



ENTRUST



nShield Web Services Option Pack

Interfaz tipo REST admitida en la nube para módulos de seguridad de hardware de alta seguridad

CARACTERÍSTICAS GENERALES

- Acceso a una solución de protección de datos de alta seguridad para aplicaciones en la nube, en centros de datos o locales
- Conexión fácil y personalizada a los servicios criptográficos del módulo de seguridad de hardware nShield
- Permite una implementación de aplicaciones dinámica, escalable y rápida
- SO flexible y compatibilidad de la arquitectura

El nShield Web Services Option Pack (WSOP) ofrece una API tipo REST ¹ entre aplicaciones que requiere claves criptográficas y servicios de protección de datos y módulos de seguridad de hardware (HSM) con certificación FIPS. Los HSMs de nShield llevan a cabo una variedad de funciones criptográficas incluyendo el cifrado, firmado, descifrado, verificación y generación de claves. Estas funciones principales están disponibles para las aplicaciones a través de una interfaz de servicio web sencilla que utiliza el protocolo universal HTTPS.

PRESTACIONES Y BENEFICIOS PARA CLAVES

- **Acceso eficaz a servicios criptográficos remotos desde aplicaciones en la nube, en centros de datos o locales**
Las aplicaciones que residen en cualquier lugar, ya sea en la nube, en centros de datos remotos o de forma local, pueden acceder a los servicios nShield a través de llamadas de servicio web basadas en https a través de la API tipo REST, aportando flexibilidad a los variados entornos informáticos actuales.
- **Proceso de implementación personalizado**
La interfaz de servicio moderna y eficiente mejora la velocidad a la que pueden desarrollarse las aplicaciones para acceder a los servicios criptográficos de HSM nShield.
- **Sin necesidad de integración por parte del cliente**
Normalmente, integrar aplicaciones con los HSMs de nShield requiere la vinculación a bibliotecas local host y la implementación de servicios locales. Al usar los servicios API tipo REST, los desarrolladores se benefician de una menor complejidad de implementación.



nShield Web Services Option Pack (WSOP)

- **SO flexible y compatibilidad de la arquitectura**

La interfaz de los servicios web tipo REST es independiente de la infraestructura de la aplicación del cliente y no requiere de un sistema operativo específico local para la aplicación, lo que simplifica la integración, particularmente en entornos personalizados.

- **Escalabilidad dinámica**

Genera cargas de trabajo de aplicaciones nuevas o adicionales sin necesidad de configurar más HSM, soporte de instalación de software o licencias de cliente; ajuste su capacidad aumentándola o reduciéndola para cumplir con sus necesidades, incluidos los nodos WSOP integrados en una arquitectura de contenedor.

- **Admisión de equilibrio de carga con dispositivos COTS dedicados**

El WSOP permite administrar la carga de trabajo del HSM usando equilibradores de carga comerciales (COTS) para simplificar la implementación/configuración del HSM y así asegurar el mejor uso del grupo de HSM.

Como comenzar con nShield Web Services Option Pack

Necesitará:

- Software Security World v12.6x o posterior
- Suscripción a nShield Solo, Connect HSM o nShield as a Service

Para usar la API tipo REST, el WSOP nShield se instala en un servidor de cliente nShield, activando el servicio y poniéndolo a disposición de conexiones directas e inmediatas desde las aplicaciones.

WSOP se configura por defecto con un grupo de certificados TLS temporales de corta duración simplemente con fines de prueba. La configuración debe actualizarse con los certificados apropiados para pruebas continuas o uso en producción.

Para el HSM nShield Connect: se necesita una licencia de cliente estándar solo para el servidor del cliente que ejecute el servicio web. Las licencias de cliente no son necesarias para conectar aplicaciones.

Nota 1: La transferencia de estado representacional o REST (por sus siglas en inglés) es una arquitectura basada en el estándar web y usa el protocolo universal HTTP para la comunicación de datos. HTTP se considera un protocolo sin estado porque cada comando se ejecuta de forma independiente, sin conocimiento de los comandos anteriores. REST se basa en recursos donde cada componente se considera un recurso al que se accede por una interfaz común usando llamadas HTTP.

Los atributos REST de WSOP incluyen:

- URI bien definidos que solo identifican "recursos", por ejemplo /keys /sign /verify, etc.
- Métodos HTTP como verbos para realizar acciones en esos recursos, por ejemplo, GET para operaciones de lectura como mostrar un listado claves, POST para operaciones de escritura como crear claves, DELETE para operaciones de eliminación como eliminar claves.

MÁS INFORMACIÓN EN [ENTRUST.COM/HSM](https://entrust.com/hsm)



nShield Web Services Option Pack

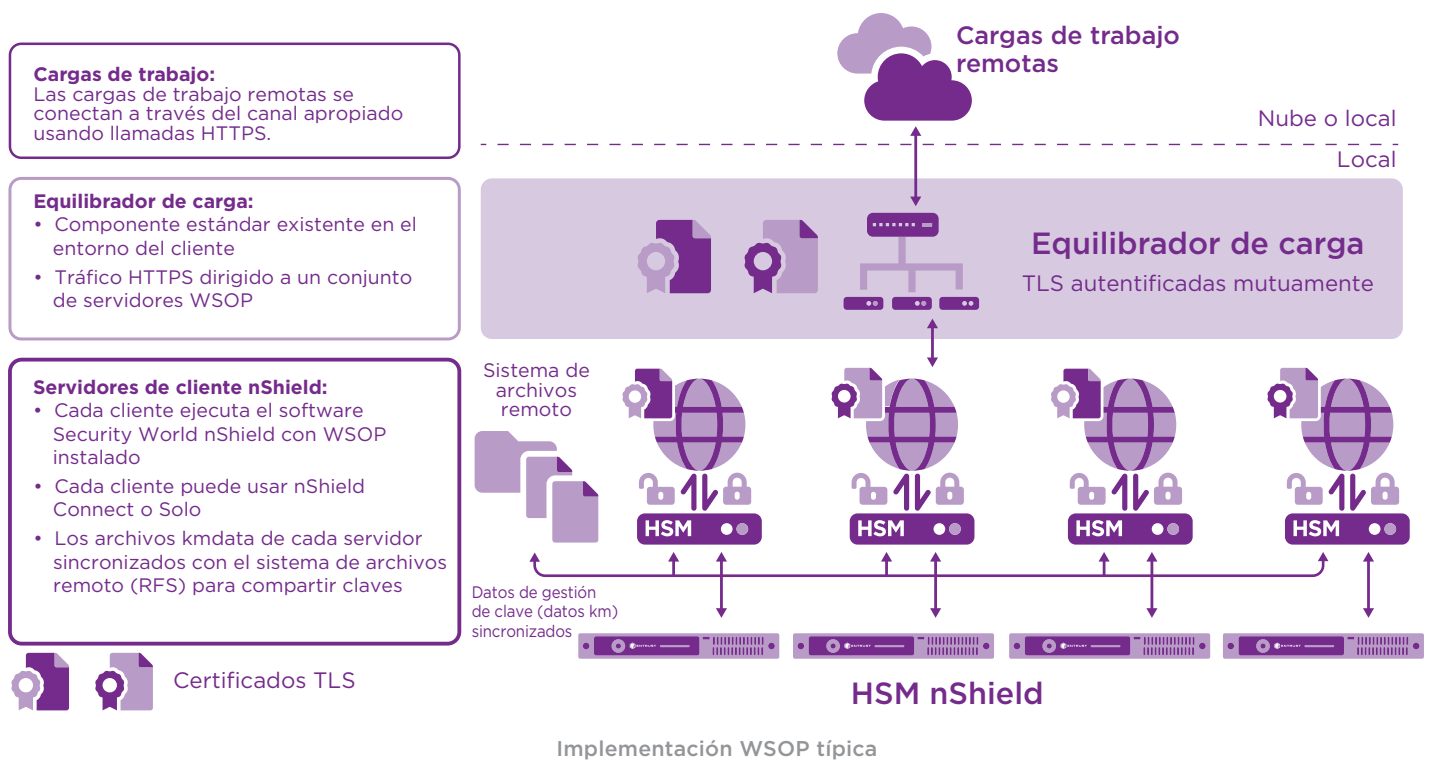
ESPECIFICACIONES TÉCNICAS

Compatibilidad nShield

El WSOP de nShield es compatible con todos los modelos de nShield Solo y los HSM Connect. El WSOP debe instalarse en un host ejecutando una versión admitida de Linux y tener el software Security World nShield instalado. WSOP admite un conjunto de tarjetas de operador y claves protegidas por Softcard. WSOP también es compatible con el paquete de opciones de contenedor de nShield, que permite que el WSOP se implemente en un entorno contenedorizado.

Compatibilidad de API

Los HSMs nShield pueden admitir aplicaciones usando la API de servicios web junto con aplicaciones que usen otras API admitidas (PKCS#11, Java, CNG, etc.).



Más información

Para saber más sobre los HSM nShield de Entrust visite [entrust.com/HSM](https://www.entrust.com/HSM). Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite [entrust.com](https://www.entrust.com)

Para saber más
sobre los HSMs
nShield de Entrust

HSMinfo@entrust.com
entrust.com/HSM

SOBRE ENTRUST CORPORATION

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Ahora más que nunca, la gente necesita experiencias seguras impecables, mientras cruzan fronteras, realizan compras, acceden digitalmente a servicios del gobierno o inician 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 de más de 150 países, no es una sorpresa que la mayoría de organizaciones autorizadas del mundo confíen en nosotros.

Más información
entrust.com/HSM

