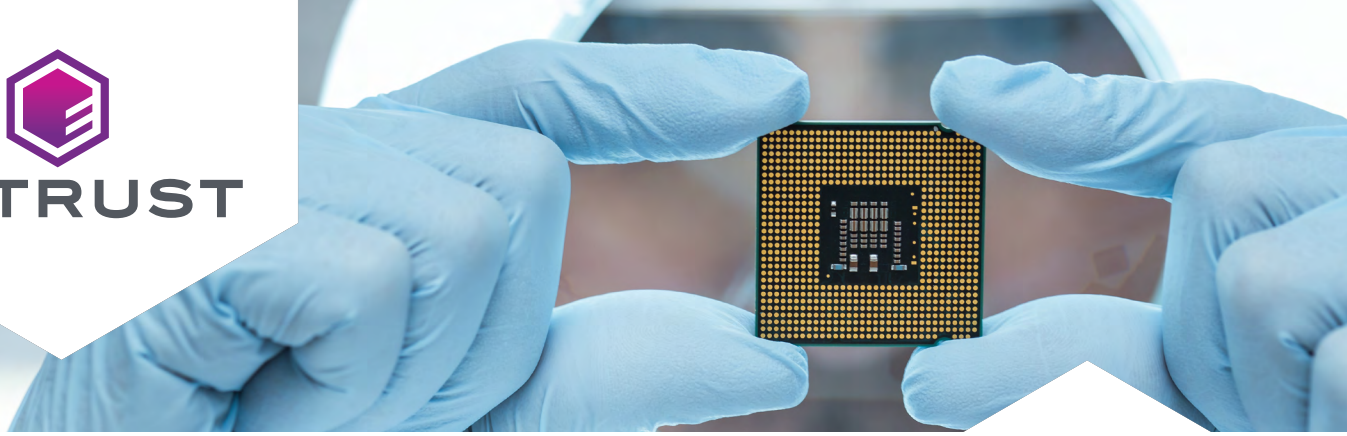

Entrust aprovisiona la identidad raíz para los microcontroladores SAM L11 preparados para el IoT de Microchip

El Internet de las cosas (IoT) se ha convertido en un fenómeno imparable. Aunque muchas personas lo consideran un número muy conservador, IDC predice que el número total de dispositivos IoT conectados superará los 40 mil millones para 2025.

No obstante, la explosiva proliferación de puntos finales relacionados con el IoT, que van desde vehículos autónomos hasta electrodomésticos inteligentes, y de equipos de atención médica hasta maquinaria agrícola, no está exenta de desafíos. Entre los más críticos se encuentra el tema de la seguridad: garantizar que todos los dispositivos se encuentren protegidos contra riesgos.

NECESIDADES DEL NEGOCIO

Anand Rangarajan, gerente de marketing de productos de Microchip Technology, explicó: “El universo de IoT actualmente no cuenta con estándares de seguridad generalizados. La enorme complejidad que resulta de incorporar medidas de seguridad adecuadas en sus productos se convierte en una propuesta abrumadora para muchos fabricantes”.

> **“La integración de la seguridad de nivel industrial en un sistema integrado es un verdadero cambio de juego para todo el mercado de IoT.”**
>
> – Anand Rangarajan, gerente de marketing de productos para Microchip Technology

APRENDA MÁS EN ENTRUST.COM/HSM

Microchip

Reconocido por su innovación continua y productos que sientan precedentes, Microchip Technology, Inc. es uno de los principales proveedores mundiales de soluciones de microcontroladores, señales mixtas, analógicas y flash-IP. Uno de los microcontroladores más recientes de la compañía, el SAM L11, galardonado con el Premio a la Innovación 2018 a la Mejor Contribución a la Seguridad de IoT en ARM Techcon, aborda específicamente las características, la funcionalidad y las necesidades de seguridad de los nodos de IoT y los terminales inteligentes, tales como dispositivos médicos, sensores y cámaras y coches.

Microchip, con sede en Chandler, Arizona, cotiza en la bolsa Nasdaq. La compañía ha enviado miles de millones de microcontroladores y microprocesadores a cientos de miles de clientes en todo el mundo.

NECESIDADES TECNOLÓGICAS

"Desde la perspectiva del microcontrolador, el tipo de caso de uso que anticipamos para el SAM L11 dicta algunas características de diseño muy exclusivas, entre ellas la necesidad de alto rendimiento, pero bajo consumo de energía", describió Rangarajan.

SOLUCIÓN

En el corazón de la arquitectura de seguridad del SAM L11 se encuentra una función de raíz de confianza creada por Microchip para permitir que se inserte una clave exclusiva del dispositivo durante la fabricación. La elección de la tecnología para gestionar y ejecutar la tarea crítica resultó ser muy sencilla. "Hemos tenido una relación de larga data con Entrust (anteriormente nCipher) y seleccionar su módulo de seguridad de hardware (HSM) para generar las claves individuales fue una decisión clara para nosotros", señaló Rangarajan.

EL HSM nShield® de Entrust es un dispositivo de seguridad de hardware certificado que ejecuta funciones críticas de cifrado, firma digital y generación de claves. La plataforma en red reforzada es altamente escalable y utiliza una arquitectura flexible única que es capaz de tasas de transacciones criptográficas líderes en la industria.

RESULTADOS

"Tener la capacidad de insertar una clave única del HSM nShield en cada microcontrolador SAM L11 permite que los dispositivos se identifiquen, verifiquen y administren individualmente de forma remota. Esto es particularmente importante cuando es necesario restablecer la confianza entre los dispositivos de IoT y otros puntos finales conectados", observó Rangarajan. "Los fabricantes ahora pueden aprovechar al máximo la nube para proporcionar una conectividad segura y generalizada entre cada nodo. Es ideal para aplicaciones tales como la protección de sensores inalámbricos , el cifrado de datos de dispositivos médicos portátiles e incluso la autenticación remota de sistemas conectados a la nube".

Parte de la atractiva propuesta de valor del microcontrolador Microchip SAM L11 es el resultado de la asociación de la empresa con Trustonic, líder en el mercado de seguridad de dispositivos con más de 1.500 millones de unidades protegidas desplegadas en todo el mundo.

Uno de los mayores avances ha sido la creación, por parte de Trustonic, de una biblioteca de funciones de seguridad, que incluye autenticación, arranque seguro, detección de manipulaciones, cifrado AES y SHA y almacenamiento seguro de claves, que se incorpora a un kit de desarrollo de software.

Microchip

> **Seleccionar el HSM nShield de Entrust para generar las claves individuales fue una decisión clara para nosotros.**
>
> – Anand Rangarajan, gerente de marketing de productos para Microchip Technology

"Los diseñadores ahora pueden usar el marco de seguridad modular para realizar llamadas API simples para acceder al muy sofisticado conjunto de capacidades de seguridad que hemos construido", comentó Rangarajan. "Ya no se requiere una gran experiencia con protocolos a nivel de chip. Esto acelera enormemente los plazos de desarrollo y reduce drásticamente la sobrecarga asociada tradicionalmente con la seguridad de un dispositivo de IoT".

La biblioteca de módulos de seguridad se basa en Kinibi-M, un entorno operativo modular, seguro por hardware, diseñado a medida por Trustonic para chipsets de IoT de tamaño limitado. Debajo de Kinibi-M, una capa de abstracción de hardware facilita la comunicación directa con el SAM L11, incluida la gestión del uso de la clave cifrada generada por nShield de Entrust.

"Los desarrolladores de Microchip del SAM L11 hicieron su propia diligencia debida para determinar que el HSM nShield de Entrust era la opción óptima para nosotros, pero por separado, Trustonic también recomendó que deberíamos utilizar el HSM Entrust. Fue muy valioso obtener un respaldo completamente independiente de nuestra decisión", recordó Rangarajan.

SIMPLIFICAR LA SEGURIDAD CON EL CHIP QUE CAMBIA EL JUEGO

El SAM L11 es el primer microcontrolador de la industria que utiliza el procesador Arm Cortex-M23 y la tecnología de seguridad integrada Arm TrustZone, lo que proporciona aislamiento reforzado por hardware entre recursos confiables y no confiables. Rangarajan reflexionó: "A pesar de la sofisticación y las capacidades integrales de la arquitectura de seguridad, el uso de Kinibi-M aún simplifica el desarrollo de aplicaciones seguras con un firmware que está completamente integrado con las funciones de seguridad de SAM L11. Además, ofrece ejemplos de código para abordar los casos de uso relevantes de IoT que podrían beneficiarse desde un dispositivo como SAM L11".

La capacidad de proporcionarles a los desarrolladores de dispositivos de IoT una base de raíz de confianza de clase mundial mediante la utilización de claves generadas por un HSM nShield® de Entrust, está en causar un impacto global significativo. Rangarajan declaró: "El enfoque que hemos adoptado significa que ahora podemos incorporar seguridad en un paquete de alto rendimiento que tiene un consumo de energía extremadamente bajo. La integración de la seguridad de nivel industrial en un sistema integrado es un verdadero cambio de juego para todo el mercado de IoT".

Microchip

TRANSFORMAR LA SEGURIDAD EN TODO EL IoT

Necesidades del negocio

- Crear una solución para proteger los nodos y los puntos finales de IoT
- Reducir la complejidad y el costo de incorporar seguridad en los dispositivos de IoT
- Elimina la necesidad de habilidades de programación especializadas a nivel de chip

Necesidades tecnológicas

- Integrar características de seguridad sólidas en un microcontrolador rápido y de bajo consumo
- Diseñar una huella pequeña para permitir su uso con aplicaciones de memoria intensiva
- Establecer una raíz de confianza

Solución

- HSM nShield de Entrust

Resultado

- Lanzamiento del microcontrolador SAM L11 con características y rendimiento líderes en la industria
- El kit de desarrollo de software ofrece acceso API simple a funciones de seguridad sofisticadas
- Reducción del tiempo de comercialización para los fabricantes de dispositivos IoT
- Habilita la confianza para los dispositivos de IoT y los datos que producen

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com