

# Axway Validation Authority Suite

## PKI safeguards for secure applications



Around the world, banks, healthcare organizations, governments, and defense agencies rely on public key infrastructures (PKIs) to secure everything from enterprise networks, to multi-million dollar electronic transactions, to military facilities. Within these PKI environments, protecting high-value assets — whether they are product plans, financial data, patient records, or physical locations — 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 & Benefits

#### 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 products certified to FIPS 140-2 Level 3 and 4, as well as smart cards such as the DoD Common Access Card and the Federal Personal Identity Verification Card or national eID-card



**Standards Support**

OCSP (RFC 2560)  
 SCVP (RFC 5055)  
 SSL 2.0, 3.0, TLS 1.0  
 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  
 CAs and CRLs using ECC keys

**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 (“John”) is authorized to access;
- Enforce John’s level of access and any enterprise policies that apply to his account;
- Federate John’s physical access rights across multiple buildings and/or geographic locations; and
- Provide visibility into the “what, where, and when” of each and every instance of John’s physical and logical access.

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

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

**Axway VA Suite**

The most widely deployed validator of digital certificates

Axway VA Suite consists of several components that provide a flexible and robust certificate validation solution for both standard and custom desktop and server applications. These components may be used together or, leveraging open standards, integrated with existing solutions using OCSP or SCVP (RFC 5055).

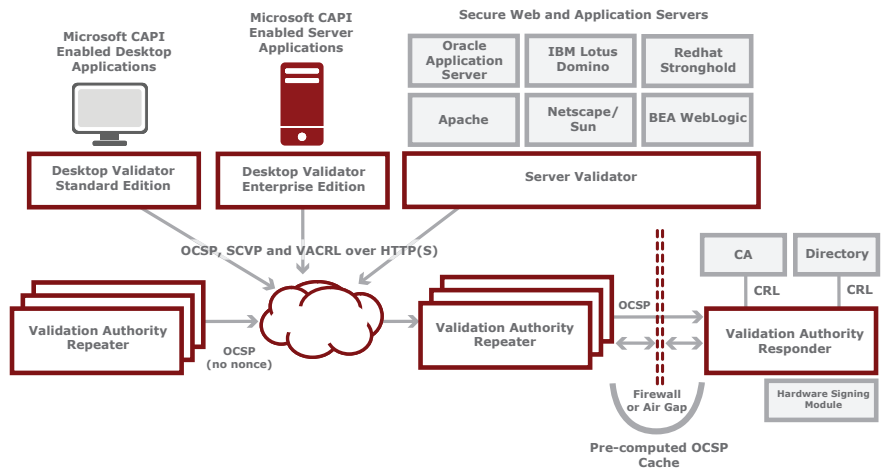
**Axway Validation Authority (VA) Suite**

**Validation Authority Server**, a 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**, a flexible client application for validating digital certificates from the most widely used secure Web servers and Web application servers

**Desktop Validator**, a flexible client application that enables Microsoft Windows-based desktop and server applications to validate digital certificates via the Microsoft Cryptographic API (CAPI)

**Validator Toolkit**, a complete set of certificate validation functions, source code examples, and reference manuals that enables certificate validation integration into commercial or custom applications developed in C/C++ or Java



With support for caching and replication of revocation data regardless of format, VA Suite enables cost-effective scalability across a wide range of operational environments, including hardware-software appliance and Java-based solutions for distributed or hosted environments.



## VA Server

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

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

Client applications can query VA Server utilizing various open standard protocols (OCSP, SCVP, CMP, VACRL), which allows 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 that allow the server to convert CA-issued CRLs — which can be as large as 40+ MB for mature PKIs — into revocation data that has a much smaller footprint.

VA Server Key Features & Benefits	
<b>VA-to-VA mirroring (replication)</b>	<ul style="list-style-type: none"><li>▪ Supports backup, load balancing, and failover by replicating the same certificate revocation data across a cluster of VA Servers</li></ul>
<b>Distributed repeater-responder caching</b>	<ul style="list-style-type: none"><li>▪ Maintains a cache loaded with OCSP responses that are pre-computed or dynamically built up by proxy client requests to a responder</li><li>▪ 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</li></ul>
<b>Robust security and non-repudiation</b>	<ul style="list-style-type: none"><li>▪ 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.</li><li>▪ Supports software, PKCS #11, and CAPI token-based hardware signing and encryption products from all leading vendors</li></ul>

## VA Server Validator

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

- Microsoft ISA
- Apache
- Oracle Application Server
- Red Hat Strong Hold
- BEA WebLogic
- IBM Lotus Domino

VA Server Validator utilizes 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.

## VA Desktop Validator

VA Desktop Validator is a flexible client solution that enables digital certificate validation in the most commonly used Microsoft Windows-based desktop and server applications. VA Desktop Validator integrates seamlessly with any Microsoft Cryptographic API (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.
- Is highly available and can be remotely installed, configured, and maintained using applications such as Microsoft SMS, CA Unicenter or Microsoft Active Directory.
- Supports single sign-on applications based on digital certificates stored on smart cards such as the DoD Common Access Card.
- Enables secure workflow applications based on digitally signed documents and secure email (S/MIME) messages.



**Server Validator & Desktop Validator Key Features & Benefits**

<b>Robust security and non-repudiation</b>	<ul style="list-style-type: none"> <li>Processes CRL data from multiple CA or VA sources to support complex trust models and certificate policy controls for path processing and policy enforcement</li> <li>Performs end-to-end certificate validation if one or more intermediate CAs are used and the validation policy requires a complete certificate chain validation</li> <li>Communicates securely with VA Server utilizing SSL/TLS, and digitally signs requests to the VA Server for deployments that require a high degree of auditability and non-repudiation</li> <li>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</li> </ul>
<b>Separate, configurable validation caches</b>	<ul style="list-style-type: none"> <li>In-memory repository of all certificate validation requests, regardless of the validation mechanism</li> <li>Disk-resident CRL repository</li> <li>Improves performance and increases reliability in environments where the underlying network is not always available.</li> <li>Robust failover mechanism supports multiple sources of revocation information, including multiple VA Servers</li> </ul>
<b>Automatic configuration</b>	<ul style="list-style-type: none"> <li>Supports automatic configuration using parameters obtained from the VA Server if the Web or application server supports auto-configuration</li> <li>Facilitates large-scale application deployments</li> </ul>

**VA Repeater Appliance and Repeater Servlet**

VA Repeater Appliance is a hardware-software appliance solution that can be installed in less than 30 minutes, and delivers the lowest total cost of ownership for distributed computing environments.

VA Repeater Servlet provides a lightweight solution for deploying a high-scale, high-reliability digital certificate infrastructure that leverages the platform independence of Java.

**VA Validator Toolkit**

VA Validator Toolkit provides a complete set of certificate validation functions, source code examples and reference manuals. The VA Validator Toolkit can save development time and money for commercial or custom PKI-enabled applications, such as network and handheld devices, physical security systems and workflow applications.

The VA Validator Toolkit 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. The VA Validator Toolkit is certified DOD JITC, IdenTrust and FIPS 140-2 Level 1 compliant. These credentials save organizations the time and cost of additional testing and certification.

**Learn More**

To learn more about how Axway Validation Authority Suite can provide your organization with a comprehensive, scalable and reliable framework for real-time validation of digital certificates and access permissions within PKI environments, email us at [axwaysolutions@axway.com](mailto:axwaysolutions@axway.com), or visit us at [www.axway.com/contact-us](http://www.axway.com/contact-us).

**System Specifications****Delivery options**

Hardened Linux appliance  
Virtualization (VMware)  
Hosted or managed service

**Platforms****(32 and 64-bit support)**

Sun Solaris 10  
Red Hat Linux 5  
Axway Appliance (Windows and Linux)  
Apple OS X  
Windows 2003, 2008, XP Vista and  
Windows 7

**Cryptographic Hardware****(FIPS 140-2 Levels 2, 3 &4)**

Thales  
AEP Systems  
SafeNet  
Eracom

**Load Balancers**

Cisco CSS and CSM  
Foundry BigIron  
F5 Big IP  
Resonate Dispatch



