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, including the US Department of Defense and all branches of the US military, US Department of Homeland Security, and US intelligence communities, as well as top financial institutions globally.

The VA suite consists of several products that provide a flexible, cost-effective, and robust solution 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™ Server (VA Server) product, a sophisticated digital certificate status responder. The VA Server maintains a store of digital certificate revocation data by obtaining the issuing CA Certificate Revocation List (CRL), a cumulative list of revoked certificates.

The VA Server is CA neutral, supports multiple CAs, several different trust models, and CA specific validation policies. To validate a digital certificate, a client application can query the VA Server rather than having to perform the cumbersome task of obtaining and processing the entire CRL every time it encounters a digital certificate. Client applications can query the VA Server utilizing various open standard protocols including the Online Certificate Status Protocol (OCSP) or the Server-based Certificate Validation Protocol (SCVP), allowing clients to delegate the entire certificate validation operation including path construction and intermediate CA validation to the VA Server.
The Tumbleweed Validation Authority Server™ (VA Server) provides a number of advanced features, making it the ideal solution for customers who need a high-performance and high-availability solution proven in a wide range of application environments.

VA Mirroring provides support for backup, load balancing and failover by replicating the same certificate revocation data across a cluster of VA Servers. Mirroring enables revocation data from a source VA to be replicated via a secure push or pull based synchronization mechanism to one or more destination VAs. Replicated revocation data can consist of pre-computed OCSP responses, CA generated full CRLs or delta CRLs representing the changes between two full CA-signed CRLs, VA manufactured delta CRLs representing the needs of the destination, or VA generated CRLs based on instant local revocation (either by the VA administrator or by a CMP message).

In addition to replication, the VA offers caching. Large-scale, robust Internet service architectures have traditionally relied on network based caches to reduce traffic, improve user wait times as well as provide additional levels of security and robustness. The VA extended this concept to digital certificate validation by introducing a distributed VA Responder-Repeater caching architecture.

A Repeater is a VA Server that maintains a cache loaded with pre-computed OCSP responses or dynamically built up by proxy of client requests to a Responder. Repeaters also support VA-to-VA mirroring and can cache revocation data in CRL form. Repeaters support the VACRL protocol, providing support for non-OCSP clients or clients that want to maintain their own revocation data caches for backup. This functionality is highly useful in low-bandwidth environments or environments where real-time network access is not possible at all times.

Since a Repeater does not need to perform cryptographic operations (the cached responses are digitally signed by the Responder), it does not require additional cryptographic hardware support, offering a cost effective way for organizations to scale their digital certificate validation infrastructure for performance and availability. Repeaters do not contain any sensitive key material and can easily reside in a different administrative domain than the Responder Server, allowing the Responder to be secured using a firewall or air gap.

Additionally, the VA product line includes the Repeater Appliance and Repeater Servlet. The Repeater Appliance is a hardware-software appliance solution, leveraging Tumbleweed’s secure, hardened Linux-based platform. The Repeater Appliance can be installed in less than thirty minutes, offering organizations the lowest total cost of ownership and an ideal solution for high scale deployments.

Since a Repeater does not need to perform cryptographic operations (the cached responses are digitally signed by the Responder), it does not require additional cryptographic hardware support, offering a cost effective way for organizations to scale their digital certificate validation infrastructure for performance and availability. Repeaters do not contain any sensitive key material and can easily reside in a different administrative domain than the Responder Server, allowing the Responder to be secured using a firewall or air gap.

The VA Server can be operated with a high-degree of security through features such as SSL based communication with clients, digitally signed client requests/responses, digitally signed XML logs and CRL archives, as well as SSL based server administration. To enhance the performance of these features, the VA supports software, PKCS #11 or CAPI token-based hardware signing and encryption products, including FIPS 140-2 Level 3 and Level 4 compliant hardware signing modules, from all leading vendors.

The VA Server can be operated with a high-degree of security through features such as SSL based communication with clients, digitally signed client requests/responses, digitally signed XML logs and CRL archives, as well as SSL based server administration. To enhance the performance of these features, the VA supports software, PKCS #11 or CAPI token-based hardware signing and encryption products, including FIPS 140-2 Level 3 and Level 4 compliant hardware signing modules, from all leading vendors.