nCIPHER AN ENTRUST DATACARD COMPANY

nCipher Security

Security World

José María Pérez Romero

Agenda

- Simplistic HSM view vs Security World approach
- Security World architecture
- Role segregation
- Advantages in Cloud deployments
- Compatibility with Containers deployments
- eIDAS: QSCD
- Resources

The nShield difference: Security World architecture

Easy scaling of nShield estates

- Performance scalability
- Unlimited number of HSMs can be pooled

Convenience, flexibility and ease of operation

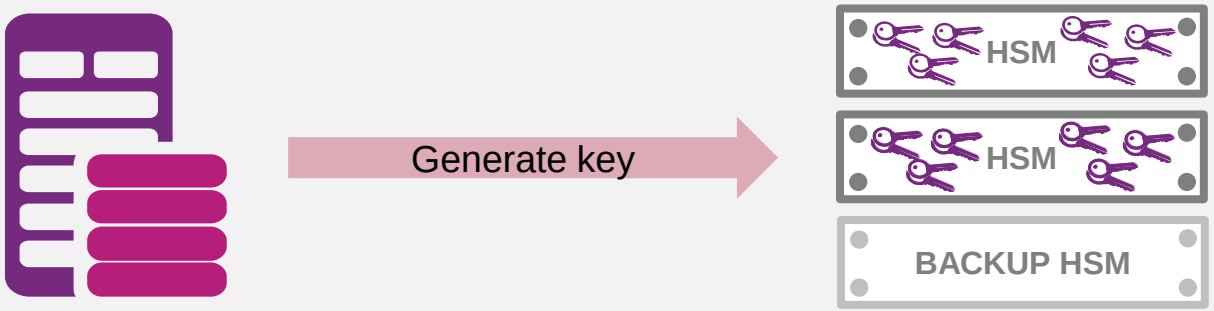
- Easy backups, eliminating manual cloning
- Unlimited storage of keys

Resilient to hardware failure

- Seamless failover and load balancing
- No single point of failure
- Units can be shipped and will never have keys in memory

Simplistic HSM view vs Security World approach

Simplistic HSM view



Keys “never” leave the HSM

Security World approach

Security World approach

MEMORY

BACKUP

Create “new world”

Generate key

APPLICATION KEY

MODULE KEY

- AES 256
- Generated with HSM RNG
- Stored into NVRAM
- Backed up onto ACS

Administrator Card Set

***K-of-N* Policy:**
N = total number of cards
K = cards required to Admin

Any combination of K cards recreates Module Key

Security World approach

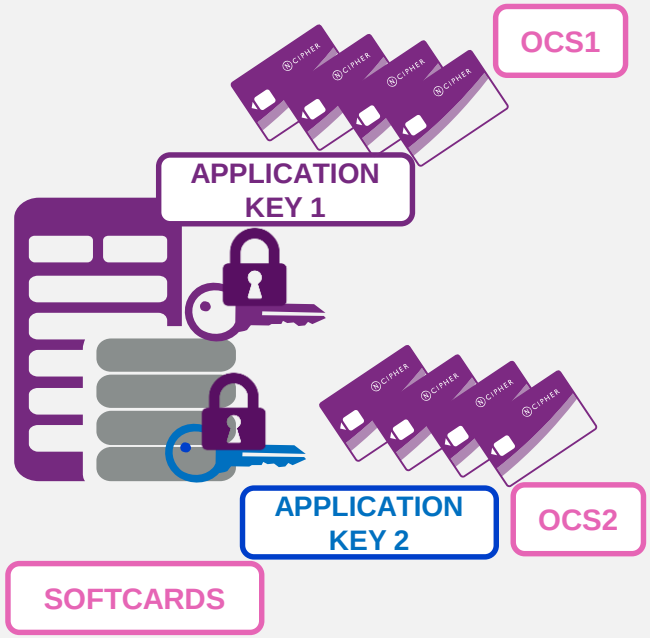
Security World approach

FIPS VALIDATED 140-2

Common Criteria

nCIPHER
AN ENTRUST DATACARD COMPANY

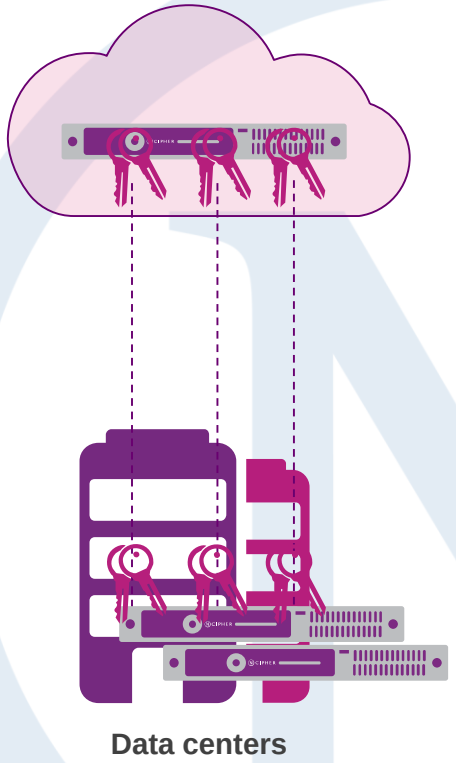
Role segregation



MODULE KEY

Advantages in Cloud deployments

- Key material stays in your control at all times
- Unique Security World architecture delivers a unified administrator and user experience
- Scale HSM operations with your specific strategy and requirements
- Keys are generated and protected separately from sensitive data



nCIPHER
AN ENTRUST DATACARD COMPANY

Compatibility with Containers deployments

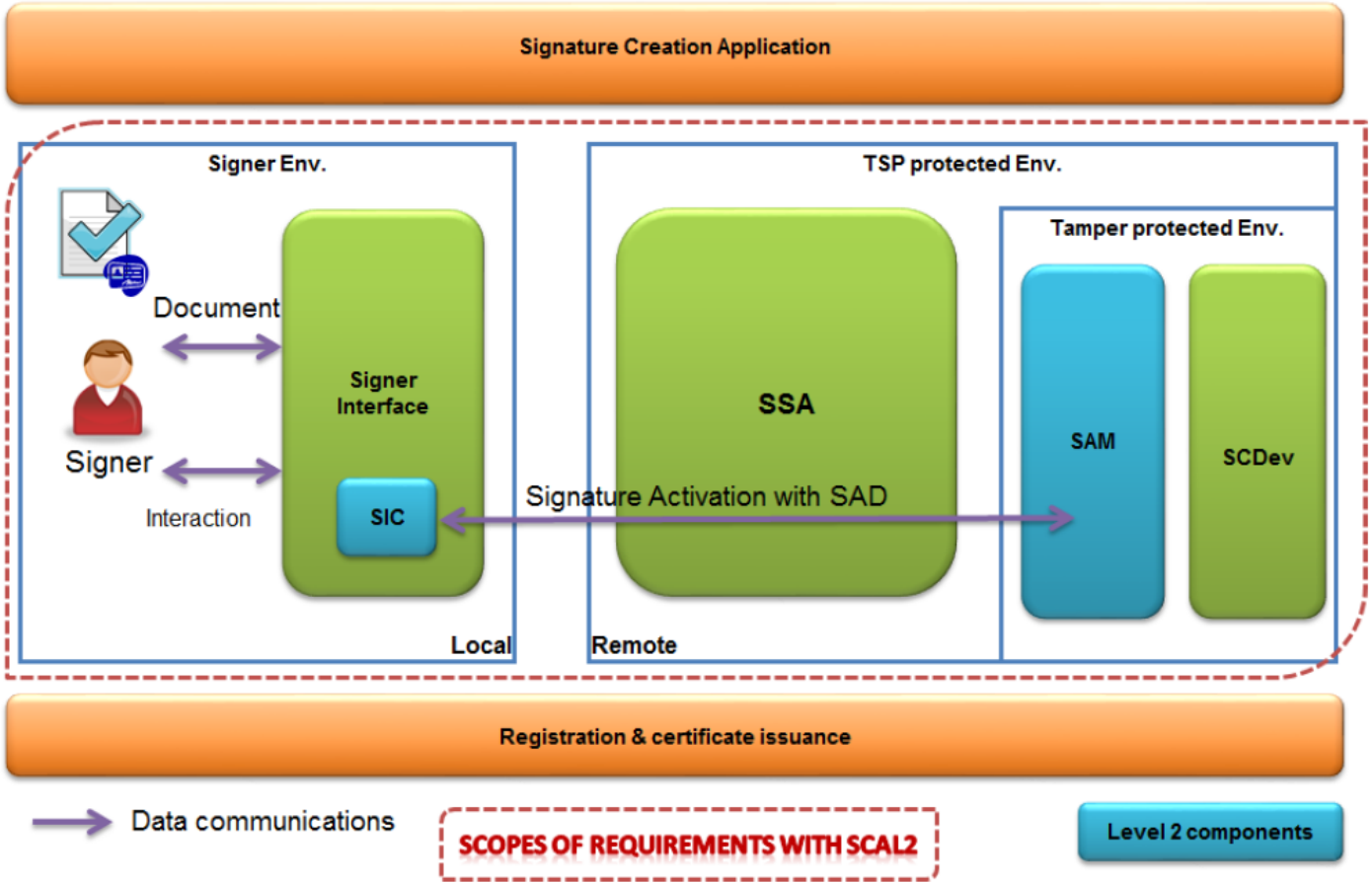
nShield Container Option Pack

- Allows developers to leverage the dynamic deployment, scalability and orchestration benefits of the platform
- Containerized applications can readily access nShield HSMs for processing sensitive data and key material
- Provides a strong building block for cloud deployments

docker kubernetes OPENSHIFT Amazon EKS

nCIPHER
AN ENTRUST DATACARD COMPANY

eIDAS: QSCD



nShield Solo XC
QSCD Type 1

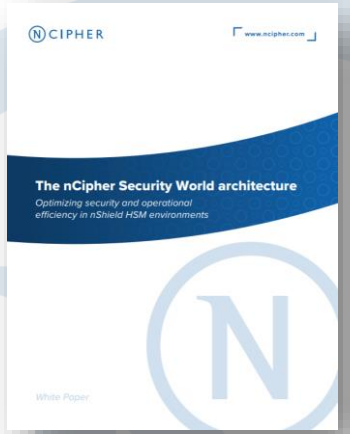
nShield Solo XC
QSCD Type 2:
EN 419-221.5

Cryptographic Module for Trust Services

nCIPHER
AN ENTRUST DATACARD COMPANY

Resources

- nCipher Security World white paper
- Find here on the nCipher website
- Security World is also referenced on nShield web pages, data sheets and family brochure
- For more information, contact your nCipher rep.



nCIPHER
AN ENTRUST DATACARD COMPANY

AN ENTRUST DATACARD COMPANY