

# Validation Authority™ Suite

Protect the integrity of your PKI



## Maximize ROI by ensuring PKI safeguards on all secure applications

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, such as passports, credit cards, security badges and other physical credentials, can expire, be revoked or otherwise become invalid over time. Just like point-of-sale credit card authorizations, digital certificate status must be validated each and every time the certificate is to be trusted.

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 including the U.S. Department of Defense, all branches of the U.S. military, the Department of Homeland Security, U.S. Intelligence communities and top financial institutions.

VA is CA-neutral and supports numerous widely adopted international security standards and open technologies. VA is certified Common Criteria, FIPS 201, NIST PDVAL, FIPS 140-2, DOD JITC, Entrust-Ready and IdenTrust compliant, and is part of the IdenTrust, SWIFT Trust Act, BACS and Global Trust Authority financial trust infrastructures. VA interoperates with leading vendor cryptographic hardware, including those 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.

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

- A sophisticated high-performance, high availability VA Server interoperable with numerous products and highly extensible through flexible, easy-to-use interfaces
- Comprehensive, scalable and reliable framework deployed by hundreds of customers worldwide 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
- Flexible multi-platform client solutions enabling digital certificate validation in both standard and custom desktop and server applications
- Supports multiple standards-based digital certificate validation protocols including OCSP, SCVP, CMP and VACRL
- Provides caching and replication of revocation data regardless of format, enabling cost-effective scalability across a wide range of operational environments, including hardware-software appliance and Java-based solutions for distributed or hosted environments
- Supports leading vendor cryptographic hardware, including those certified to FIPS 140-2 Level 3 and 4, to accelerate digital signing and SSL/TLS operations

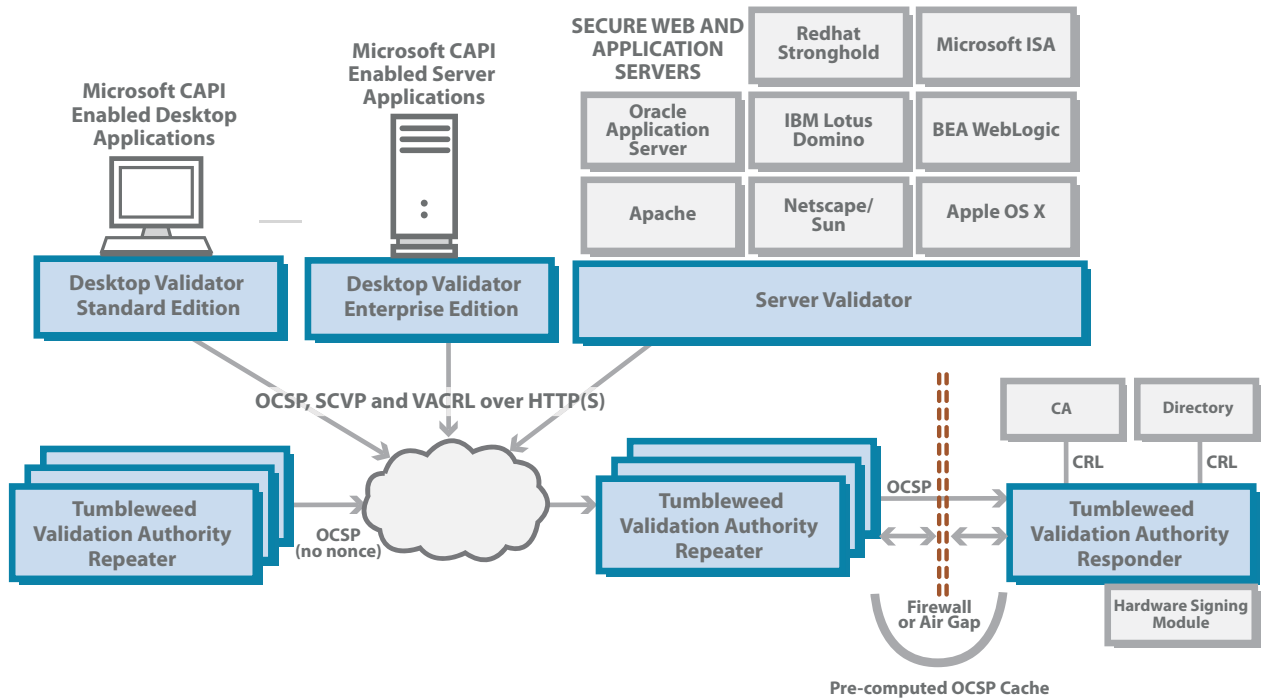
### CERTIFICATIONS

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





# Tumbleweed Validation Authority™ Suite



## SYSTEM SPECIFICATIONS

<b>Platforms</b> (32 and 64-bit support)	<ul style="list-style-type: none"> <li>• Microsoft Windows XP, Vista, 2000 and 2003</li> <li>• Sun Solaris 2.9-2.10</li> <li>• RedHat Linux 4-5</li> <li>• Tumbleweed Appliance</li> <li>• Apple OS X</li> </ul>
<b>Cryptographic Hardware</b>	<ul style="list-style-type: none"> <li>• nCipher</li> <li>• AEP Systems</li> <li>• SafeNet</li> <li>• Eracom</li> </ul>
<b>Load Balancers</b>	<ul style="list-style-type: none"> <li>• Cisco CSS and CSM</li> <li>• Foundry BigIron</li> <li>• F5 Big IP</li> <li>• Resonate Dispatch</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>• OSCP (IETF RFC 2560)</li> <li>• SCVP (RFC 5055)</li> <li>• CMP (IETF RFC 2510)</li> <li>• SSL 2.0, 3.0, TLS 1.0</li> <li>• X509v3 digital certificate format</li> <li>• CRLv2 and delta CRL revocation data</li> <li>• LDAP(S), FTP, HTTP(S) CRL retrieval</li> <li>• SNMP and HTTPS administration</li> <li>• RSA PKCS#1, #7, #10, #11</li> <li>• RSA SHA-1, SHA-256, SHA-512 and MD5</li> <li>• Microsoft Cryptographic API</li> <li>• Supports CAs and CRLs using ECC keys</li> </ul>

## VALIDATION AUTHORITY SERVER

A high-performance multi-platform server that processes client digital certificate status queries using a number of different protocols including OCSP, SCVP, CMP and VACRL. 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, and distributed Repeater-Responder caching of pre-computed and dynamic OCSP responses. The VA Server provides robust non-repudiation features including digitally signed responses, digitally signed logs and CRL archives. 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 failover support through multiple validation mechanisms.

## DESKTOP VALIDATOR

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 failover mechanism with multiple revocation data sources, remote management via Microsoft SMS, CA Unicenter and Microsoft Active Directory. Desktop Validator 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 OCSP response cache that can be pre-computed or dynamically generated. These solutions do not contain any sensitive cryptographic material (since cached OCSP 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.

## TUMBLEWEED PRODUCT LINES



### Managed File Transfer

SecureTransport™ provides a centrally managed system for monitoring and managing secure file transfer activity across multiple file transfer sites or applications. SecureTransport integrates with the existing infrastructure and allows organizations to meet regulatory compliance mandates, and control and manage the transfer of files inside and outside of the corporate firewall.



### Email Encryption

Secure Messenger™ is an email encryption platform that protects, analyzes, manages and reports on email traffic flowing in and out of the organization. Secure Messenger's enterprise-class, component-based architecture includes a state-of-the-art SMTP relay and a powerful policy engine. By monitoring messaging at the Internet gateway with a complete set of email security capabilities, Secure Messenger provides the most effective and reliable method to secure inbound and outbound email streams.



### Email Security

MailGate® is a robust, easy-to-manage email security solution providing comprehensive inbound threat protection and outbound data loss prevention. Unrivaled antivirus, antispam, and Intelligent Edge Defense capabilities deflect junk email and inbound attacks, eliminating up to 90 percent of email traffic before it enters the network. MailGate's simple checkbox content filtering, an intuitive policy manager and automatic gateway-to-gateway encryption make it easy to prevent accidental data leakage.





### Identity Validation

Validation Authority™ ensures the validity and integrity of highly valued and trusted transactions by validating digital certificates in real time. This comprehensive, scalable and reliable framework can validate certificates issued by any Certificate Authority.

# Tumbleweed Validation Authority™ Suite

## TUMBLEWEED APPLIANCES SPECIFICATIONS

	 <b>4600 series</b>	 <b>5600 series</b>
Form factor	1U rack height	
Processors	1 quad-core Xeon processor	1 quad-core Xeon processor
Memory	2GB	4GB
Hard drives	2x 146GB, SAS, 3.5-inch	2x 300GB, SAS, 3.5-inch
Hard drive controller	PERC 6/i, integrated controller card, battery-backed cache, RAID1 (mirrored)	
Effective hard drive storage	146GB	300GB
Network interfaces	2x 10/100/1000 Ethernet interfaces	
USB 2.0 ports	2 front, 2 rear	
Video connector	1 front, 1 rear	
Serial connector	1 rear	
Systems management	Remote access card, 5th generation, 10/100 Ethernet interface	
CD/DVD drive	DVD-ROM	
Rack rails	Sliding Rapid/Versa universal rails and cable management arm	
Size	Height: 1.67" (4.3 cm) Width: 16.7" (42.6cm) Depth: 30.4" (77.2 cm)	
Weight	40.7 lbs (18.4 kg)	43.7 lbs (19.8 kg)
Electrical	110/220VAC auto-switching universal; 167W	110/220VAC auto-switching universal; 213W
Power supplies	670W power supply	Dual redundant 670W power supplies (hot-swappable)

## OPERATING, STORAGE ENVIRONMENT (APPLIES TO ALL APPLIANCE MODELS)

	<b>Operating environment</b>	<b>Storage environment</b>
Temperature	50°F to 95°F (10° to 35°C)	-40°F to 149°F (-40° to 65°C)
Relative humidity	20% to 80% non-condensing (twmax=29°C)	5% to 95% non-condensing (twmax=38°C)
Max. humidity gradient	10% per hour	10% per hour
Max. Vibration	0.26G at 5Hz to 350Hz for 2 minutes	1.54G random vibration at 10Hz to 250Hz for 15 minutes
Max. Shock	1 shock pulse of 41G for up to 2ms	6 shock pulses of 71G for up to 2ms
Altitude	50 ft to 10,000 ft (-16m to 3,048m)	-50 ft to 35,000 ft (-16m to 10,600m)

### LEARN MORE TODAY

To learn more about Tumbleweed's Validation Authority Suite, contact your regional office, email us at [info@tumbleweed.com](mailto:info@tumbleweed.com), or visit us at [www.tumbleweed.com](http://www.tumbleweed.com)



**North America**  
Corporate Headquarters  
Tumbleweed Communications Corp.  
700 Saginaw Drive  
Redwood City, CA 94063  
Phone: 1-877-282-7390

Web: [www.tumbleweed.com](http://www.tumbleweed.com)  
E mail: [info@tumbleweed.com](mailto:info@tumbleweed.com)

**EMEA**  
Tumbleweed Communications Ltd.  
Hurst Grove, Sandford Lane  
Hurst, Berkshire RG10 OSQ  
UK  
Phone: +44 (0)118 934 7100

**APAC**  
Tumbleweed Communications  
2, Havelock Road. #03-16.  
Apollo Centre.  
Singapore 059763  
Phone: +65 6438 0706

© 2008 Tumbleweed Communications Corp. All rights reserved. Tumbleweed is a registered trademark and Tumbleweed MailGate, Tumbleweed Email Firewall, Tumbleweed Secure Messenger, Tumbleweed SecureTransport, and Tumbleweed Validation Authority are trademarks of Tumbleweed Communications Corp. All other brand names are the trademarks of their respective owners. 05/08