



Validation Authority™ Server Validator

Banks, governments, and businesses worldwide rely on their Public Key Infrastructure (PKI) to secure their mission-critical web-based applications. Trusting an invalid certificate exposes an organization to potential fraud, theft, and compromise. Organizations rely on the Tumbleweed Validation Authority™ Server Validator to safeguard their PKI enabled web-based applications against expired, revoked, or otherwise invalid digital certificates.



PKI enabled systems depend on digital certificates, electronic credentials issued by a certificate authority (CA), to establish identity and trust. However, digital certificates alone are not enough to ensure the integrity of PKI solutions. Electronic credentials like passports, credit cards, security badges, and other physical credentials, can become expired, revoked, or otherwise invalid over time. Similar to point of sale credit card authorizations, digital certificate status must be validated whenever the certificate is to be trusted.

The **Tumbleweed Validation Authority™ (VA)** suite offers a comprehensive, scalable, and reliable framework for real-time validation of digital certificates. VA is a proven, fourth-generation solution that has been deployed by hundreds of customers worldwide for over eight years. Customers include the US Department of Defense, all branches of the US military, the Department of Homeland Security, US Intelligence communities, and top financial institutions globally.

The VA suite consists of several products for flexible, cost-effective, and robust solutions ideally suited to a wide range of client applications in diverse operating environments. At the core of the VA suite is the **Tumbleweed Validation Authority™ (VA Server)**, a sophisticated digital certificate status responder. Another essential part of the VA solution, **Server Validator (SV)**, is a multi-platform client solution for enabling digital certificate validation in commonly used web based application server environments.

SV utilizes native interfaces in leading web application servers to add digital certificate validation functionality for that product's PKI based client authentication. SV queries a VA Server (or any standards based digital certificate validation responder) or utilizes a Certificate Revocation List (CRL) to determine the status of a digital certificate presented by a client. Clients with revoked or expired certificates are denied access to the application. SV offers additional advanced features for high performance, availability, and ease of administration.

CERTIFICATIONS

- Common Criteria
- FIPS 201
- NIST PDVAL
- FIPS 140-2
- DOD JITC
- Entrust-Ready
- IdenTrust Compliant



FEATURES

- A multi-platform client solution for enabling PKI digital certificate validation in the most commonly used web based application server environments.
- Utilizes native interfaces in application servers to ensure that digital certificates are validated when authenticating clients.
- Supports multiple trust models, validation policies using standards-based digital certificate validation protocols including OCSP and SCVP as well as Tumbleweed's VACRL protocol.
- Maintains an in-memory cache of all certificate validation responses, regardless of the validation mechanism used, and a disk-resident CRL cache, which can be tuned for maximum performance and availability.
- Secure SSL/TLS communication with VA Server and ability to sign validation queries for non-repudiation as well as robust fail-over mechanism for querying multiple VA Servers.
- Robust administration through native user interfaces as well as auto configuration via the VA Server to facilitate large scale deployments.

Validation Authority™ Server Validator

The Tumbleweed Server Validator (SV) leverages native web and application server interfaces and is installed as a “plug-in”, ensuring the server does not accept revoked or expired certificates while performing client authentication (establishing a secure channel with a client).

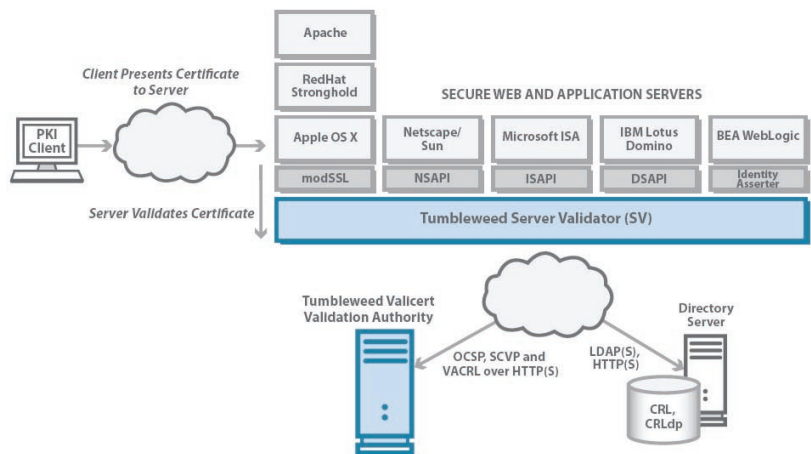
SV enables digital certificate validation via standard protocol queries to a VA Server (or other OCSP or SCVP standards based responder) or by CRL lookups. SV improves digital certificate validation’s reliability and performance by using the VA Server and the Tumbleweed VACRL protocol to distribute CA or VA manufactured CRLs and delta CRLs to SV enabled application servers.

SV is CA neutral and can support CRL data from multiple CA or VA sources. SV can support complex trust models and supports RFC 3280 certificate policy controls for path processing and policy enforcement. SV will perform end-to-end (complete) certificate validation if one or more intermediate CA’s are used, and the validation policy requires end-to-end (complete) certificate chain validation.

SV can communicate securely with the VA Server by utilizing SSL/TLS. SV supports different trust models and can support validation of the VA Server certificate. SV can also digitally sign requests to the VA server for deployments that require a high degree of audit and non-repudiation. SV offers support for cryptographic hardware via the standard PKCS #11 interface, including FIPS 140-2 Level 3 and 4, which can be used to accelerate digital signing.

SV provides support for two separate, configurable validation caches. One is an in-memory repository of all certificate validation responses, regardless of the validation mechanism used. The other is a disk-resident CRL repository. Caching parameters, including the time-to-live of response and the total size of the cache, are flexible to meet the requirements of a specific deployment. Caching can be used to improve performance and increase reliability in environments where the underlying network is not always available. SV also offers a robust fail-over mechanism for querying multiple VA Servers.

SV can be automatically configured using parameters obtained from the VA Server. This integration between the SV and the VA Server greatly facilitates the operation of SV in a large-scale application deployment.



KEY BENEFITS

- Ensures mission-critical web applications do not rely on invalid digital certificates.
- High-performance, high-availability solution with support for multiple digital validation mechanisms and high scale deployments.
- Open standards based – easy to integrate, easy to evolve – and commercially integrated with numerous partner applications.

SYSTEM SPECIFICATIONS

Web Servers/ Platforms	<ul style="list-style-type: none"> • Apache Windows 2000/2003, Linux, Solaris, Apple OS X • BEA WebLogic Windows 2000/2003, Linux, Solaris, Apple OS X • IBM Lotus Domino Windows 2000/2003, Linux, Solaris, AIX • Microsoft ISA Windows 2000/2003 • Sun/Netscape Windows 2000/2003, Linux, Solaris • Oracle Application Server Windows 2000/2003, Linux, Solaris
---------------------------	---

Cryptographic Hardware	<ul style="list-style-type: none"> • nCipher • AEP Systems • SafeNet • Eracom
---------------------------	---

Load Balancers	<ul style="list-style-type: none"> • Cisco CSS and CSM • Foundary BigIron • F5 Big IP • Resonate Dispatch
----------------	---

Standards	<ul style="list-style-type: none"> • OCSP (IETF RFC 2560) • SCVP (IETF Draft) • SSL 2.0, 3.0, TLS 1.0 • X509v3 digital certificate format • CRLv2 and delta CRL revocation data • LDAP(S), HTTP(S) and file based CRL retrieval • RSA PKCS#1, #7, #11 • RSA SHA-1 and MD5
-----------	---



California, USA
Corporate Headquarters
Tumbleweed Communications Corp.
700 Saginaw Drive
Redwood City, CA 94063

New York, USA
Tumbleweed Communications Corp.
245 Park Ave, 24th Floor
New York, NY 10167

United Kingdom
Tumbleweed Communications Ltd.
Hurst Grove, Sanford Lane
Hurst, Berkshire RG10 OSQ
UK

APAC
Tumbleweed Communications
Centennial Tower, Level 21
3 Temasek Avenue
Singapore 039190

© 2007 Tumbleweed Communications Corp. All rights reserved. Tumbleweed is a registered trademark and Tumbleweed Validation Authority is a trademark of Tumbleweed Communications Corp. All other brand names are the trademarks of their respective owners.
04/07

Phone: 650-216-2000/800-696-1978
www.tumbleweed.com

Phone: 212-209-7363/800-696-1978
www.tumbleweed.com

Phone: +44 (0)118 934 7100
www.tumbleweed.com

Phone: 65-65497143
www.tumbleweed.com