S C O P E

Deploy containerized applications integrated with high-assurance nShield hardware security modules

HIGHLIGHTS

- Allows customers to build their containerized deployments in conjunction with an nShield HSM, for
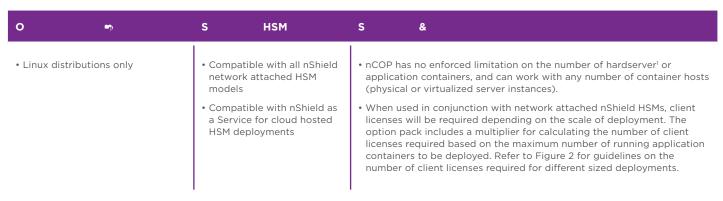
High level architecture

The nCOP provides easy access to a flexible and scalable containerized architecture that interoperates with an existing nShield HSM and Security World environment.

On premises or hosted

Figure 1: High level architecture of nCOP

TECHNICAL SPECIFICATIONS

O		S	HSM	S	&
• Linux distributions only		• Compatible with all nShield network attached HSM models • Compatible with nShield as a Service for cloud hosted HSM deployments		• nCOP has no enforced limitation on the number of hardserver[1] or application containers, and can work with any number of container hosts (physical or virtualized server instances). • When used in conjunction with network attached nShield HSMs, client licenses will be required depending on the scale of deployment. The option pack includes a multiplier for calculating the number of client licenses required based on the maximum number of running application containers to be deployed. Refer to Figure 2 for guidelines on the number of client licenses required for different sized deployments.	

N HSM	M	M
5	5	50
10	10	100
15	15	150
20	20	200
>25	25	> 250 Recommend purchase of enterprise client licenses

Figure 2: Required number of client licenses per HSM based on container host and application container sizing

Note 1: The hardserver is the daemon service component of the nShield Security World software - which is responsible for secure communication with nShield devices across the network. Client components including PKCS#11 and Java libraries use sockets to interface with this process.

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

HSM @ .