VALUE DRIVER SERIES | FLYER

**IF YOU'RE A:**

- CIO
- Director of IT Services
- Director of Identity and Access Management
- Director of PKI Services

**WHO NEEDS TO:**

- Validate digital certificates reliably and rapidly
- Gain centralized management of digital certificate validation with granular control
- Ensure built-in failover and redundancy

**BUT CURRENTLY:**

- Certificate validation sometimes fails, blocking user logins and apps
- Some networks can't validate certificates, so they're still using login/password
- Servers have backdoor logins, because certificate authentication isn't reliable

**THEN:**

It's time to transform your PKI infrastructure into a secure and reliable engine of trust with Axway Validation Authority.

axway.com

# Safeguard mission-critical PKIs with Axway Validation Authority

## Validate digital certificates rapidly with High Availability and data from local sources

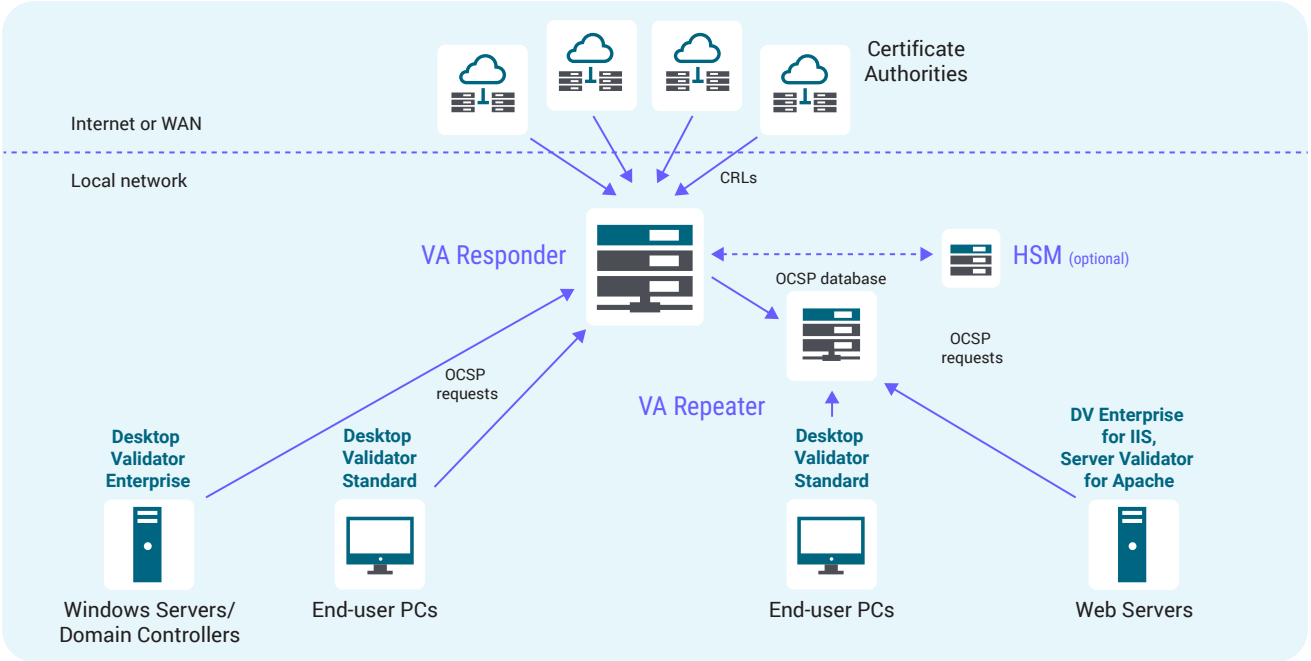
Certificate validation is a requirement of the digital trust landscape, but is too often an obstacle to user productivity. Axway Validation Authority (VA) Suite offers a comprehensive, scalable, and reliable solution for rapid validation of digital certificates within public key infrastructure (PKI) environments.

Axway Validation Authority is certificate-authority (CA) agnostic and provides support for multiple CAs, several different trust models, and CA-specific validation policies. As online transactions and data exchange soar, you face heightened risks from sophisticated cyberthreats and evolving compliance demands. Axway Validation Authority steps in as the guardian of your environment, ensuring the validity and authenticity of digital certificates and safeguarding PKI operations, rapidly and reliably.

90% of federal agencies have adopted PKI technologies to secure their communications and data exchanges[1]

1 GDIT Research, November 2022

**Axway Validation Authority (VA) Suite components**




*Axway VA Suite offers cost-effective scalability across a wide range of desktop and server environments.*

## Move beyond depending on remote validation sources

Reliance on traditional PKI validation at the Certificate Authority creates operational delays, reliability uncertainties, and even network congestion — all critical issues in high-stakes environments like today's federal government operations. This results in:

- **Failed or delayed smartcard authentication.** Users are unable to log in to their systems because their digital certificates can't be validated.
- **Failed or delayed encryption/signing operations.** Signed messages are blocked because the signing certificate can't be validated.
- **Network congestion/slowdown.** All end devices start downloading full Certificate Revocation Lists (CRLs) because the CA's OCSP Responders are down.
- **Compliance violations.** The certificate validation reliability forces a reversion to login/password operations.

Addressing these issues requires a solution that provides instant, reliable validation of digital certificates, while also providing centralized management of CA-specific requirements, automatic failover steps, and depth of required logging.

Move beyond the limitations of remote CA-based certificate validation and bandwidth-hogging CRLs with Axway Validation Authority (VA) Suite. It offers local rapid validation of digital certificates, delivering:

- **Instant validation.** OCSP and SCVP requests are handled by a local Responder.
- **Enhanced security.** Rapid and reliable certificate validation enables you to eliminate login/password access.

By implementing Axway VA Suite, you transform your PKI environment from a vulnerable bottleneck into a secure, efficient engine of trust. You gain reliable smartcard authentication, increased user productivity, and more efficient operations. It's not just about validation, it's about establishing your secure digital foundation for the future.

## Flexible component architecture to fit your needs

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. You can use these components together or separately to support a myriad of different PKI architectures.

### VA Server: Responder and Repeater

Prevent revoked credentials from being used for smart card authentication, digital signing, and digital encryption with Axway VA Server. The sophisticated but automated Axway OCSP Responder is the core of the Axway VA software suite. Additional VA Servers can be deployed as Axway OCSP Repeaters to support large and/or distributed workloads and high availability.

### VA Desktop Validator

VA Desktop Validator (DV) is a flexible client solution that allows digital certificate validation in the most commonly used Microsoft Windows-based desktop and server applications. The VA DV series are clients that sit on Windows Desktops (DV Standard) and Servers (DV Enterprise) to enhance the operating system's validation capabilities and integrates seamlessly with any Microsoft CAPI-compliant client or server application.

### VA Server Validator

VA Server Validator (SV) is a flexible client application that provides digital certificate validation for Apache Web Server running on Windows Server or RHEL. VA Server Validator uses the native interfaces of the server to add digital certificate validation functionality as part of the product's PKI-based client authentication.

### VA Validator Toolkit Java

VA Validator Toolkit Java supplies a complete set of certificate validation functions, source code examples, and reference manuals. The VA Validator Toolkit can save development time and expense for any application that needs to include PKI capabilities.

45% reduction in security breaches achieved by organizations using PKI to stop unauthorized access or data exfiltration[1]

1 Government Business Council, 2023 Cybersecurity Survey

## Axway VA Suite: Key features and benefits

Axway VA Suite delivers business and technical advantages that have earned it wide adoption across the U.S. DOD and other federal agencies. These include:

| | |
|---|---|
| Comprehensive VA solution | • One-stop shop for organizations seeking a reliable, rapid, and centralized approach to certificate validation<br>• Supports all appropriate international security standards and open technologies<br>• Robust local OCSP and SCVP Responder, Repeater, and client functionalities eliminate need for CRL downloads to every local device |
| Scalability and reliability | • Handles high volumes of validation requests with potentially zero downtime<br>• Distributed architecture and fault tolerance features make it ideal for mission-critical deployments |
| Flexibility and integration | • Integrates seamlessly with existing PKI environments<br>• Supports various protocols, including OCSP, SCVP, CRL, and proprietary low-bandwidth protocols<br>• Caters to diverse validation needs and simplifies deployment<br>• API interfaces support programmatic integration |
| Ease of administration and expansion | • Intuitive interface and easy administration speed adoptions and reduce burdens on IT<br>• Ability to export and import configurations simplifies deployment of additional components |
| Advanced monitoring and reporting | • Provides comprehensive insights into validation activity<br>• Enables troubleshooting and compliance reporting |
| Support for distributed coverage and High Availability | • Responder and Repeater software enable digital certificate validation over a wide geographical area while also supporting High Availability for mission-critical requirements |
| High Availability on the client side | • Desktop Validator for Windows and Server Validator for Apache Web Server support failover options to multiple certificate revocation information sources<br>• These clients also can extend the life of CRL info for isolated networks |

80% of federal agencies implementing PKI and digital certificates achieved full compliance with the Homeland Security Presidential Directive 12 (HSPD-12)[1]

## Why choose Axway for Certificate Validation?

Axway offers dedicated customer support and professional services to assist your agency in deploying, customizing, and managing VA infrastructure. Seamless integrations streamline workflows, user-friendly interfaces empower all, and Axway's renowned service ensures a smooth journey.

Working with Axway, you can embrace PKI transformation with confidence. Partner with Axway VA Suite to protect your PKI landscape, on your terms, for rapid validation of digital certificates and unparalleled digital trust.

### Ensuring always-on access to global procurement services

The Defense Logistics Agency (DLA) manages the global defense supply chain for the U.S. military, other federal agencies, and partner and allied nations. For over 20 years, the DLA has trusted Axway Validation Authority for validation of digital certificates for millions of these users, ensuring that they're able to use their CAC/PIV smartcards to access DLA's critical web applications rapidly and reliably.

> *"Because we support millions of stakeholders, we need a solution that can validate certificates reliably, at speed and scale. That's exactly what Axway Validation Authority lets us do.*
>
> Joe Sergewich, PKI Engineer
> at Defense Logistics Agency

99.99% availability for public key infrastructure

Millions of low latency requests per year

24/7 access to mission-critical systems

**Read the case study →**

1 National Institute of Standards compliance report, June 2020

## Ready to transform your PKI environment for instant trust?

**Start here →**