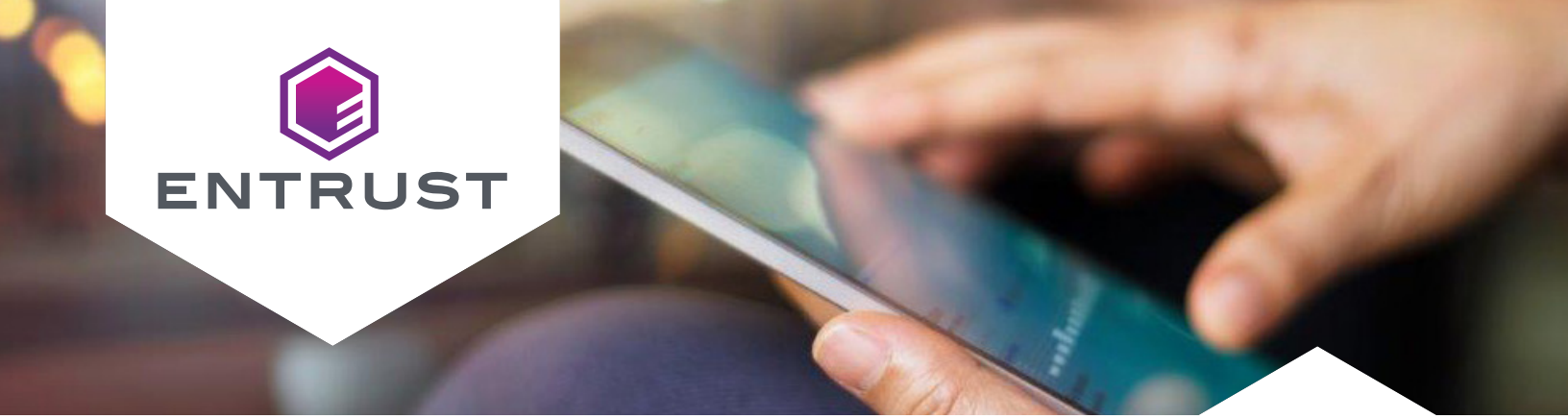


# nShield Web Services Option Pack

## Cloud-friendly REST-like interface to high assurance hardware security modules

### HIGHLIGHTS

- Access to high security data protection solution from cloud, data center or on-premises applications
- Streamlined, easy connection to nShield hardware security module cryptographic services
- Enables fast and scalable dynamic application deployment
- Flexible OS and architecture support

The nShield Web Services Option Pack (WSOP) provides a REST-like[1] API between applications requiring cryptographic key and data protection services and FIPS certified nShield hardware security modules (HSMs). nShield HSMs perform a variety of cryptographic functions including encryption, decryption, signing, verifying, and key generation. These core functions are now available to applications through a simple web-service interface utilizing the universal HTTPS protocol.

### KEY FEATURES & BENEFITS

- **Efficient access to remote cryptographic services from the cloud, data center or on-premises applications**
  Applications that reside anywhere, whether in the cloud, in remote data centers or locally, can access nShield services through https based web service calls via the REST-like API, bringing greater flexibility to today's varied computing environments.
- **Streamlined development process**
  The efficient, modern web service interface improves the speed with which applications can be developed to access nShield HSM crypto services.
- **No need for client-side integration**
  Typically, integrating applications with nShield HSMs requires binding to local host libraries and deploying local services; by using the web services REST-like API, developers benefit from reduced deployment complexity.

# nShield Web Services Option Pack

- **Flexible OS and architecture support**
  The web services REST-like interface is independent of client application infrastructure and requires no OS-specific software local to the application, thus simplifying integration, particularly in custom environments

- **Dynamic scalability**
  Spin up new or additional application workloads without requiring further HSM configuration, support software installation or client licenses; adjust your capacity up or down to meet demand easily - including WSOP nodes when deployed in a container architecture

- **Support load balancing using dedicated COTS appliances**
  WSOP allows the HSM workload to be managed using commercial off-the-shelf (COTS) load balancers simplifying the HSM deployment/ configuration and ensuring the best utilization of a pool of HSMs

## Getting started with nShield Web Services Option Pack

You will need:

- Security World software v12.6x or greater
- nShield Solo, Connect HSM or nShield as a Service subscription

To use the REST-like API, the nShield WSOP is installed on an nShield client server, activating the service and making it available for direct and immediate connections from applications.

WSOP is configured by default with a set of temporary, short term TLS certificates solely for testing purposes. The configuration should be updated with appropriate certificates for ongoing testing or production use.

For nShield Connect HSMs: a standard client license is required only for the client server running the web service. Client licences are not required for connecting applications.

Note 1: REST (REpresentational State Transfer) is a web standards based architecture and uses the universal HTTP Protocol for data communication. HTTP is considered a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. REST is resource based where every component is considered a resource which is accessed by a common interface using HTTP calls.

WSOP REST'ful attributes include:
- well-defined URI's that uniquely identify "resources" e.g. /keys /sign /verify etc.
- HTTP methods as verbs to perform actions on that resource e.g. GET for read operations such as listing keys, POST for write operations such as creating keys, DELETE for delete operations such as deleting keys.

# nShield Web Services Option Pack

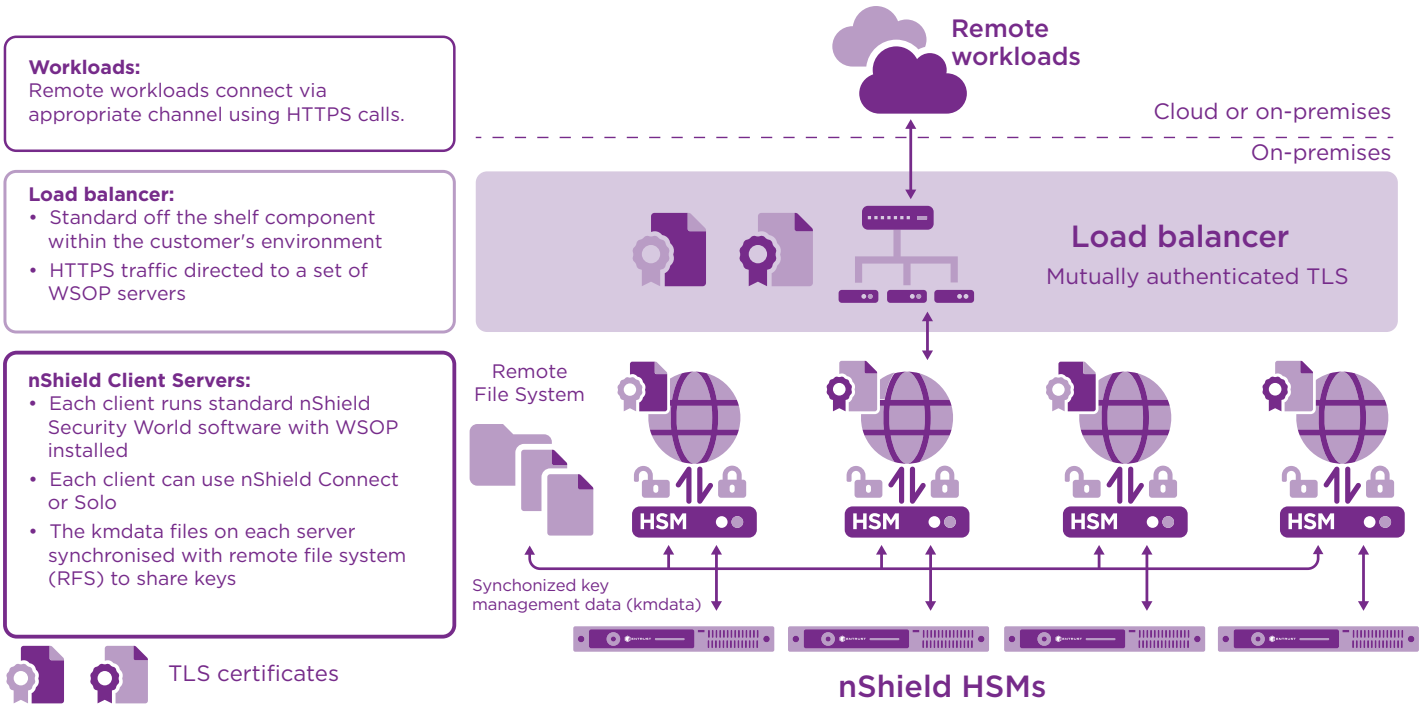
## TECHNICAL SPECIFICATIONS

### nShield compatibility

The nShield WSOP is compatible with all models of nShield Solo and Connect HSMs. The WSOP must be installed onto a host running a supported version of the Linux OS and have the nShield Security World software installed. WSOP supports Operator Card Set & Softcard protected keys. WSOP is also compatible with the nShield Container Option Pack allowing WSOP to be deployed in a containerized environment.

### API compatibility

nShield HSMs can support applications using the web services API in conjunction with applications using other supported APIs (PKCS#11, Java, CNG, etc.).




Typical WSOP deployment

## Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

**HSMinfo@entrust.com**
**entrust.com/HSM**

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
**entrust.com/HSM**



ENTRUST

**Contact us:**
**HSMinfo@entrust.com**