# Soluciones de code signing de Entrust

## Seguridad de alta confiabilidad para code signing

### CARACTERÍSTICAS PRINCIPALES

- Asegura la autoría, fecha de publicación y contenido
- Establece la integridad del software
- Protege valiosas claves de code signing

## Desafíos de la distribución de códigos

El negocio de TI es complejo y utiliza software de una amplia variedad de fuentes para que una organización funcione. Las empresas que desarrollan software, ya sea para uso interno o para vender a sus clientes, necesitan crear o respaldar mecanismos que demuestren la autenticidad de su software. Garantizar esta seguridad requiere lo siguiente:

- Validando el proceso de firma, de tal manera que solo el código correcto se firme con las claves correctas
- Administrar las claves de firma privadas para que no sean robadas, lo que permite que versiones no autorizadas lleguen a sus clientes.
- Proporcionando un seguimiento de auditoría de toda la actividad de firmas

Entrust cuenta con gran experiencia en el desarrollo e implementación de soluciones seguras de code signing que resuelven los desafíos del proceso en cuanto a integridad, autorización y protección de claves privadas al proporcionar las siguientes capacidades:

- Reduce el riesgo de robo de claves, imposiciones corporativas y alteración de software malicioso
- Permite que los usuarios finales verifiquen la fuente y la integridad del software y detecten la alteración o inserción de un código malicioso
- Ayuda a evitar que los usuarios abandonen la instalación debido a los fuertes diálogos de advertencia de los sistemas operativos para software no firmado
- Proporciona control de acceso, flujo de trabajo de aprobación, capacidades de automatización y de auditoría para operaciones de firma de códigos.

Para ofrecer estas capacidades, Entrust ofrece dos soluciones de firma de código que se basan en los módulos de seguridad de hardware (HSMs) nShield de Entrust como la raíz de confianza. Estas soluciones son:

- Code Signing Gateway
- Code Signing con integración directa de HSM

### Qué es el código

El código puede verse como un paquete binario de información que se consume o ejecuta en las plataformas de destino. Los ejemplos de código incluyen paquetes ejecutables, paquetes de instalación, paquetes de firmware y entornos integrados.

**APRENDA MÁS EN ENTRUST.COM/HSM**

# Soluciones de code signing de Entrust

## Firma de códigos con los HSMS de Entrust como raíz de confianza

Code signing es la aplicación de firmas digitales para la publicación de software. Code signing le permite a los usuarios finales verificar la fuente y la integridad del software al autenticar la identidad del editor; también ayuda a evitar que los usuarios abandonen las instalaciones de software, ya que los sistemas operativos presentan diálogos de advertencia fuertes para el software sin firmar.

Las soluciones de firma de códigos utilizan el par de claves públicas/privadas del originador del software y un certificado digital, que incluye la clave pública del originador del software y está firmado por una CA adecuada, para que el usuario final pueda verificar el código. El proceso comienza cuando el creador del software hace un hash del código que se va a distribuir y utiliza su clave privada para firmar/cifrar el hash. Después distribuye el hash cifrado y el código original, junto con el certificado digital, en un paquete para el usuario final. En el último paso, el usuario final utiliza la clave pública del creador del software para descifrar el código cifrado y con hash y compara el hash resultante con un hash regenerado del código recibido. Si los hashes son idénticos, se verifica el código.

La clave privada es fundamental para la seguridad del sistema de firma de códigos y nunca debe ser revelada o compartida. Si la clave privada se compromete, el sistema de confianza falla. La seguridad de la clave de firma privada apuntala el proceso de firma de códigos.

Para aplicaciones confidenciales tales como la firma de códigos, proteger la clave privada cuando está en uso y cuando no está en uso es fundamental para crear una solución segura. Los HSMs proporcionan un entorno certificado a prueba de manipulaciones indebidas para proteger las llaves durante todo su ciclo de vida

## Code Signing Gateway

Para las organizaciones más grandes que necesitan un proceso de aprobación de firmas de software altamente controlado, el Code Signing Gateway ofrece una gama de funciones de automatización de flujo de trabajo flexibles y centralizadas que ayudan a las organizaciones de desarrollo de software a cumplir con los sólidos requisitos de seguridad. Code Signing Gateway es un servidor centralizado alojado por el cliente que ejecuta aplicaciones de flujo de trabajo de firma de código Entrust.

El Code Signing Gateway administra el flujo de trabajo, acepta solicitudes, notifica a los aprobadores por correo electrónico, administra los tiempos de espera, reconoce las aprobaciones, registra la actividad y entrega un código firmado al área de preparación. Apoya múltiples usuarios y funciones, incluidos, por ejemplo: los administradores de Code Signing Gateway, los desarrolladores de aplicaciones empresariales, de escritorio, IoT o móviles, el equipo de administración y los que aprueban code signing. La integración de Active Directory se utiliza para la autorización de grupos de trabajo y la autenticación de usuarios.

## HSMs de uso general de nShield

Los HSMs nShield son dispositivos certificados, fortalecidos y a prueba de manipulaciones indebidas que proporcionan un entorno seguro para generar y proteger las claves utilizadas para una variedad de aplicaciones. Los HSMs nShield están disponibles en tres factores de forma:

- nShield Connect, un dispositivo que sirve múltiples aplicaciones a través de una red, también disponible como un nShield Solo de servicio,
- una tarjeta PCIe que atiende aplicaciones en un solo servidor
- nShield Edge, un dispositivo de escritorio con conexión USB para transacciones de menor volumen

Los módulos de seguridad de hardware nShield Edge están certificados para FIPS 140-2 Nivel 2 y Nivel 3

# Soluciones de firma de códigos de Entrust

Los HSMs nShield de Entrust se usan para proteger la llave privada que se usa para firmar el código. Las llaves de firma residen en los HSMs y se asignan a múltiples perfiles de firma que se pueden crear en Code Signing Gateway.

Code Signing Gateway se integra con herramientas de firma estándar como Oracle Jarsigner, Microsoft SignTool, la herramienta de firma de códigos de Apple y la utilidad de firma de código de Android. El esquema del proceso se ilustra en la Figura 1.

Como funcionalidad adicional incluye múltiples perfiles de firma que se pueden definir para utilizar una serie de certificados digitales que admiten múltiples perfiles de firma, registro centralizado, almacenamiento de archivos, integración con un servicio de marca de tiempo, así como integración con Microsoft Defender para verificar si hay virus en los archivos antes de firmar.

Code Signing Gateway de Entrust es una solución personalizada para el entorno único de cada cliente por parte del equipo de servicios profesionales de Entrust.

## Code Signing con integración directa del HSM

La integración directa con HSM nShield de Entrust proporciona una solución para un pequeño número de desarrolladores con una simple separación de tareas. Normalmente se utiliza para estaciones de trabajo de desarrollador individuales o servidores de firma de códigos exclusivos. La clave privada utilizada para la firma de códigos es generada y protegida por el HSM nShield.

La firma de códigos se integra con el HSM mediante una API estándar, por ejemplo, Java Cryptography Extension (JCE) y Microsoft CAPI así como CNG, y utiliza herramientas de terceros como Jarsigner, SignTool y Open SSL para crear solicitudes de firma para su ejecución a través del HSM.

## Más información

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

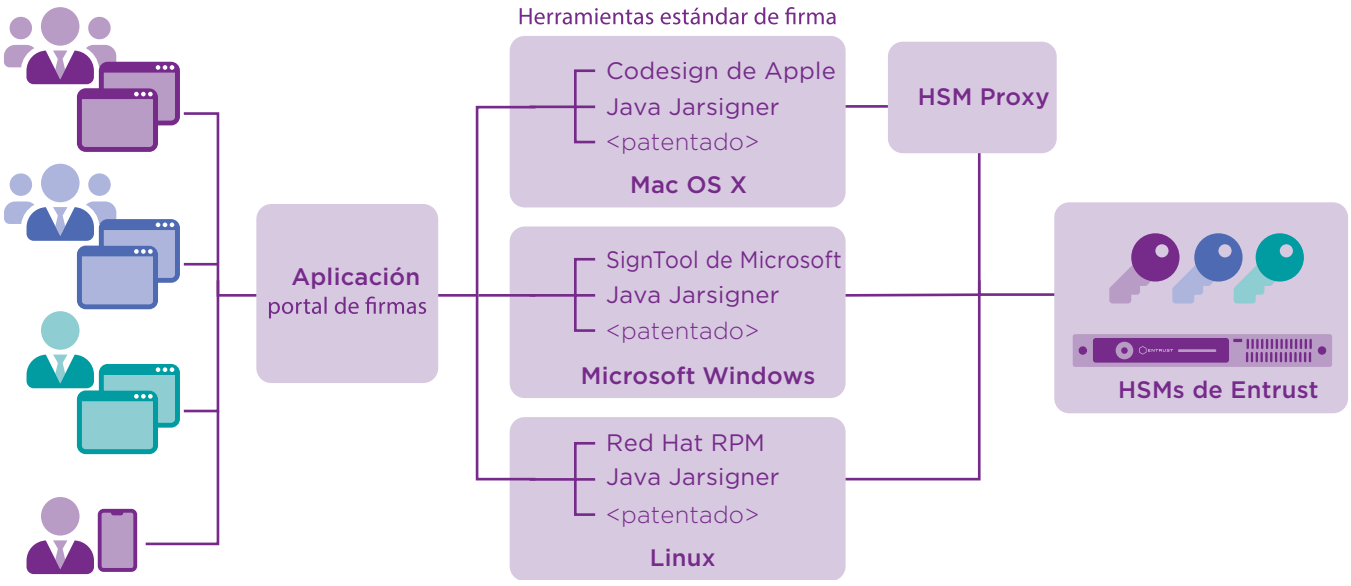


Figura 1: Esquema de Code Signing Gateway

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**