

Tumbleweed Validation Authority™

Validator Toolkit

Banks, governments, and businesses world wide have invested in a Public Key Infrastructure (PKI) to secure everything from corporate network access, to multi-million dollar electronic transactions, to physical access of military facilities. To maximize their return on investment, organizations rely on the **Tumbleweed Validation Authority™ Validator Toolkit** for digital certificate validation in commercial or custom PKI enabled applications, protecting the integrity of their PKI solutions and safeguarding against potential fraud, theft, and compromise.

FEATURES

- A complete set of certificate validation functions, source code examples, and a reference manual to allow PKI application developers to validate digital certificates.
- Support for C/C++ and Java on numerous platforms proven in a wide range of commercial applications.
- High-level API with low-level client protocol support for OCSP, SCVP, CMP, CRL DP as well as support for CRL processing, allows developers to select the appropriate underlying validation method for their application.
- Provides developers with API functions for X509v3 certificate parsing and IETF RFC 3280 chain building to PKI enable their applications.
- Supports flexible VA trust model and customizable validation policies, greatly simplifying the development efforts faced by application developers dealing with the challenges of validation in complex PKI environments.
- Support for SSL, TLS and digest/basic authentication with proxy servers.
- Robust logging for troubleshooting and auditing.
- Certified Identrus, and FIPS 140-1 Level 1 compliant version available to save time and cost of testing and certification.

Electronic credentials like passports, credit cards, security badges, and other physical credentials, can become expired, revoked, or otherwise invalid over time. Digital certificates alone are not enough to ensure the integrity of PKI solutions. 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 digital certificate status checking. VA is a proven, fourth-generation solution deployed by hundreds of customers worldwide for over six years. Customers include the US Department of Defense (DOD), 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 Valicert Validation Authority™ (VA Server)** product, a sophisticated digital certificate status responder. Another essential part of the VA solution, the **Validator Toolkit (VTK)** product, is a client solution for enabling digital certificate validation in commercial or custom developed PKI enabled applications.

The VTK includes a complete set of certificate validation functions, source code examples, and reference manuals for integrating digital certificate validation into C/C++ or Java applications (for network and hand-held devices, physical security systems, and custom PKI-enabled workflow applications). The VTK saves development time and cost by abstracting the complexities of PKI digital certificate validation into a three step process which developers can implement through easy to understand C/C++ and Java interfaces.

The VTK supports a number of different digital certificate validation mechanisms including Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP), Simple Certificate Validation Protocol (SCVP), Certificate Management Protocol (CMP) as well as Tumbleweed's VACRL protocol, allowing developers to select the optimal solution for their application. Additionally the VTK supports several different validation trust models as well as specific validation policies.

Additionally the VTK has undergone extensive testing/evaluation and been certified Identrus and FIPS 140-1 Level 1 compliant saving organizations the time and expense of testing and certification.

The Tumbleweed Validator Toolkit (VTK) allows developers to integrate digital certificate validation into their client applications. The VTK provides an API that can be used to integrate digital certificate validation into an application in three simple steps.

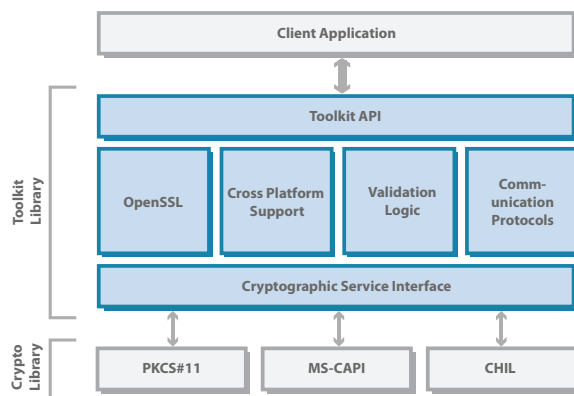
| | |
|--|--|
| Step 1 One time initialization and configuration | <ul style="list-style-type: none"> • Create toolkit context • Configure validation options including protocol • Supply trusted VA and CA certificates • Other start-time configuration |
| Step 2 Per-Validation calls | <ul style="list-style-type: none"> • Create validation query • Add certificates or certificate chain to validate • Add any stateful validation data • Call toolkit validation function <ul style="list-style-type: none"> - Exchange data with VA Server - Verify response - Determine status • Free validation query |
| Step 3 Resource cleanup and termination | <ul style="list-style-type: none"> • Free toolkit resources – toolkit context • Call toolkit termination function |

The VTK provides support for multiple digital certificate validation mechanisms including CA issued Certificate Revocation Lists, Online Certificate Status Protocol (OCSP), Simple Certificate Validation Protocol (SCVP), and VACRL, Tumbleweed's CRL replication protocol for VA manufactured CRL and delta CRL. The VTK APIs insulate the application from the specifics of the underlying mechanism.

The VTK is CA neutral and can support CRL data from multiple CA or VA sources and provides a robust mechanism for CA specific validation policies. VTK can support complex trust models and supports RFC 3280 certificate policy controls for path processing and policy enforcement. The VTK will perform end-to-end (complete) certificate validation if one or more intermediate CAs or VAs are used, and the validation policy requires end-to-end (complete) certificate chain validation.

VTK provides support for securely communicating with a VA Server by utilizing SSL/TLS and has been extensively tested with numerous proxy servers and load balancers. VTK supports different trust models and can support validation of the VA Server certificate. VTK also provides the capability of digitally signing requests to the VA server for deployments that require a high degree of audit and non-repudiation. VTK 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. The VTK offers callback mechanisms to support digital certificates and keys stored on smart cards such as the DOD common access card or hand-held wireless devices through standard interfaces such as Microsoft Cryptographic API (CAPI), PKCS#11 or CHIL.

The VTK provides an ideal solution for PKI enabling network devices such as VPN or WLAN gateways as well as physical security systems.



KEY BENEFITS

- Saves development time and cost by providing application developers an easy to use toolkit to validate PKI digital certificates.
- Flexible architecture – supports numerous low-level validation mechanisms and encapsulates them in a high-level API.
- Open standards based – easy to integrate, easy to evolve – and commercially integrated with numerous partner applications.
- Ideal solution for custom PKI enabled workflow applications, hardware-software devices, and other turn-key PKI solutions.



System Specifications

| | |
|------------------------|---|
| Languages | <ul style="list-style-type: none"> • C/C++ • Java • COM libraries |
| Platforms | <ul style="list-style-type: none"> • Windows XP and 2000/2003 • Solaris 2.7-2.10 • IBM AIX 4.3.3 • HP UX 11.0 • FreeBSD • True64 • Redhat Linux 7.2/8.0 |
| Cryptographic Hardware | <ul style="list-style-type: none"> • nCipher • AEP Systems • SafeNet • Eracom |
| Standards | <ul style="list-style-type: none"> • OCSP (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), HTTP(S), and file based CRL retrieval • RSA PKCS#1, #11, MS-CAPI, CHIL |

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