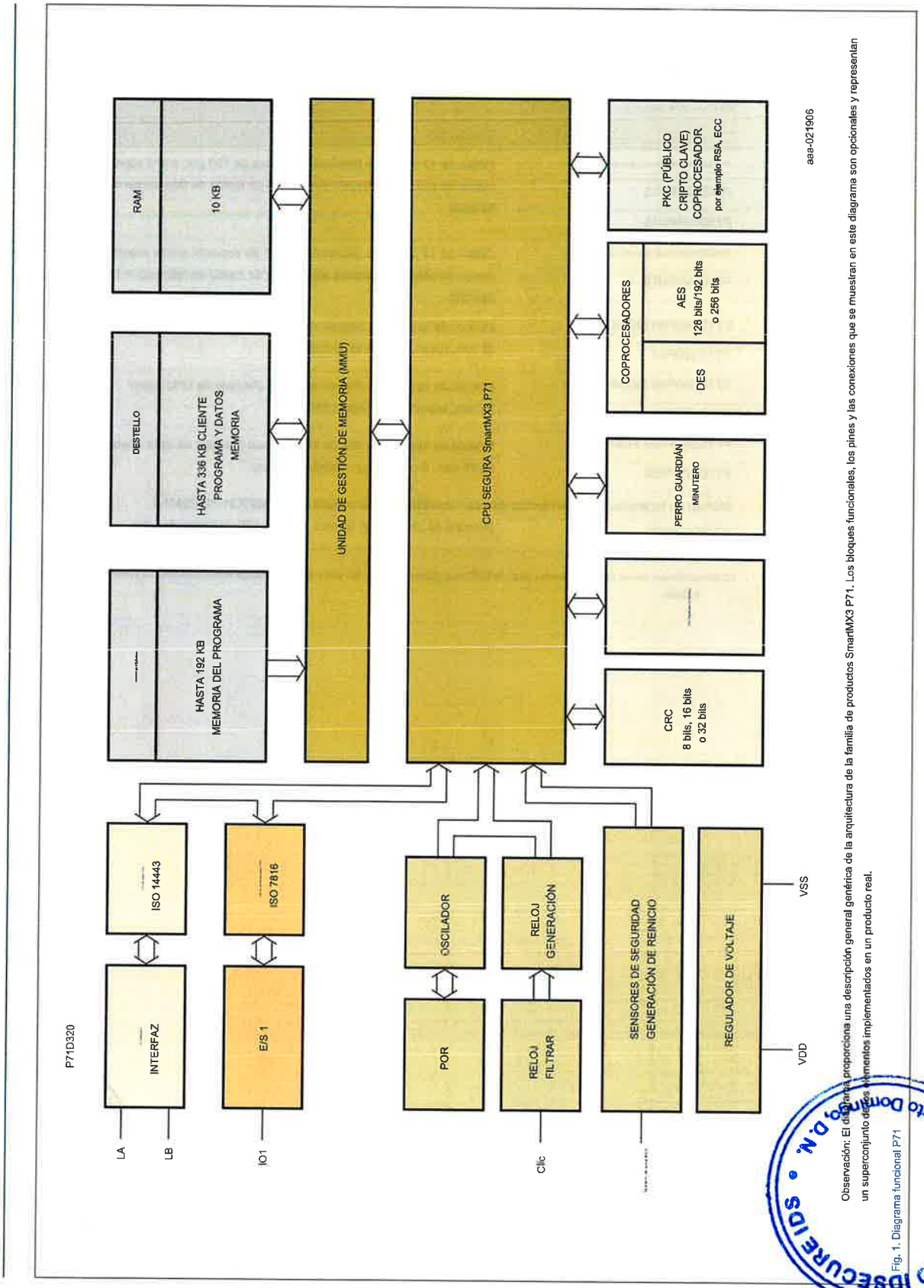
6. Información para pedidos

Tabla 2. Información para pedidos

Número de tipo [1]	Paquete		
—	Nombre	Descripción	Versión
P71D240PU15 Módulo de fuente de alimentación P71D320PU15 P70D144PU15		Oblea de 12 pulgadas (aserrada; espesor de 150 µm; sobre soporte de marco de película; marcado electrónico de matriz de falla según formato SECSII)	NAU000
P71D240PU75 Módulo de fuente de alimentación P71D320PU75		Oblea de 12 pulgadas (aserrada; 75 µm de espesor; sobre soporte de marco de película; marcado electrónico de matriz de falla según formato SECSII)	NAU000
P71D240PA4 MOB4 P71D320PA4		Módulo de tarjeta con chip sin contacto (formato de cinta super 35 mm, espesor del módulo 320 µm)	SOT500-2
P71D240PA6 MOB6 P71D320PA6		Módulo de tarjeta con chip sin contacto (formato de cinta super 35 mm, espesor del módulo 250 µm)	SOT500-3
P71D240PX30 PDM1.1 P71D320PX30		Módulo de tarjeta con chip de interfaz dual (formato de cinta súper de 35 mm, 8 contactos); múltiples fuentes	SOT658-3
Módulo de tarjeta con chip de interfaz dual con revestimiento de paladio P71D240PX31 Pd-PDM1.1 P71D320PX31		(formato de cinta super 35 mm, 8 contactos); múltiples fuentes	SOT658-3

[1] Comuníquese con su oficina de ventas local de NXP para obtener información sobre tipos de entrega adicionales y su lanzamiento y certificación relacionada. estado.

QM



Observación: El diagrama proporciona una descripción general genérica de la arquitectura de la familia de productos SmartMX3 P71. Los bloques funcionales, los pines y las conexiones que se muestran en este diagrama son opcionales y representan un superconjunto de los elementos implementados en un producto real.

Fig. 1. Diagrama funcional P71

7. Diagrama funcional

8. Historial de revisiones

Tabla 3. Historial de revisiones

Identificación del documento	Fecha de lanzamiento	Estado de la hoja de datos	Aviso de cambio	Reemplaza
295730	15 de junio de 2017	Ficha técnica breve del producto	-	295711
	• Actualización general			
295711	25 de enero de 2017	Ficha técnica breve y objetiva -		-
	• Actualización general			
295710	27 de marzo de 2016	Ficha técnica breve y objetiva -		-
	• Versión inicial			

PH

9. Información legal

9.1 Estado de la hoja de datos

Estado del documento [1][2]	Estado del producto[3]	Definición
Hoja de datos objetiva [breve]	Desarrollo	Este documento contiene datos de la especificación objetiva para el desarrollo del producto.
Hoja de datos preliminar [breve]	Calificación	Este documento contiene datos de la especificación preliminar.
Hoja de datos del producto [breve]	Producción	Este documento contiene la especificación del producto.

[1] Consulte el documento emitido más recientemente antes de iniciar o completar un diseño.

[2] El término "hoja de datos breve" se explica en la sección "Definiciones".

[3] El estado del producto de los dispositivos descritos en este documento puede haber cambiado desde que se publicó este documento y puede diferir en el caso de varios dispositivos. El estado más reciente del producto La información está disponible en Internet en la URL http://www.nxp.com.

9.2 Definiciones

Borrador: el documento es solo una versión preliminar. El contenido aún se encuentra bajo revisión interna y sujeto a aprobación formal, lo que puede dar lugar a modificaciones o adiciones. NXP Semiconductors no ofrece declaraciones ni garantías en cuanto a la precisión o integridad de la información incluida en este documento y no será responsable de las consecuencias del uso de dicha información.

Ficha técnica breve: una ficha técnica breve es un extracto de una ficha técnica completa con el mismo número de tipo de producto y título. Una ficha técnica breve está destinada únicamente a una referencia rápida y no debe confiarse en que contenga información detallada y completa. Para obtener información detallada y completa, consulte la ficha técnica completa correspondiente, que está disponible a pedido a través de la oficina de ventas local de NXP Semiconductors. En caso de cualquier inconsistencia o conflicto con la ficha técnica breve, prevalecerá la ficha técnica completa.

Especificación del producto: la información y los datos proporcionados en una hoja de datos del producto definirán la especificación del producto acordada entre NXP Semiconductors y su cliente, a menos que NXP Semiconductors y el cliente hayan acordado explícitamente lo contrario por escrito. Sin embargo, en ningún caso será válido un acuerdo en el que se considere que el producto de NXP Semiconductors ofrece funciones y cualidades que van más allá de las descritas en la hoja de datos del producto.

9.3 Descargo de responsabilidad

Garantía y responsabilidad limitadas: se considera que la información contenida en este documento es precisa y confiable. Sin embargo, NXP Semiconductors no ofrece declaraciones ni garantías, expresas o implícitas, sobre la precisión o integridad de dicha información y no será responsable de las consecuencias del uso de dicha información. NXP Semiconductors no asume ninguna responsabilidad por el contenido de este documento si lo proporciona una fuente de información ajena a NXP Semiconductors.

En ningún caso NXP Semiconductors será responsable de ningún daño indirecto, incidental, punitivo, especial o consecuente (incluidos, sin limitación, pérdida de ganancias, pérdida de ahorros, interrupción del negocio, costos relacionados con la eliminación o reemplazo de cualquier producto o cargos por reelaboración) ya sea que dichos daños se basen o no en agravio (incluida negligencia), garantía, incumplimiento de contrato o cualquier otra teoría legal.

Sin perjuicio de los daños que el cliente pueda sufrir por cualquier motivo, la responsabilidad agregada y acumulativa de NXP Semiconductors hacia el cliente por los productos aquí descritos estará limitada de acuerdo con los Términos y condiciones de venta comercial de NXP Semiconductors.

Derecho a realizar cambios: NXP Semiconductors se reserva el derecho a realizar cambios en la información publicada en este documento, incluidas, entre otras, las especificaciones y descripciones de productos, en cualquier momento y sin previo aviso. Este documento reemplaza toda la información proporcionada antes de su publicación.

Idoneidad para el uso: los productos de NXP Semiconductors no están diseñados, autorizados ni garantizados para su uso en sistemas o equipos de soporte vital, críticos para la vida o la seguridad, ni en aplicaciones en las que se pueda esperar razonablemente que una falla o mal funcionamiento de un producto de NXP Semiconductors resulte en lesiones personales, muerte o daños graves a la propiedad o al medio ambiente. NXP Semiconductors y sus proveedores no aceptan ninguna responsabilidad por la inclusión y/o el uso de productos de NXP Semiconductors en dichos equipos o aplicaciones y, por lo tanto, dicha inclusión y/o uso es por cuenta y riesgo del cliente.

Aplicaciones: Las aplicaciones que se describen en este documento para cualquiera de estos productos se ofrecen únicamente con fines ilustrativos. NXP Semiconductors no realiza declaraciones ni garantiza que dichas aplicaciones sean adecuadas para el uso especificado sin realizar más pruebas o modificaciones.

Los clientes son responsables del diseño y el funcionamiento de sus aplicaciones y productos utilizando productos de NXP Semiconductors, y NXP Semiconductors no acepta ninguna responsabilidad por cualquier asistencia con las aplicaciones o el diseño de productos del cliente. Es responsabilidad exclusiva del cliente determinar si el producto de NXP Semiconductors es adecuado y apto para las aplicaciones y productos planificados del cliente, así como para la aplicación y el uso planificados de los clientes externos del cliente. Los clientes deben proporcionar las salvaguardas adecuadas de diseño y funcionamiento para minimizar los riesgos asociados con sus aplicaciones y productos.

NXP Semiconductors no acepta ninguna responsabilidad relacionada con cualquier defecto, daño, costo o problema que se base en cualquier debilidad o defecto en las aplicaciones o productos del cliente, o la aplicación o uso por parte de terceros clientes del cliente. El cliente es responsable de realizar todas las pruebas necesarias para las aplicaciones y productos del cliente utilizando productos de NXP Semiconductors con el fin de evitar un defecto de las aplicaciones y productos o de la aplicación o uso por parte de terceros clientes del cliente. NXP no acepta ninguna responsabilidad a este respecto.

Valores límite: la tensión por encima de uno o más valores límite (según se define en el Sistema de valores máximos absolutos de IEC 60134) provocará daños permanentes al dispositivo. Los valores límite son solo valores de tensión y no se garantiza el funcionamiento (adecuado) del dispositivo en estas o en cualquier otra condición por encima de las que se indican en la sección Condiciones de funcionamiento recomendadas (si las hay) o en las secciones Características de este documento.

La exposición repetida a valores límite afectará de forma permanente e irreversible la calidad y fiabilidad del dispositivo.

Términos y condiciones de venta comercial — NXP Semiconductors

Los productos se venden sujetos a los términos y condiciones generales de venta comercial, publicados en http://www.nxp.com/profile/terms, A menos que se haya acordado lo contrario en un contrato individual válido por escrito. En caso de que se celebre un contrato individual, solo se aplicarán los términos y condiciones del contrato respectivo. NXP Semiconductors se opone expresamente a la aplicación de los términos y condiciones generales del cliente en relación con la compra de productos de NXP Semiconductors por parte del cliente.

Ninguna oferta de venta o licencia: nada en este documento puede interpretarse o entenderse como una oferta de venta de productos abierta a la aceptación o la concesión, transferencia o implicación de cualquier licencia bajo cualquier derecho de autor, patente u otros derechos de propiedad industrial o intelectual.

Clasificación de exportación controlada (1) — El contenido de este documento está sujeto a controles de exportación. La exportación o el suministro a las partes incluidas en la lista requiere una autorización previa de las autoridades competentes. El número de clasificación de control de exportación (ECCN) es 5E002.

Datos de referencia rápida: Los datos de referencia rápida son un extracto de los datos del producto proporcionados en las secciones Valores límite y Características de este documento y, como tales, no son completos, exhaustivos ni legalmente vinculantes.

Productos no aptos para uso en la industria automotriz: a menos que esta hoja de datos indique expresamente que este producto específico de NXP Semiconductors está apto para uso en la industria automotriz, el producto no es apto para uso en la industria automotriz. No está apto ni probado de acuerdo con los requisitos de aplicación o pruebas de la industria automotriz. NXP Semiconductors no acepta ninguna responsabilidad por la inclusión o el uso de productos no aptos para uso en la industria automotriz en equipos o aplicaciones automotrices.

En el caso de que el cliente utilice el producto para diseño y uso en aplicaciones automotrices según especificaciones y estándares automotrices, el cliente (a) deberá utilizar el producto sin la garantía de NXP Semiconductors del producto para dichas aplicaciones, uso y especificaciones automotrices, y (b) siempre que el cliente utilice el producto para aplicaciones automotrices más allá de las especificaciones de NXP Semiconductors, dicho uso será únicamente por cuenta y riesgo del cliente, y (c) el cliente indemnizará completamente a NXP Semiconductors por cualquier responsabilidad, daños o reclamos por productos defectuosos que resulten del diseño y uso del producto por parte del cliente para aplicaciones automotrices más allá de la garantía estándar de NXP Semiconductors y las especificaciones del producto de NXP Semiconductors.

Traducciones: La versión de un documento que no esté en inglés (traducida) es solo para referencia. La versión en inglés prevalecerá en caso de discrepancia entre la versión traducida y la versión en inglés.

9.4 Licencias

Circuitos integrados con funcionalidad de contramedidas DPA

Los circuitos integrados NXP que contienen funciones que implementan contramedidas para el análisis de potencia diferencial y el análisis de potencia simple se producen y venden bajo la licencia correspondiente de Cryptography Research, Inc.

Circuitos integrados con funcionalidad de contramedidas DPA

Los circuitos integrados NXP que contienen funciones que implementan contramedidas para el análisis de potencia diferencial y el análisis de potencia simple se producen y venden bajo la licencia correspondiente de Cryptography Research, Inc.

9.5 Marcas comerciales

Aviso: Todas las marcas, nombres de productos, nombres de servicios y marcas comerciales a las que se hace referencia son propiedad de sus respectivos dueños.

DESFire es una marca comercial de NXP Semiconductors NV

FabKey es una marca registrada de NXP Semiconductors NV

MIFARE — es una marca comercial de NXP Semiconductors NV

MIFARE FleX es una marca comercial de NXP Semiconductors NV

MIFARE Plus es una marca comercial de NXP Semiconductors NV

SmartMX es una marca comercial de NXP Semiconductors NV

10. Información de contacto

Para obtener más información, visite: http://www.nxp.com

Para obtener direcciones de oficinas de ventas, envíe un correo electrónico a: salesaddresses@nxp.com

11. Tablas

PM

12. Figuras

13. Contenido

Para obtener más información, visite: http://www.nxp.com
Para obtener direcciones de oficinas de ventas, envíe un correo electrónico a: salesaddresses@nxp.com

Fecha de lanzamiento: 15 de junio de 2017
Identificador del documento: 295730