Axway Validation Authority Suite

Secure applications with PKI safeguards

The Federal Government relies on public key infrastructures (PKIs) to secure everything from mission-critical networks, to military facilities and public infrastructure, to multi-million dollar electronic transactions. Within these PKI environments, protecting high-value assets — whether sensitive defense data, contractor communications, or military installations — requires both vigilance and diligence.

Axway Validation Authority (VA) Suite offers a comprehensive, scalable, and reliable framework for real-time validation of digital certificates and access permissions within PKI environments. VA Suite is Certificate Authority (CA)-neutral and provides support for multiple CAs, several different trust models, and CA-specific validation policies.

Axway VA Suite is:

- **Vigilant** in determining whether people are who they say they are and if their digital certificates are valid and current.
- **Diligent** in verifying which secure applications, networks, and locations the owner of a valid digital certificate is authorized to access at any given point in time.

VA Suite key features and benefits

For flexible and robust certificate validation, Axway Identity Validation Suite is CA-neutral and supports all widely adopted international security standards and open technologies:	• Certified to meet Common Criteria (EAL 3), FIPS 201, NIST PDVAL, FIPS 140-2, and DoD JITC standards • OCSP and SCVP compliant (RFC 2560, RFC 5055) • Entrust-ready and IdenTrust-compliant • Part of the IdenTrust, SWIFT Trust Act, BACS, and Global Trust Authority financial trust infrastructures • Interoperable with leading cryptographic hardware, including smart cards like the DoD Common Access Card and the Federal Personal Identity Verification Card or national eID-card, as well as products certified to FIPS 140-2 Level 3
Next-generation certificate validation Identifying invalid or revoked digital certificates is just the tip of the PKI iceberg. Beneath the surface, a secure PKI also needs to:	• Know which applications and/or network locations a user is authorized to access • Enforce the user's level of access and any agency policies that apply to the user's account • Federate the user's physical access rights across multiple buildings and/or geographic locations • Provide visibility into the what, where, and when of each and every instance of the user's physical and logical access

Standards support

OCSP (RFC 2560)
IPv6 and IPv4
SCVP (RFC 5055)
SSL 3.0, TLS 1.2
X509v3 digital certificate format
CRLv2 and delta CRL revocation data
LDAP(S), FTP, HTTP(S) CRL retrieval
SNMP and HTTPS administration
RSA PKCS#1,#7,#10,#11
RSA SHA-1, SHA-256. SHA-512 and MD5
Microsoft Cryptographic API
ECC prime 256,384
ECCDSA

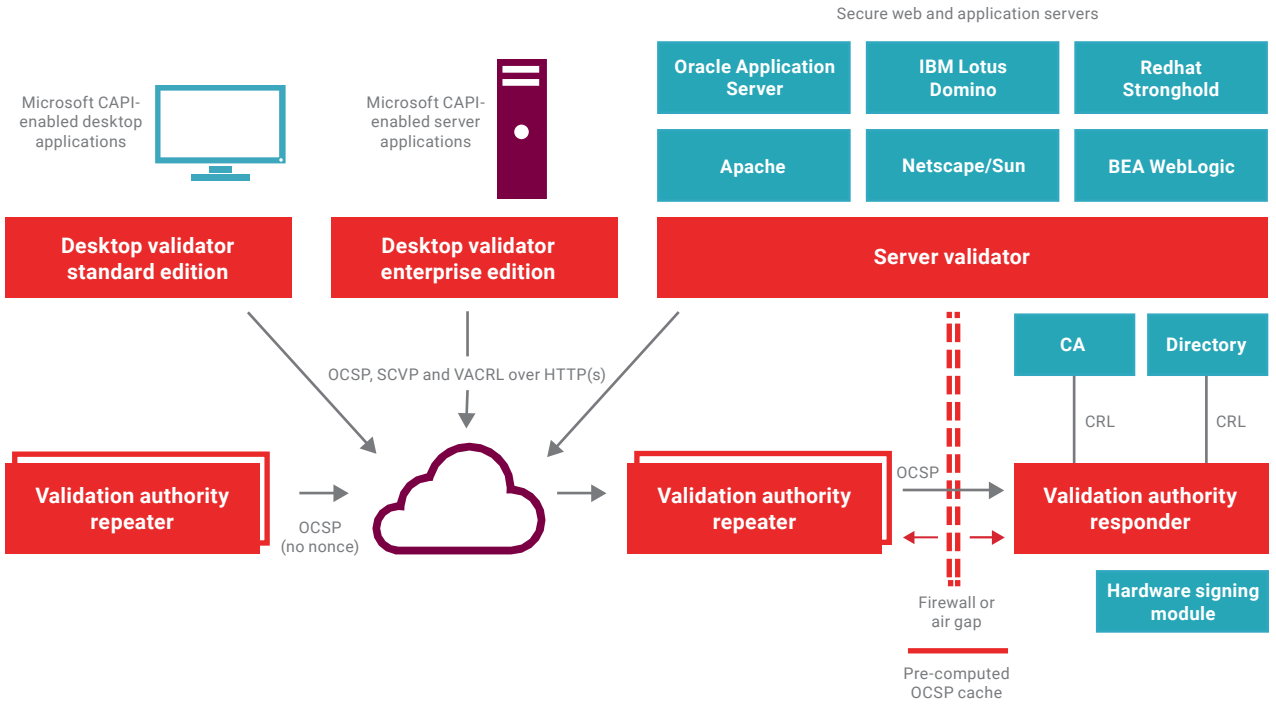
Axway Validation Authority Suite Components

Validation Authority Server. High-performance, multi-platform server that processes client digital certificate status queries using a variety of protocols, including OCSP, SCVP, CMP, and VACRL

Server Validator. Flexible client application for validating digital certificates from the most widely used secure web servers and web application servers

Desktop Validator. Flexible client application that allows Microsoft Windows-based desktop and server applications to validate digital certificates via the Microsoft Cryptographic API (CAPI)

Validator Toolkits. Complete set of certificate validation functions, source code examples, and reference manuals that enables certificate validation integration into COTS or custom applications developed in C/C++ or Java



Axway VA Suite Server-based Certificate Validation Protocol (SCVP) technologies let applications delegate both revocation-checking and path validation to a trusted server in a single request.

SCVP enables harvesting of an entity's credentials for the full range of access rights, cross-validated across multiple certificate chains by highly accredited certification issuers.

The most widely deployed validator of digital certificates

Axway VA Suite is widely deployed across the DoD and other government agencies. It consists of several components that provide a flexible and robust certificate validation solution for both standard and custom desktop and server applications. These components can be used together or, leveraging open standards, integrated with existing solutions using OCSP or SCVP (RFC 5055).

VA Suite offers cost-effective scalability across a wide range of operational environments, with support for caching and replication of revocation data, regardless of format. The Department of Homeland Security uses Axway VA for up to 350,000 users across its organization, helping secure and support cross-agency collaboration.

VA server key features and benefits

VA-to-VA mirroring (replication)	• Supports backup, load balancing, and failover by replicating the same certificate revocation data across a cluster of VA Servers
Distributed repeater-responder caching	• Maintains a cache loaded with OCSP responses that are precomputed or dynamically built up by proxy client requests to a responder • Supports non-OCSP clients or clients that want to maintain their own revocation data caches for backup and in low-bandwidth and non-real-time environments, such as Naval operations or first responders
Robust security and non-repudiation	• Supports SSL-based communications with clients, digitally signed client requests/responses, and digitally signed XML logs and CRL archives, as well as SSL-based server administration • Supports software, PKCS #11, and CAPI token-based hardware signing and encryption products from all leading vendors

VA Server

Prevent revoked credentials from being used for secure email, smart card login, network access (including wireless), or other sensitive electronic transactions with VA Server — a sophisticated digital certificate status responder and the core of Axway VA Suite.

To validate a digital certificate, a client application can simply query the VA Server rather than perform the cumbersome task of obtaining and processing the entire Certificate Revocation List (CRL) every time it encounters a digital certificate. That's because VA Server maintains a store of digital certificate revocation data by obtaining the CRL from the issuing CA.

Client applications can query VA Server using various open standard protocols (OCSP, SCVP, CMP, VACRL), allowing them to delegate the entire certificate validation operation — including path construction and intermediate CA validation — to the VA Server.

For tactical environments, or where bandwidth is limited, VA Server also supports protocols like Compact CRL and VACRL. The server can convert

CA-issued CRLs — which can be over 40 MB for mature PKIs — into revocation data with a much smaller footprint.

VA Server Validator

VA Server Validator is a flexible client application that allows digital certificate validation on the most widely used secure web and application servers available on UNIX, Windows, and Apple platforms, including:

- Apache
- Oracle Application Server

VA Server Validator uses the native interfaces of these web and application servers to add digital certificate validation functionality as part of the product's PKI-based client authentication. Working as a plug-in, VA Server Validator can query a VA Server (or any other standards-based digital certificate validation responder) or utilize a CRL to determine the status of a digital certificate presented by a client. Clients with revoked or expired certificates are denied access to the server or application.

Server validator and desktop validator key features and benefits

Robust security and non-repudiation	• Processes CRL data from multiple CA or VA sources to support complex trust models and certificate policy controls for path processing and policy enforcement • Performs end-to-end certificate validation if one or more intermediate CAs are used and the validation policy requires a complete certificate chain validation • Communicates securely with VA Server utilizing SSL/TLS and digitally signs requests to VA Server for deployments requiring a high degree of auditability and non-repudiation • Supports cryptographic hardware via the standard PKCS #11 interface, including FIPS 140-2 Level 3 and 4, which can be used to accelerate digital signing and SSL/TLS operations
Separate, configurable validation caches	• Provides in-memory repository of all certificate validation requests, regardless of the validation mechanism • Supplies disk-resident CRL repository • Improves performance and increases reliability in environments where the underlying network is not always available • Supports multiple sources of revocation information, including multiple VA Servers, via robust failover mechanism
Automatic configuration	• Supports automatic configuration using parameters obtained from the VA Server if the web or application server supports auto-configuration • Facilitates large-scale application deployments

System Specifications

Delivery options
Software application

Platforms
(64-bit support)
Sun Solaris 10
Red Hat Linux 5, 6
Windows 2003, 2008, 2012, XP, Vista and Windows 7

Cryptographic hardware
(FIPS 140-2 Levels 2, 3 &4)
Thales
SafeNet
AEP Networks

Load balancers
Cisco CSS and CSM
Foundry BigIron
F5 Big IP
Resonate Dispatch

VA Desktop Validator

VA Desktop Validator is a flexible client solution that allows digital certificate validation in the most commonly used Microsoft Windows-based desktop and server applications. VA Desktop Validator integrates seamlessly with any Microsoft CAPI-compliant client or server application.

- Validates digital certificates encountered by PKI-enabled Windows applications via CRL lookups or standard protocol queries to a VA Server or other OCSP or SCVP standards-based responder
- Provides high availability and can be remotely installed, configured, and maintained using applications like Microsoft SMS, CA Unicenter, or Microsoft Active Directory
- Supports single sign-on applications based on digital certificates stored on smart cards like the DoD Common Access Card or Federal PIV card
- Facilitates secure workflow applications based on digitally signed documents and secure email (S/MIME) messages

VA Validator Toolkits

VA Validator Toolkits supplies a complete set of certificate validation functions, source code examples, and reference manuals. The VA Validator Toolkits can save development time and money for agency PKI-enabled applications like network and handheld devices, physical security systems, and workflow applications.

VA Validator Toolkits encapsulates the complexities of PKI digital certificate validation in a three-step process that developers can implement through easy-to-understand C/C++ and Java interfaces. VA Validator Toolkit for C/C++ is certified DOD JITC, IdenTrust, and FIPS 140-2 Level 1 compliant. These credentials save agencies and contractors the time and cost of additional testing and certification. The VA Validator Java Toolkit uses third-party Java security providers to execute cryptographic functions.

axway.com/en/enterprise-solutions/validation-authority

AXWAY_DS_AXWAY-VA-SUITE_EN_101217