The VA is composed of two software components that, together, build a secure certificate validation infrastructure, as shown in the diagram on the next page. Typically, a PKI environment will deploy one Validation Authority in a single, secured location, which may be the same location as the Certificate Authority (CA). The Validation Authority publishes Distributed OCSP validation proofs to any number of VA Responders, which provide standard OCSP service to relying parties using an OCSP toolkit, application or plug-in.

Key features
The VA introduces a distributed infrastructure for certificate validation that is fundamentally superior to any CRL or Traditional OCSP scheme in the following areas:

- **Security** – VA Responders have no private keys, so they require little physical or network protection. VA Responders cannot provide false responses, even if compromised. Additionally, the VA uses FIPS 140-2 certified cryptography.
- **Scalability** – VA Responders can be rapidly deployed in any number of locations to scale to meet the needs of hundreds of remote sites.
- **Availability** – Since the VA Responders can be easily replicated in many locations, overall service availability is extremely high, with excellent survivability under attack when compared to centralized, trusted topologies.
- **Performance** – VA Responders can be placed close to relying parties to support extremely low latency for OCSP responses.
- **Cost effective** – Validation Authority pricing allows for unlimited Responder deployments at a fraction of the cost of the Traditional OCSP model. In addition, there are no per-transaction costs.
- **Ease of management** – Since the Responders represent stateless, appliance-grade functionality, only the central Validation Authority requires management. To ease management, the VA is configurable through a full-featured web interface.
- **Fully licensed** – The VA represents the only authorized OCSP implementation covered by HID Global’s intellectual property, including US patents 5,666,416 and 5,717,758.
- **Standards compliant** – While the VA represents a revolutionary approach to certificate validation, it integrates seamlessly with existing PKI products from HID Global and other vendors, through standards, such as X.509, OCSP and LDAP. The Validation Authority is FIPS 201 approved.
HID Global’s Smart Data Bridge™ (optional)
The Smart Data Bridge is an optional component, which constantly monitors data sources for certificate status updates, and pushes these changes to the HID Global’s Validation Authority whenever they occur.

HID Global’s Complimentary Products
- Responder Appliance
- Desktop Validation Client™
- Server Validation Extension™ for Microsoft IIS
- Server Validation Extension™ for Microsoft Domain Controller
- Server Validation Extension™ for Microsoft Exchange Outlook® Web Access

Licensing
Whether used for information security, such as secure mail, or physical security, such as an electronic access control system, a secure PKI needs a strong validation infrastructure to provide secure authorization using digital certificates.

The VA is currently available for purchase and deployment. Contact HID Global to receive more information or to discuss professional services to assist in the deployment of a secure and scalable validation infrastructure.

Supported platforms
- Microsoft Windows Server® 2008 R2 and 2012 R2
- Red Hat® Enterprise Linux v.5, 6 and 7
- Sun® Solaris™ 10

Supported databases
- Microsoft SQL Server™ 2008 and 2012
- Oracle® 9i, 10g and 11
- PostgreSQL 8.4

Supported certificate authorities
- Supports all industry standards-compliant certificate authorities

Supported security modules
- SafeNet® Luna® SA and Luna PCI
- Thales® nShield™ Connect and nShield Solo
- AEP™ Keyper Enterprise and Keyper Plus