

Tumbleweed Validation Authority™ Suite

Banks, governments, and businesses worldwide rely on their Public Key Infrastructure (PKI) and digital certificates to secure everything from corporate network access to multi-million dollar electronic transactions to physical access of military facilities. Trusting an invalid certificate can expose an organization to potential fraud, theft, and compromise. Organizations rely on the **Tumbleweed Validation Authority™ Suite**, the leading identity validation solution, to protect the integrity of their PKI. Digital certificate validation enables organizations to maximize their return on investment by ensuring their PKI safeguards all their secure applications.

FEATURES

- High-performance, high-availability VA Server for responding to digital certificate validation requests, offering numerous advanced features to address the requirements of diverse deployment environments.
- Flexible multi-platform client solutions enabling digital certificate validation in both commonly used and custom developed desktop and server applications.
- Supports multiple standards based digital certificate validation protocols including OCSP, SCVP, and CMP as well as Tumbleweed's VACRL protocol.
- Supports CA neutral CRL processing, offering support for different trust models and validation policies.
- Provides replication of revocation data, regardless of format, for mirroring to multiple VA Servers for load-balancing and failover.
- Provides caching of revocation data, regardless of format, enabling cost-effective scalability in a wide range of operational environments, including hardware-software appliance and Java based solutions for distributed or hosted environments.
- Secure SSL/TLS communication and support for digitally signed validation requests/responses for non-repudiation.
- Supports leading vendor cryptographic hardware, including FIPS 140-2 Level 3 and 4, to accelerate digital signing and SSL/TLS operations.
- Certified DOD JITC, Identrus, FIPS 140-1 Level-1 and Common Criteria compliant.

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)** 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 six 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 is CA neutral and supports numerous widely adopted international security standards and open technologies. VA is certified FIPS 140-1, DOD JITC, Identrus, and Common Criteria compliant, and is part of the Identrus, SWIFT Trust Act, BACS and Global Trust Authority financial trust infrastructures. The VA interoperates with cryptographic hardware, including FIPS 140-2 Level 3 and 4 devices as well as smart cards such as the DOD Common Access Card.

The VA suite consists of several products that provide a flexible, cost-effective, and robust solution ideally suited to client applications in diverse operating environments. At the core of the VA suite is the **Valicert Validation Authority**, a sophisticated digital certificate status responder. The VA suite also includes **Server Validator**, **Standard Desktop Validator**, **Enterprise Desktop Validator**, and the **Validator Toolkit**, which provide multiplatform client solutions enabling digital certificate validation in both commonly used and custom developed desktop and server applications.

Tumbleweed Valicert Validation Authority (VA Server)

A high-performance multi-platform server that processes client digital certificate status queries using a number of different protocols including OSCP, SCVP, and VACRL. The VA Server offers advanced features including support for multiple CAs, various validation trust models, CA-specific validation policies, VA-to-VA mirroring (replication) of CA and VA manufactured CRLs and delta-CRLs, distributed Repeater-Responder caching of pre-computed and dynamic OSCP responses. The VA Server provides robust non-repudiation features including digitally signed responses, digitally signed logs, and CRL archives. The VA Server also provides superior operational capabilities through the support of FIPS 140-2 Level 3 and Level 4 compliant cryptographic hardware, as well as robust monitoring, administration, and auditing.

Server Validator

A flexible client application for enabling digital certificate validation in the most widely used secure Web servers and Web application servers available on UNIX, Windows, and Apple platforms including Microsoft ISA, Apache, Oracle Application Server, Red Hat Strong Hold, BEA WebLogic, and IBM Lotus Domino, with support for automatic configuration and fail-over support through the use of multiple validation mechanisms.

Desktop Validator, Standard and Enterprise

Flexible client solutions for enabling Microsoft Windows based desktop and server applications to validate digital certificates via the Microsoft Cryptographic API (CAPI), including support for FIPS 140-2 Level 2 smart cards such as DOD Common Access Card, flexible default and CA specific validation rules, robust fail-over mechanism with multiple revocation data sources, remote management via Microsoft SMS, CA Unicenter, and Microsoft Active Directory. DV can also be automatically configured via the VA Server for ease of large-scale deployment.

Validator Toolkit

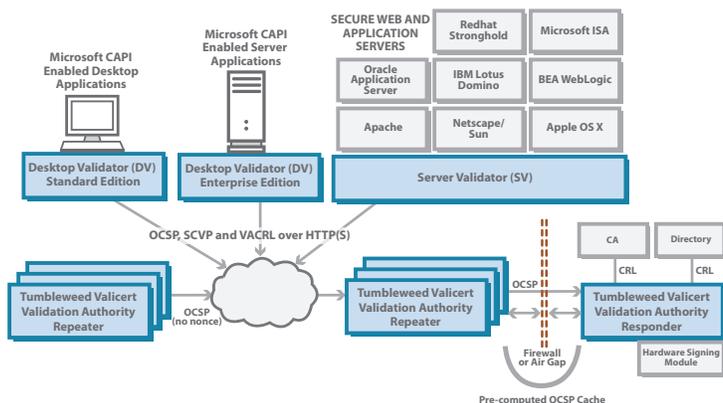
A complete set of certificate validation functions, source code examples and reference manuals that enables certificate validation integration into commercial or custom applications developed in C/C++ or Java such as network and hand-held devices, physical security systems, and custom PKI-enabled workflow applications.

Repeater Appliance and Repeater Servlet

Lightweight solutions for deploying a high-scale, high-availability digital certificate infrastructure based on an OSCP response cache that can be pre-computed or dynamically generated. These solutions do not contain any sensitive cryptographic material (since cached OSCP responses are generated by a VA Responder Server) and can easily reside in a different administrative domain than the VA Responder Server, making them ideal solutions for distributed computing environments or hosted application environments.

VA Publisher

A sophisticated component of the VA Server that aggregates revocation data from multiple CAs, files or directory servers for publishing to a VA Server, to other files, or even to other directory servers, and integrates with CA products to automatically push revocation information upon availability.



KEY BENEFITS

- Comprehensive, scalable, and reliable framework deployed by hundreds of customers worldwide to provide digital certificate validation on a wide range of platforms in diverse operating environments.
- Open standards based – easy to integrate, easy to evolve – and commercially integrated with numerous partner applications.
- High-performance client-server products with support for multiple digital validation mechanisms to ensure integrity of solution.
- Interoperable with numerous products and highly extensible through flexible, easy-to-use interfaces.



System Specifications

Platforms	<ul style="list-style-type: none"> • Microsoft Windows XP and 2000/2003 • Sun Solaris 2.7-2.10 • RedHat Linux • Tumbleweed Appliance • Apple OS X • IBM AIX
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"> • OSCP (IETF RFC 2560) • SCVP (IETF Draft) • CMP (IETF RFC 2510) • 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 HTTP administration • RSA PKCS#1, #7, #10, #11 • RSA SHA-1 and MD5 • Microsoft Cryptographic API

Tumbleweed Communications

California, USA

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

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

New York, USA

Tumbleweed Communications Corp.
14 Wall Street, 12th Floor
New York, NY 10005

Phone: 212-791-9450/800-696-1978
www.tumbleweed.com

United Kingdom

Tumbleweed Communications UK
Hurst Grove, Sandford Lane
Hurst, Berkshire RG10 0SQ
U.K.

Phone: +44 118 934 7100
www.tumbleweed.co.uk



© 2005 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.
04/05