Enhanced security, speed and compliance for Axway Validation Authority Server

Thales nShield hardware security modules protect cryptographic keys for the Axway VA Server, accelerate operations, and achieve compliance with FIPS and Common Criteria.

BENEFITS:

- Protects the VA digital certificates that in turn validate the organizational digital certificates issued by a CA
- Boosts performance in environments that experience a 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+
- Assures business continuity through high-availability hardware
- Many joint reference implementations

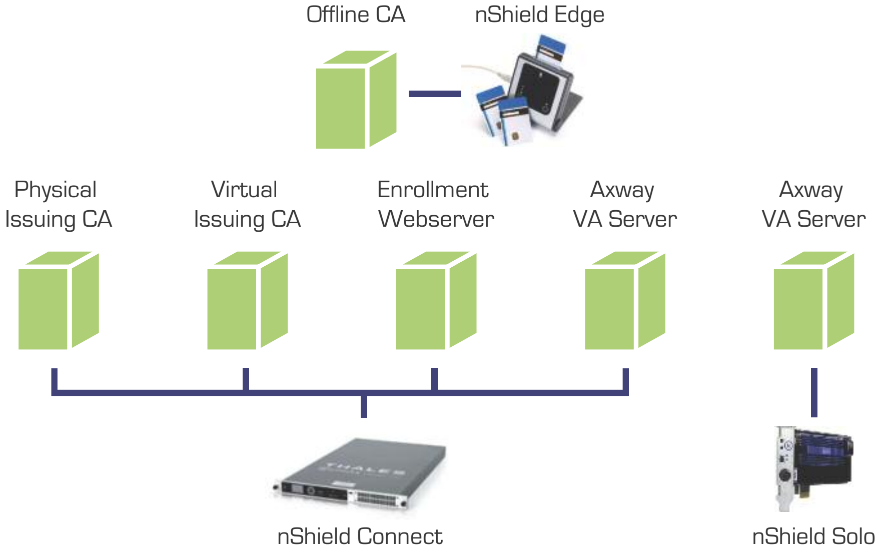
Assuring the validity of digital identities

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, 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.

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. Thales nShield hardware security modules (HSMs) integrate with Axway VA Server to protect keys, accelerate these operations, and add FIPS-compliant key management. nShield HSMs can:

- Protect the OCSP, 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+



Passing audits and achieving compliance

HSMs are considered an industry best practice to protect cryptographic keys. Many security policies and regulations recommend key management practices that are easiest fulfilled with HSMs, such as:

- Protect cryptographic keys in tamper-resistant hardware
- Store keys in fewest possible locations and forms
- Require dual control for key use
- Use FIPS 140-2 and Common Criteria validated key storage

By using HSMs, organizations achieve compliance, ensuring smooth audits, and raising the overall security assurance of their solution.

Protects PKI with trusted security

Validated to some of the highest security standards, nShield HSMs protect 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 nShield HSMs increase security assurance for high-value applications

Dual control administration and operation

nShield HSMs enforce your security policy to increase security and enable you to easily demonstrate compliance to auditors.

- Dual control with two-factor authentication: A quorum of administrators (k of n) may be 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 Operator: Remotely present operator credentials to HSMs in other locations, reducing travel needs.

Recommended Thales products

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

- nShield Solo: Embedded HSM with PCI or PCI Express interface 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: Thales publishes integration guides with fully tested integrations for quick deployment on Windows Server.
- 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: The network-attached nShield Connect can concurrently service many different applications, in addition to PKI.

For more information, visit www.thalesgroup.com/iss

Thales Information Technology Security

Americas: 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Unit 4101 41/F 248, Queen's Road East, Wanchai, Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa: Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com