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
**SYSTEM SPECIFICATIONS**

**Platforms**
- Microsoft Windows XP, Vista, 2000 and 2003
- Sun Solaris 2.9-2.10
- RedHat Linux 4-5
- Tumbleweed Appliance
- Apple OS X

**Cryptographic Hardware**
- nCipher
- AEP Systems
- SafeNet
- Eracom

**Load Balancers**
- Cisco CSS and CSM
- Foundary BigIbron
- F5 Big IP
- Resonate Dispatch

**Standards**
- OCSP (IETF RFC 2560)
- SCVP (RFC 5055)
- 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 HTTPS administration
- RSA PKCS#1, #7, #10, #11
- RSA SHA-1, SHA-256, SHA-512 and MD5
- Microsoft Cryptographic API
- Supports CAs and CRLs using ECC keys
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 APPLIANCES SPECIFICATIONS

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

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

<table>
<thead>
<tr>
<th></th>
<th>Operating environment</th>
<th>Storage environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>50°F to 95°F (10° to 35°C)</td>
<td>-40°F to 149°F (-40° to 65°C)</td>
</tr>
<tr>
<td>Relative humidity</td>
<td>20% to 80% non-condensing (twmax=29°C)</td>
<td>5% to 95% non-condensing (twmax=38°C)</td>
</tr>
<tr>
<td>Max. humidity gradient</td>
<td>10% per hour</td>
<td>10% per hour</td>
</tr>
<tr>
<td>Max. Vibration</td>
<td>0.26G at 5Hz to 350Hz for 2 minutes</td>
<td>1.5G random vibration at 10Hz to 250Hz for 15 minutes</td>
</tr>
<tr>
<td>Max. Shock</td>
<td>1 shock pulse of 41G for up to 2ms</td>
<td>6 shock pulses of 71G for up to 2ms</td>
</tr>
<tr>
<td>Altitude</td>
<td>50 ft to 10,000 ft (-16m to 3,048m)</td>
<td>-50 ft to 35,000 ft (-16m to 10,600m)</td>
</tr>
</tbody>
</table>

### LEARN MORE TODAY

To learn more about Tumbleweed's Validation Authority Suite, contact your regional office, email us at info@tumbleweed.com, or visit us at www.tumbleweed.com

---

**North America**
Corporate Headquarters
1600 Seaport Blvd
Suite 400, South Bldg.
Redwood City, CA 94063
Tel: 1-877-282-7390
Web: www.tumbleweed.com
E mail: info@tumbleweed.com

**EMEA**
Teal House, 2nd floor
3 Cowley Business Park
High Street, Cowley
Oxford, OX4 4JQ
Tel: +44 (0) 1865 202 780

**APAC**
8 Shenton Way
#31-01 Temasek Tower
Singapore 068811
Tel: +65 6419 5486
Fax: +65 6777 3922

---

Copyright © Axway, 2009 All rights reserved. Tumbleweed, the Arrows logo, SecureTransport, Secure Messenger, MailGate and Validation Authority are either registered trademarks or trademarks of Axway in the United States and/or other countries. All other trademarks are the property of their respective owners. 3/09