ADSS SCVP Server

FIPS 201 Certified Validation Authority

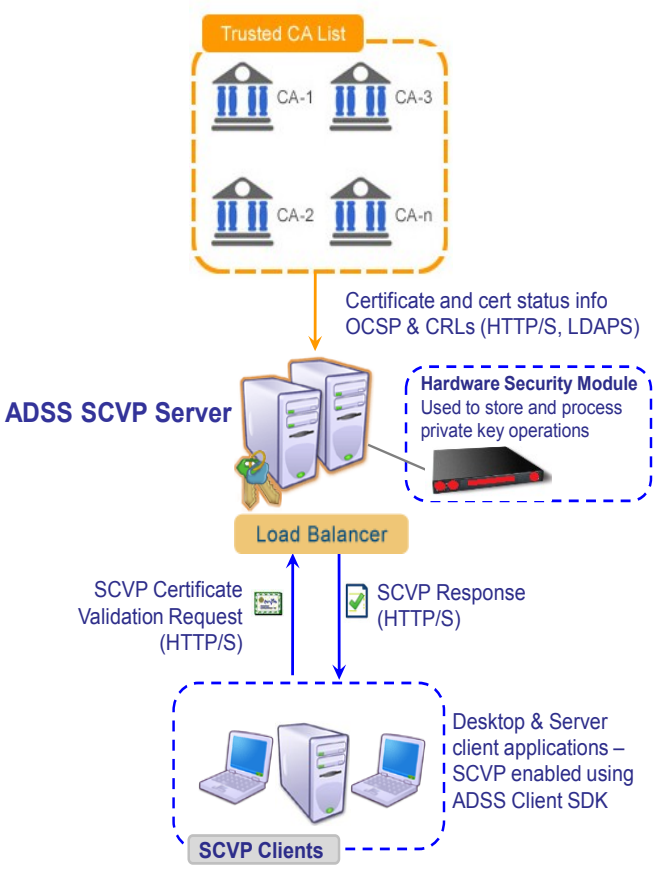
The Ascertia ADSS Server is a multi-function server offering a range of trust services for digital signature creation and verification, e-ID validation, time stamping and long-term archiving. The ADSS Client SDK provides a very effective SCVP client. This datasheet describes the ADSS SCVP Server.

Validating the trustworthiness of digital certificates can be complex and it normally requires sophisticated client-side logic. The Server-based Certificate Validation Protocol (SCVP) standard was created to allow business applications to be less aware and delegate all aspects of certificate validation to a trusted server.

ADSS SCVP Server meets the RFC 5055 SCVP standard for full path validation of X.509 e-ID certificates and is FIPS 201 certified. It is Federal PKI PD-VAL certified and is the first SCVP product to pass the updated SHA-2 NIST PKITS path discovery and validation test suite.

Certificate path discovery and validation is complex especially within Bridge CA environments. If certificate handling is to be widely deployed in a variety of applications and environments, the amount of processing an application needs to perform before it can accept a certificate needs to be reduced.

There are a variety of applications that can make use of public key certificates, but these applications can be significantly burdened with the overhead of constructing and validating the certification paths and handling the many PKI complexities. ADSS SCVP Server has been carefully built to make it very easy for multiple business applications to very easily delegate the whole trust decision process to a fast reliable security server with just a few lines of code.



Why use ADSS SCVP Server
Provides full certificate path discovery and validation (unlike OCSP protocols where the client builds the path and must check individual certificates).
Complies with IETF RFC 5055, including historic certificate validation and passes the PKITS test suite.
Designed to be highly effective for Enterprise or Managed Service Provider solutions.
Enforces client authentication using SSL certificates, SCVP request signing and/or IP address filtering.
Retrieves certificate information and certificate status information from back-end PKIs using AIA, CDP or LDAP based information plus OCSP and CRL data.
Includes ADSS CRL Monitor, a powerful watch-dog CRL monitoring, retrieving and alerting module.
Supports strong hash algorithms SHA-1, SHA256, SHA384 and SHA-512, together with up to 4096-bit keys. Supports RSA and ECDSA algorithms. Supports FIPS 140-2 and CC EAL4+ HSMs.
Provides detailed transaction logs, with effective viewing, searching, reporting and archiving options.
Includes the ADSS Client SDK for easy integration of SCVP protocol in desktop and server applications.
Offers a human-readable transaction viewer for SCVP protocol requests and responses.
Supports multiple Validation Policies, with their own Trust Anchors and validation algorithm settings.
It's easy to install, configure and manage using secure web-browser management screens.
Offers strong role-based access controls for administrators and features optional dual controls.
Provides HMAC protected system event & operator activity logging.
Provides assured throughput, scalability & resilience.

RFC 5055 Compliant SCVP Validation Authority

Key Features

Flexibility: Supports the configuration of multiple SCVP validation policies each with their own Trust Anchors and detailed validation algorithm parameters.

Full Validation: Complies fully with RFC5280 certificate path validation algorithm, including support for following aspects:

- Inhibit Any Policy
- Require Explicit Policy
- Acceptable Certificate Policy Set
- Inhibit Policy Mapping
- Permitted/excluded Subject Names
- Trust Anchors
- Acceptable Key Usages
- Acceptable Extended Key Usages

These inputs into the certificate path validation algorithm may be pre-configured within SCVP validation policies or be specified by clients within their request messages.

Want Backs: ADSS SCVP Server can return to clients the full certificate path, public key info, revocation status evidence and other related info as specified in RFC 5055.

High-Availability: ADSS SCVP Server can be easily implemented as a highly available service to meet demanding service level agreement needs. Multiple servers can work in parallel using standard load-balancing techniques and a resilient secondary site can also be established. Network HSMs, system platforms and database management systems can be used as required to meet availability requirements.

Flexible Trust Model: The keys used by ADSS SCVP Server can be self-certified, or CA issued certificates. The internal CA module or an external CA can be used.

Maximum Security: Strong authentication of clients and operators using certificates. ADSS SCVP Server keys can be managed inside a secure FIPS or CC approved HSM. Logs are tamper-evident. Tight role-based access control is provided and dual control operations are optional.

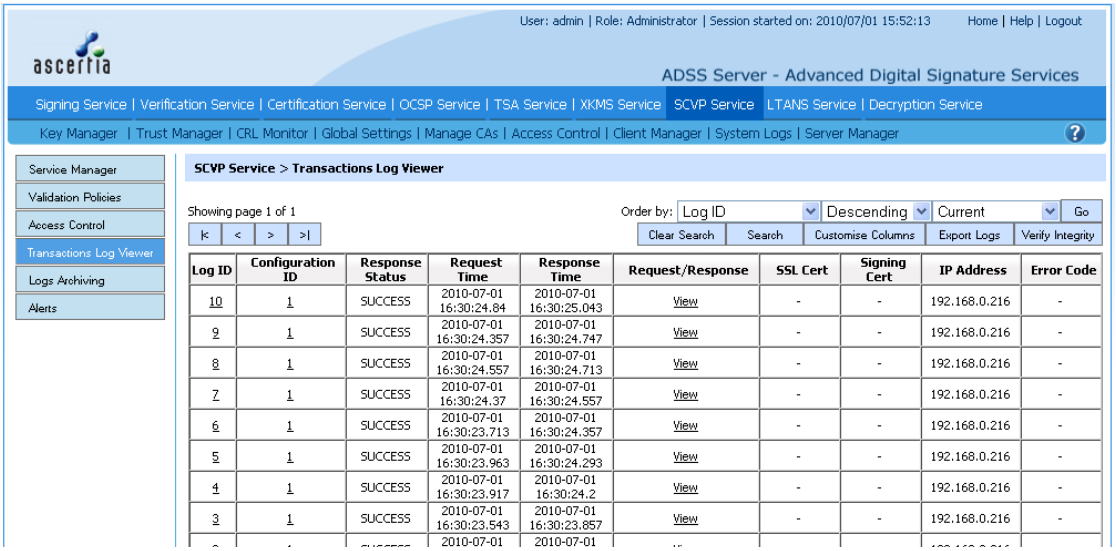
Easy Administration: Simple installation wizard, automated archiving, automated system integrity checking, real-time alerting and other similar features ensure ADSS Server is extremely easy to administer.

Advanced Functionality: ADSS SCVP Server has many advanced features such as mandating that SCVP requests are signed, supporting multiple certificates within a single validation request and support for name validation algorithm.

Historic Validation: It is possible for clients to validate certificate's trustworthiness in the past. ADSS SCVP Server maintains an archive of old CRLs. This is an essential requirement for verifying signed documents historically especially during dispute resolution.

Client APIs & Test Tools: Ascertia provides ADSS Client SDK which offers a high-level API for SCVP in both Java and .NET. An ADSS Server Test Tool is also available for testing purposes.

This screenshot shows the detail from just one of the log details screen. Each request/response can be viewed in detail including a drill down screen that shows the exact steps followed in validating the certificate path, ideal for learning why a particular response was given. This saves hours of valuable time from subject experts.



ADSS SCVP Server Standards Compliance:

Front-end Interface:	HTTP & HTTPS Server-based Certificate Validation Protocol (SCVP as specified in RFC 5055)
PKI standards:	PKCS#10, PKCS#7, PKCS#11, RFC 5280, SSL/TLS
Back-end Interface:	OCSP (over HTTP/S), LDAP/S and HTTP/S for CRL Retrieval
Platforms:	Windows 2003 & 2008 Server (32/64), various Linux systems (32/64), Solaris 10, 11(x86)
Databases:	SQL Server 2005 & 2008 (and Express), Oracle 10g, 11g, PostgreSQL 8,9, MySQL 5
HSMs	SafeNet Luna and ProtectServer HSMs, Thales nCipher HSMs and Utimaco HSMs

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 1256 895416 US: +1 508 283 1890
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

Digitally Signed By: Rod Crook
Reason: I approve this document
09/07/2012 22:47:07 GMT +01:00