

## nCipher nShield hardware security modules (HSMs) provide root of trust for Axway VA Server

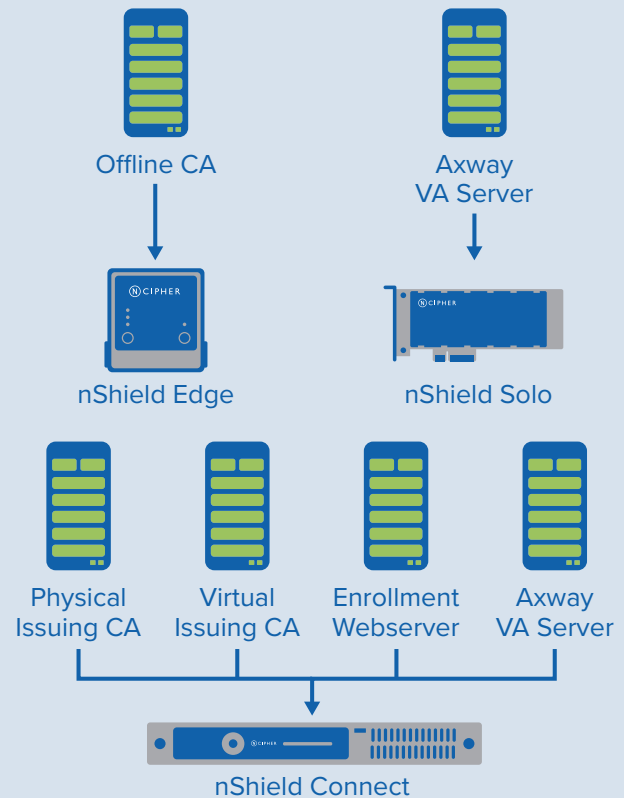
- Protects VA digital certificates that validate digital certificates issued by a CA
- Boosts performance in environments with high volume of validation requests
- Ensures smooth audits by employing industry best practices and due process
- Achieves compliance with FIPS 140-2 and Common Criteria EAL 4+ standards
- Assures business continuity through high-availability hardware platform



# Enhanced security, speed and compliance for Axway Validation Authority Server

### ASSURING THE VALIDITY OF DIGITAL IDENTITIES

Axway Validation Authority (VA) Suite protects mission-critical infrastructures, ensuring that revoked or invalid credentials cannot be used for secure email, smart card login, network access (including wireless), or other sensitive electronic transactions. The VA Suite can scale to the largest enterprise needs and enables the real-time validation of digital certificates. Systems relying on public key infrastructure (PKI) depend on the validity of digital certificates, the credentials issued by a Certification Authority (CA), to provide identity and trust. Electronic credentials such as smartcards, e-passports, security badges and other user identities can expire or be revoked. Before authenticating an identity, organizations must verify that the certificate is still valid.



# Enhanced security, speed and compliance for Axway Validation Authority Server

## ENHANCING SECURITY, SPEED, AND COMPLIANCE

Axway VA Server uses encryption and digital signatures to prove the authenticity of its responses to the clients and ensure the confidentiality of the requests. These operations rely on the security of their cryptographic keys. nCipher nShield HSMs integrate with Axway VA Server to protect keys, accelerate operations, and facilitate auditing and regulatory compliance. nShield HSMs can:

- Protect the OSCP, SCVP response signing and SSL keys for the Axway VA Server
- Improve server performance when there are high volume requests to validate certificates
- Add compliance with FIPS 140-2 Level 3 and Common Criteria EAL 4+ standards

## COLLABORATIVE RELATIONSHIP

Axway and nCipher have established a joint collaborative relationship with the integration of each solution:

- Joint support and service relationship to better serve customers who operate VA Server with integrated nCipher nShield HSMs
- Remote access to HSM (nSRES) for R&D to integrate VA Server with latest nCipher nShield HSMs

HSMs are considered an industry best practice to protect cryptographic keys and to facilitate auditing and compliance. Many security policies and regulations recommend key management practices that include HSMs to:

- Protect cryptographic keys in tamper resistant hardware
- Store keys in fewest possible number of locations and forms
- Enforce dual controls for key use to reduce insider threats

By using HSMs, organizations can achieve compliance, ensure smooth audits, and increase the overall security assurance of their solution. HSMs protect PKIs with trusted security validated to some of the highest security standards, securing identities in even the most demanding environments.

- Hardware key protection: HSMs store and protect CA signing keys used for issuing digital certificates in secure, tamper-resistant hardware to prevent theft and uncontrolled copying to backup tapes or USB drives
- Certified security: Validated for compliance with FIPS 140-2 Level 3 and Common Criteria EAL 4+
- Approved for high-security applications: Tamper-resistant and tamper-responsive hardware increase security assurance for high-value applications with dual control administration and operation

nShield HSMs enforce your security policy enabling you to easily demonstrate compliance to auditors.

- Dual control with two-factor authentication: A quorum of administrators (k of n) is required to present smart card credentials to carry out certain tasks
- Separation of roles: Security administration and operation are separated, providing an additional level of dual control
- Remote Operation: Remotely present operator credentials to nShield HSMs in other locations reducing the need for travel

## RECOMMENDED NCIPHER PRODUCTS

The following nShield HSMs are recommended for use with Axway VA Server:

- nShield Solo: Embedded HSM for one client
- nShield Connect: Network-attached HSM for up to 100 clients

## EASY SETUP AND FLEXIBLE DEPLOYMENT

nShield HSMs integrate readily with Axway VA Server through an industry-standard PKCS#11 interface.

- Easy deployment: nCipher publishes integration guides with fully tested integrations for quick deployment on Windows Server and Linux
- Extensible infrastructure: Expand the use of nShield HSMs, including support for other solutions, including those for certificate, identity, and card management, database encryption, and web servers

## SCALABLE AND COST-EFFECTIVE PROTECTION

Security World, the nShield key management system, enables the option of sharing keys across HSMs.

- Business continuity: Resilient hardware with hot-swap power supplies and redundant fans to keep your PKI running. HSMs can be clustered for load balancing
- Virtualization: The use of virtualization in data centers introduces new security concerns. nShield HSMs protect keys for virtual servers to prevent key proliferation
- Low cost of operations: Key backups can be carried out remotely and automatically
- High performance: Hardware acceleration helps avoid bottlenecks for Axway VA Server or high-volume CAs
- Shared resource: Network-attached nShield Connect HSMs can concurrently service many different applications, in addition to PKIs

For more information, visit [www.ncipher.com](http://www.ncipher.com) and [www.axway.com](http://www.axway.com)

Search: nCipherSecurity



©nCipher - May 2020 • PLB9324

[www.ncipher.com](http://www.ncipher.com)

