ENTRUST

M E

Microsoft

m I C

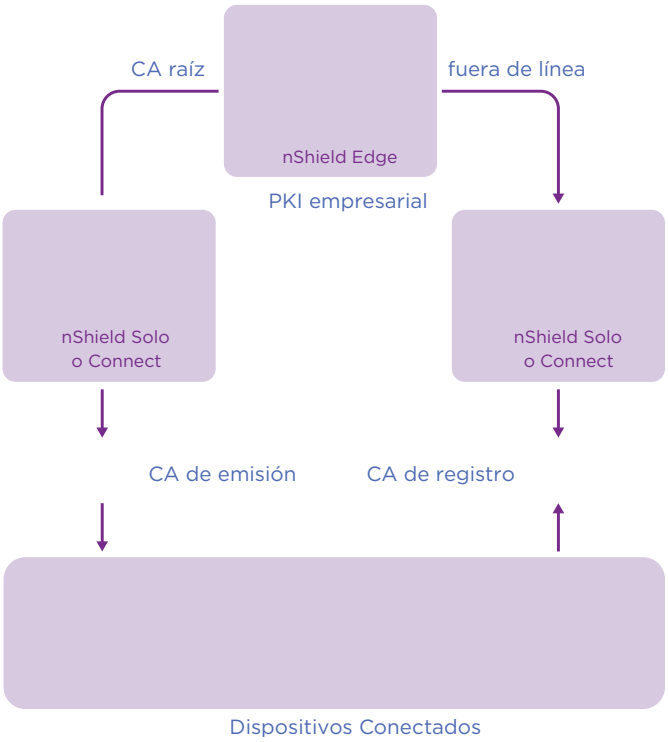
Los servicios de inscripci[o]n de dispositivos y los m[o]dulos de seguridad de hardware permiten el registro seguro de dispositivos del IoT

CA AC E ICA P INCIPALE

- 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.

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