nShield Web Services Option Pack

- 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

nShield Web Services Option Pack

Cloud-friendly REST-like interface to high assurance hardware security modules
The nShield Web Services Option Pack (WSOP) provides a REST-like 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.

The key benefits of the nShield WSOP are:

- **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.

- **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 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.

**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.).

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 RESTful 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.
**Workloads:** Remote workloads connect via appropriate channel using HTTPS calls.

**Load Balancer:**
- Standard off the shelf component within the customer's environment
- HTTPS traffic directed to a set of WSOP servers

**nShield Client Servers:**
- Each client runs standard nShield Security World software with WSOP installed
- Each client can use nShield Connect or Solo
- The kmdata files on each server synchronised with Remote File System (RFS) to share keys

**TLS certificates**

**Remote workloads**

**Load Balancer**
Mutually authenticated TLS

**Remote File System**

**nShield HSMs**

Figure 1: Typical WSOP deployment

**LEARN MORE**
To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com
ABOUT NCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today’s fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com