Microsoft y Entrust ofrecen seguridad y confianza mejoradas para el Internet de las Cosas

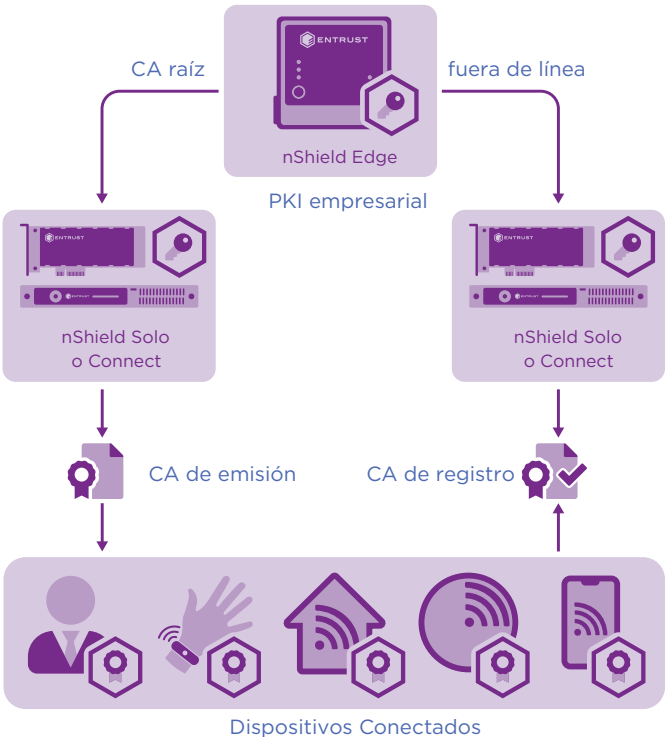
Los servicios de inscripción de dispositivos y los módulos de seguridad de hardware permiten el registro seguro de dispositivos del IoT

CARACTERÍSTICAS PRINCIPALES

- Aumente la integridad de los certificados de dispositivos de red
- Habilite el uso de la PKI existente para admitir el registro de dispositivos
- Ofrezca almacenamiento y administración de claves seguros
- Proporcione protección de claves con validación FIPS 140-2 nivel 3
- Facilite la auditoría y el cumplimiento de las normas de seguridad de datos

El problema: el creciente número de dispositivos de red conectados al Internet que utilizan certificados digitales para identificación y autenticación también deben admitir la inscripción de certificados

A medida que hay más dispositivos conectados al Internet y a redes empresariales, su identificación y autenticación son de vital importancia. Los dispositivos no autorizados pueden crear vectores para la introducción de malware en dominios cerrados, lo que supone riesgos importantes. Si bien las infraestructuras de



Los HSMs nShield de Entrust no solo protegen la raíz PKI empresarial y las claves de la CA emisora, sino también las claves privadas que se utilizan para vincular los certificados de dispositivo a la raíz de confianza de la CA para la integridad y validación del certificado.

APRENDA MÁS EN ENTRUST.COM/HSM

Microsoft y Entrust ofrecen seguridad y confianza mejoradas para el Internet de las cosas

clave pública (PKI) se utilizan para emitir y administrar las credenciales del dispositivo para la identificación y autenticación, también debe existir un proceso de registro confiable.

El desafío: permitir que un número creciente de dispositivos conectados registren certificados de forma segura utilizando credenciales confiables basadas en dominios

La emisión de certificados de dispositivo es solo el primer paso para establecer un entorno de red seguro donde un número creciente de dispositivos autorizados se conectan a dominios restringidos. Es necesario inscribir estos certificados de una autoridad de certificación (CA) para validar y controlar las conexiones de los dispositivos. Proteger y administrar las claves criptográficas que sustentan el proceso de registro es vital para proporcionar una base de confianza para todo el sistema.

La solución: usar Microsoft y Entrust juntos puede permitir la inscripción segura de certificados de dispositivos conectados

Al ser una de las instalaciones de Microsoft Active Directory Certificate Services (AD CS), Network Device Enrollment Service (NDES) implementa el Simple Certificate Enrollment Protocol (SCEP) para definir la comunicación entre los dispositivos conectados y una autoridad de registro (RA) para la inscripción de certificados. Las soluciones locales y basadas en la nube, tales como Microsoft Intune y System Configuration Manager, usan NDES para aprovisionar e inscribir dispositivos. NDES permite la inscripción y validación de identidades digitales de dispositivos conectados a servidores Windows vinculándolos a una clave privada correspondiente. Utilizando una CA como raíz de confianza, el servicio permite la inscripción de certificados y la validación de su autenticidad e integridad.

Cuando el proceso de emisión se ejecuta en un servidor utilizando una clave almacenada localmente en un archivo, la clave puede estar sujeta a ataques que la hacen vulnerable a la duplicación, modificación y sustitución. Los módulos de seguridad de hardware (HSMs) nShield de Entrust aumentan el nivel de seguridad del proceso de inscripción de certificados al proteger la clave NDES privada. Los HSMs nShield® de Entrust se integran con Microsoft NDES mediante las interfaces de programación de aplicaciones criptográficas (CAPI) estándar de Microsoft.

¿Por qué utilizar HSMs de Entrust con Microsoft NDES?

A medida que se implementan más dispositivos conectados para respaldar el creciente Internet de las cosas (IoT), se espera que las PKIs no solo protejan la clave privada de la CA raíz que respalda la seguridad de los certificados emitidos en todo el dominio, sino también el registro de este número creciente de certificados. Las PKIs organizativas que no utilizan HSMs para proteger sus claves privadas y que no emplear mecanismos para inscribir y validar certificados, las dejan vulnerables a interrupciones con posibles consecuencias graves. Los HSMs proporcionan un entorno reforzado que protege las claves críticas para la seguridad contra el robo y el uso indebido, y permite la administración de su ciclo de vida completo con soporte de conmutación por error donde se utilizan múltiples HSMs para alta disponibilidad. Vincular la emisión de certificados a las verificaciones y aprobaciones de identidad mediante HSMs nShield de Entrust, y controlar la inscripción y validación de certificados, han sido lecciones importantes aprendidas de los compromisos de seguridad de CA.

Microsoft y Entrust ofrecen seguridad y confianza mejoradas para el Internet de las cosas

Los HSMs nShield de Entrust certificados según estrictos estándares de seguridad, incluidos FIPS 140-2 Nivel 3:

- Almacenan la CA raíz y las claves de inscripción en un entorno seguro y resistente a manipulaciones indebidas
- Gestionan el acceso de administradores con una política basada en tarjetas inteligentes y autenticación de dos factores
- Cumplen con los requisitos normativos del sector público, los servicios financieros y las empresas

HSMs de Entrust

Los HSMs nShield de Entrust han admitido a AD CS desde su lanzamiento de Windows Server 2003 y se han implementado en una amplia base global de clientes. El soporte de NDES es una extensión de este servicio. Al simplificar la administración de credenciales en múltiples aplicaciones y PKI, pueden operar en entornos virtualizados, incluido Hyper-V. Los HSMs nShield de Entrust ayudan a las organizaciones a cumplir con los requisitos en materia de auditoría y cumplimiento, como el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) y se encuentran disponibles en las siguientes variantes:

- nShield Edge: HSM portátil con conexión USB para CA raíz fuera de línea
- nShield Solo+ / Solo XC: HSM PCI Express de alto rendimiento integrado para servidores
- nShield Connect / Connect XC: HSM de alto rendimiento conectado a la red para centros de datos

Microsoft

Microsoft ha transformado la forma como se comparten los recursos empresariales y cómo se administran las identidades y los controles de acceso. Los sistemas basados en Microsoft AD CS y NDES brindan servicios personalizados para crear y administrar certificados de clave pública para establecer entornos comerciales confiables entre personas y dispositivos. Microsoft NDES:

- Provee y registra certificados de dispositivo con RA
- Asegura la inscripción con credenciales basadas en dominio
- Habilita el servicio de validación y revocación de certificados

www.microsoft.com

Más información

Para saber más sobre los HSMs nShield de Entrust visite **entrust.com/HSM**. Para conocer más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite **entrust.com**

Para saber más sobre los HSMs nShield de Entrust

HSMinfo@entrust.com

entrust.com/HSM

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

Contáctenos:
HSMinfo@entrust.com