nCIPHER

nCipher Security Updates

Trust. Integrity. Control.

Ena Hurmola
Senior Solutions Consultant, CISSP
nCipher Security

AGENDA

- **nCipher Security as company**
  - Company introduction
  - nShield overview
  - eIDAS qSCD updates
  - FIPS 140-2 certification updates
- **nCipher Use Cases**
  - eIDAS Remote Signing
  - Other use cases
    - Local PKI and HSM usage
    - Hybrid PKI Authentication Infrastructure
    - Cloud Information Protection - BYOK/Microsoft Azure KeyVault API

nCipher Security

20+ Years of delivering trusted threat protection and enabling compliance

Deep expertise and track record in applied cryptography

HSM market leader with a long history of industry certifications and validation

nCIPHER

Trust
Integrity
Control

Cloud
IoT
Blockchain
Payments

Solutions delivering trust for business critical applications and information

1000+ 

Organizations rely on nCipher to secure and globally support their applications and information

- 5 of the top 10 Fortune 100
- 10 of the top 20 FTSE 100

What's happening with nCipher Security?

In Q4 2018

- the European Union Commission required Thales to break the General Purpose HSM business out of their organization so they could complete the acquisition of Gelmato.

1st January 2019

- nCipher became a standalone company offer the General Purpose HSM (nShield) product range owned by Thales but to be sold.

22nd February

- Entrust Datacard agreed to purchase nCipher from Thales.
- The acquisition of nCipher is expected to be closed by the end of the quarter.

nCIPHER

nCipher under Entrust Datacard ownership

Organization	• Focused set of goals on selling General Purpose HSMs to the broadest possible set of customers and use cases
Partnership	• nCipher plan to continue to support all of our partners and remain vendor neutral in these markets.
Competitiveness	• We also understand that our partners support competitive HSMs as we support other PKI and eSign partners.
nFinity Program	• nCipher will continue to support Technology partners through the nFinity partner program
Confidentiality	• nCipher will maintain confidentiality of our partners information per our contracts and NDAs.

nCIPHER

Hardware Security Modules (HSMs) provide the foundation of trust

Highest level of protection for encryption or signing keys

Implement and enforce customer-defined policy

"Harden" applications that use cryptography

Source of high quality random numbers for keys

A Hardware Security Module (HSM) is a certified, trusted platform for performing cryptographic operations and protecting keys

nCIPHER

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

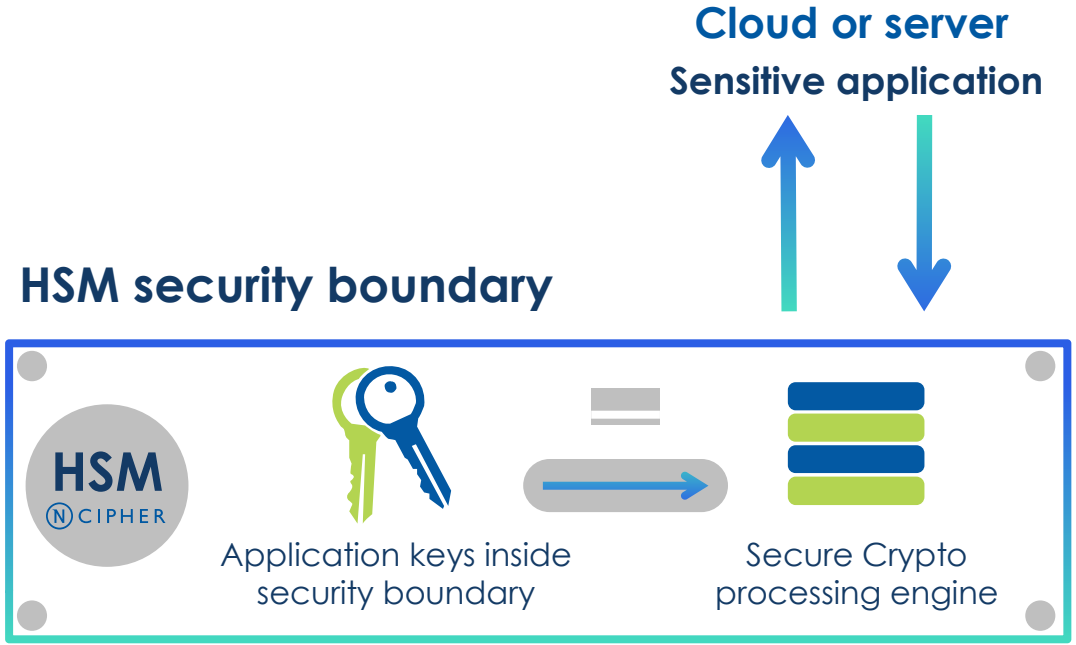
Resilient to hardware failure

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

The nShield difference: CodeSafe

CodeSafe is a secure run-time environment within the certified HSM boundary

- Ability to remove applications from more vulnerable cloud or server environments



Examples:

- Consensus logic for blockchain
- Manufacturing controls for IoT device key injection
- Code signing
- More… including custom

nCIPHER

nShield Certification Updates

Updates on FIPS 140-2 and CC EAL4+/qCSD certification

nShields with eIDAS certification

nShield + models are compliant to eIDAS standards

- nShield Solo+ and Connect+ were certified to Common Criteria* (CC) by the Italian certification agency, OCSI, in March 2016.
- OCSI granted **nShield** the status of **Secure Signature Creation Devices (SSCDs)** and as **Qualified Signature/Electronic SEAL Creation Devices (QSCDs)/**

http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/dispositivi-accertati

nShield XC models is under certification for EN 419 221 -5

- New generation nShields are currently under going new EN 419 221-5 profile of Common Criteria certification.

http://www.tuv-nederland.nl/nl/38/ongoing_certifications.html

*EAL4+ (AVA_VAN.5)
Find the OCSI certification doc on our website.

nShield firmware and FIPS 140-2 Certifications

	Latest FIPS	Latest non-FIPS on DVD[1]	Latest non FIPS by download[2]	In certification for FIPS[3]	In certification for CC[3]
Edge	2.61.1	2.65.2	12.50.2	12.50.8	NA
nShield +	2.61.2	12.40.0	12.50.2	12.50.8	NA
nShield XC	3.4.2	3.3.25	12.50.2	12.50.xx	12.50.7

- All nShield models are FIPS 140-2 Certified.
- Due to the increased security requirements with NIST SP800-131A Revision 1 and NIST Implementation Guidance, some of the existing certificates became temporary historical, and revised with new certification status.
- nShield + models and Edge for the FIPS certification.

Security world includes CC compliant mode

FIPS-140-2-level-3

- Security World compliant with FIPS140-2 level 3 .

Common-Criteria-Cmts

- Security World compliant with Common Criteria PP 419 221-5.

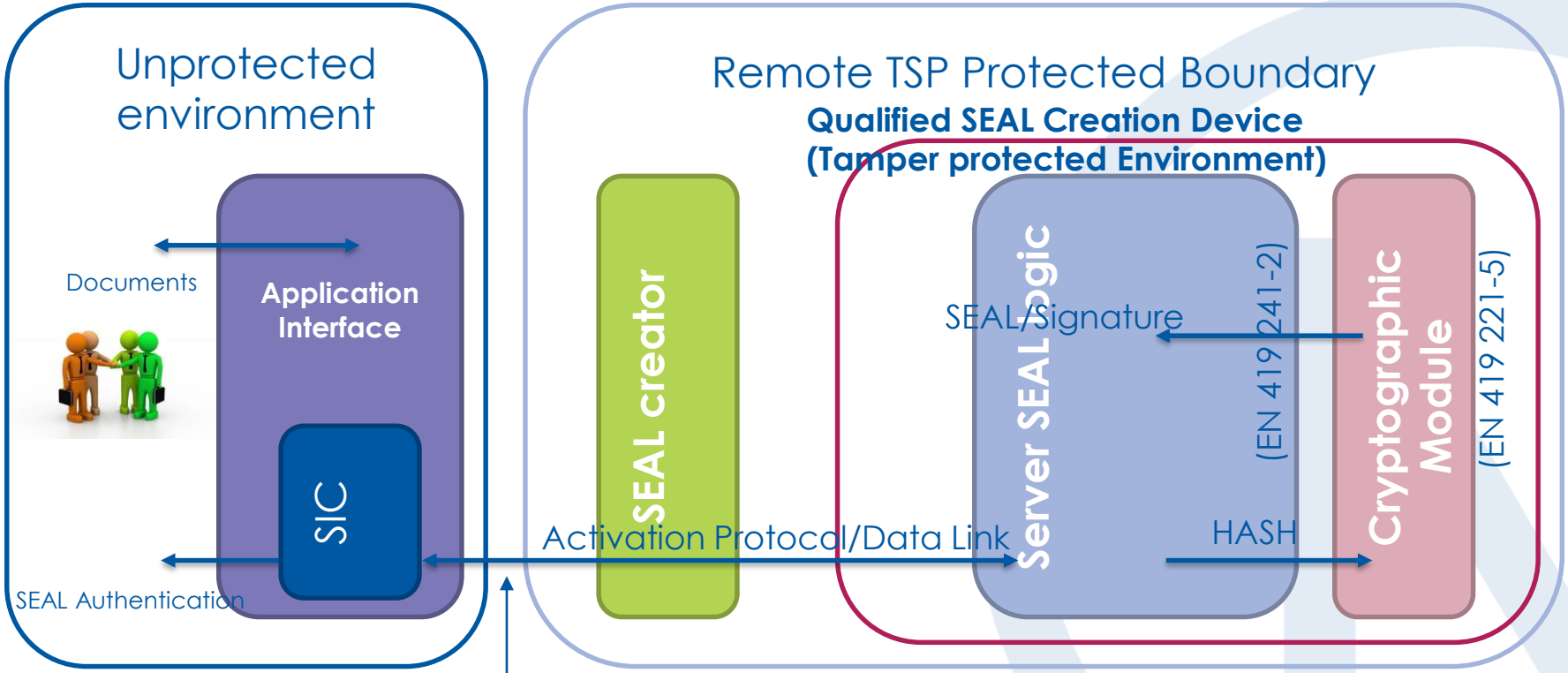
(Standard mode)

- Security World compliant with FIPS 140-2 level 2.

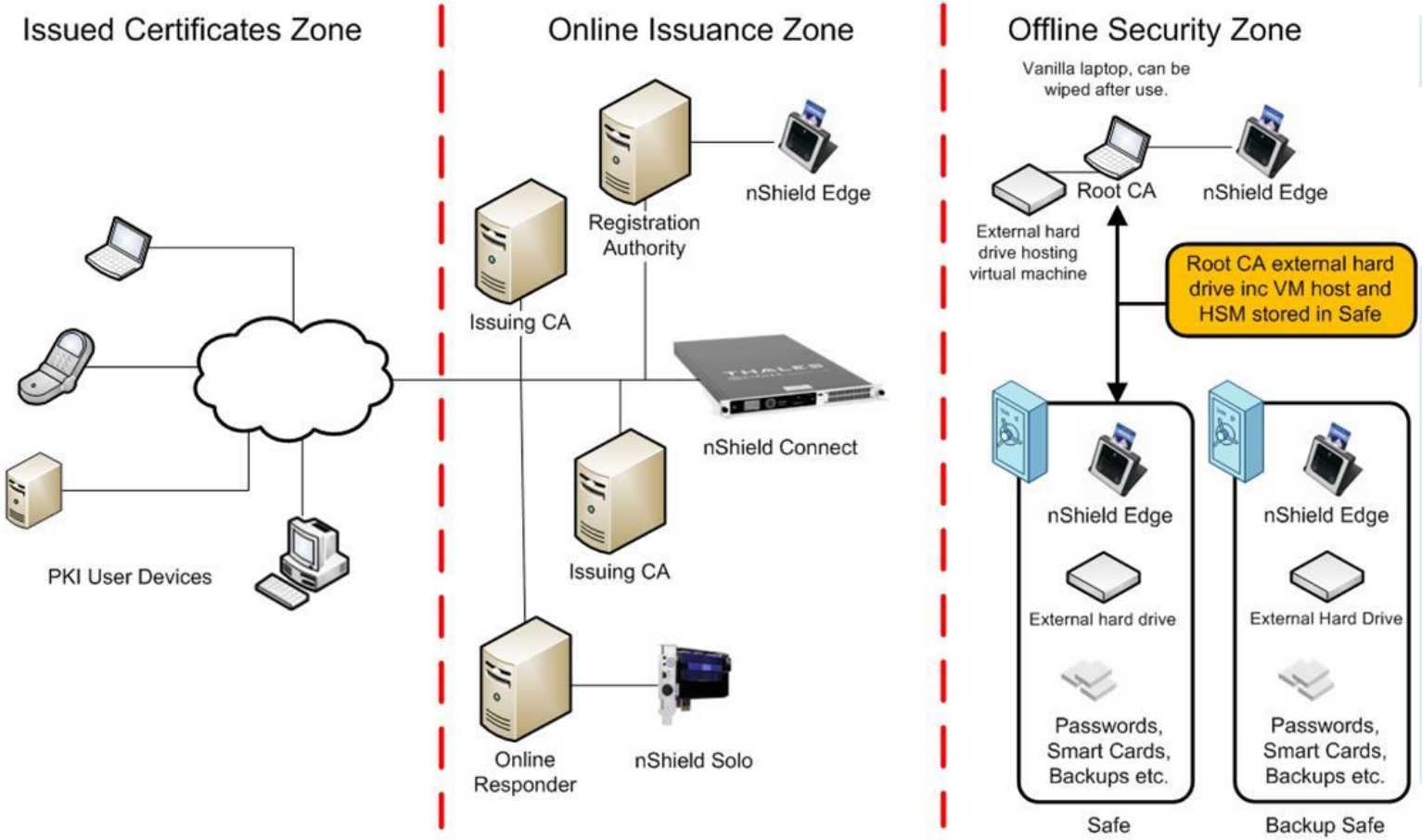
Use case examples & Case Study

Using HSMs for different purposes, different ways

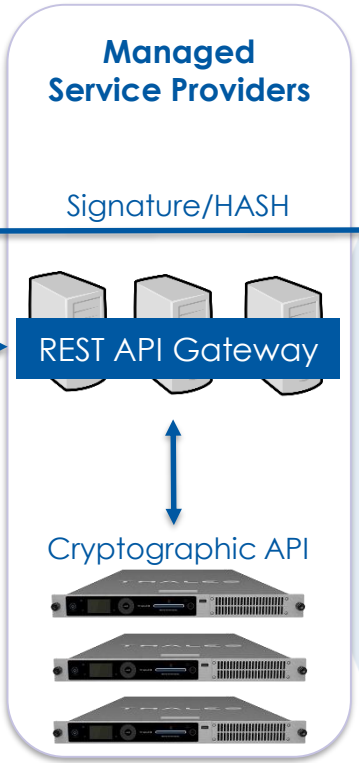
eIDAS Remote Signature



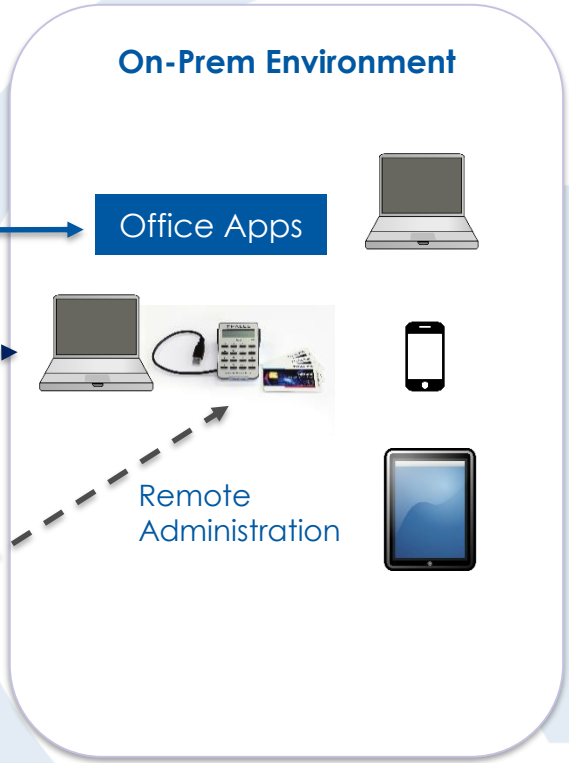
Traditional Public Key Infrastructure (PKI)



Hybrid PKI Authentication Infrastructure



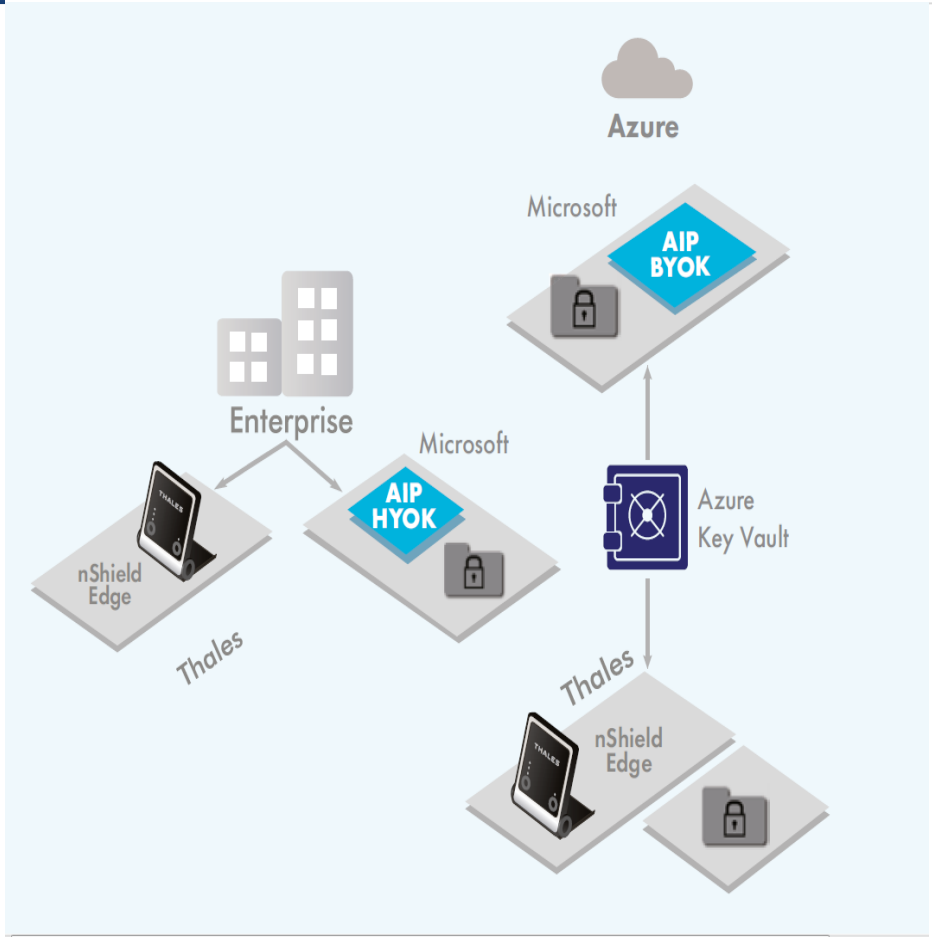
REST API



FIPS 140-2 level3/eIDAS qCSD

nCIPHER

Microsoft Azure BYOK and HYOK (Cloud)



Microsoft Azure KeyVault services

- Azure keyVault let you generate your own key and used as your tenant key

BYOK in Microsoft Azure

- Keys are transferred to nShield within Azure, providing HSM security at both ends.
- Azure KeyVault can be utilized in:
  - Office 365
  - SharePoint
  - Information protection
  - Market place

nCIPHER

nCIPHER

Thank you!

www.ncipher.com