ADSS SCVP Server

FIPS 201 Certified Validation Authority

ADSS TSA Server is a well-proven, standards-based product that can be deployed on premise or as part of a cloud service. It offers high throughput and high availability, scalable to meet the most demanding needs. As a strategic product for Ascertia, it offers support for the latest Windows and Linux operating systems, databases and HSMs from the major vendors.

SCVP Overview

Digital certificates provide individuals, organisations, applications, and devices with trustworthy digital identities for use within the digital world. Digital certificates can be issued from a variety of issuers globally, and digital certificates need to be trusted and verified across a range of differing trust architectures:

- Traditional Hierarchies consisting of Root and Subordinate CA and in some cases Policy CA's
- Cross-Certified Hierarchies of CA's
- Bridged PKI's where many Roots participate.

In these complex PKI deployments, each Root CA will assert different policies that must be processed and understood by end entities.

When a relying party needs to validate the signature on a document or when a user or device is authenticating using a certificate, it must process the digital certificates used as part of the signature verification or authentication process, it must verify the certificate can be chained to a trusted Root CA, this process may involve certificate chain validation across several issuers and in some cases across multiple trust infrastructures.

The process of validating the trustworthiness of digital certificates in such sophisticated architectures is complex and requires sophisticated client-side validation logic. The Server-based Certificate Validation Protocol (SCVP) standard was created to allow business applications and constrained devices to be less aware and delegates all aspects of certificate validation to a trusted server.

Ascertia ADSS SCVP Server is unmatched in this area.

Key Features

- **Flexibility:** Supports the configuration of multiple SCVP validation policies each with their own Trust Anchors and detailed validation algorithm parameters.
- **Standards Compliance**: Fully compliant with RFC 5055 SCVP standard including historic certificate validation, has undergone FIPS 201 Certification and Federal PKI PDV Certification.
- **Flexible Deployment Options**: Can be deployed and operated in-house and as a solution for Managed Service Providers looking for fast, scalable, secure products featuring detailed logging, transaction log analysis and reporting
- **Cryptography Support**: 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
- **High-Availability**: ADSS SCVP Server is well proven at offering high throughput, high availability and scales to meet the most demanding business needs.
- **Comprehensive Validation Checking:** Provides full certificate delegated path discovery (DPD) and delegated path validation (DPV) – this is different to OCSP protocols where the client builds the path and checks each individual certificate.
- **CWA 14167-1 Compliant:** Meets the requirements for trustworthy systems including strong role-based access controls, optional dual controls, detailed and secure transactional, system event & operator activity logging.

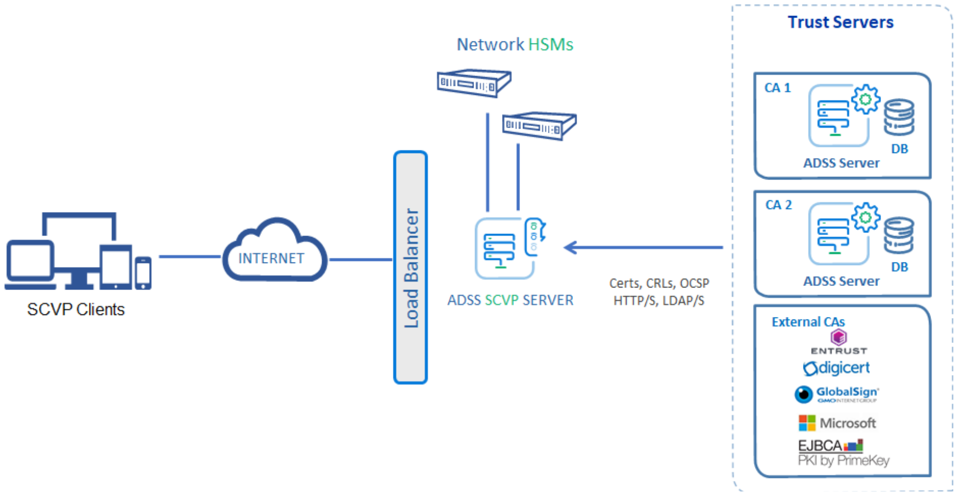
ADSS TSA Server Architecture

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

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 makes it very easy for one or multiple business applications to delegate the whole trust decision process to a fast, reliable SCVP Validation Authority server with just a few lines of code.



Key Features

Full Validation: Complies fully with the RFC 5280 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.

Secure 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.

Advanced Features (Cont.)

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.

ADSS SCVP Server is an advanced Timestamping Server that supports multiple TSA policies, provides role based operator access controls and high availability configurations.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

Supported Operating Systems:

Microsoft Server 2022, 2019, 2016
Linux RedHat, SUSE, CentOS, Ubuntu

Supported Databases:

Microsoft SQL Server 2022, 2019, 2017
Oracle 19c, 18c
Azure SQL Database (Database-as-a-service)
PostgreSQL 14, 13, 12, 11
MySQL 8, 5
Percona-XtraDB-Cluster 8, 5

Supported Security Modules

Thales Luna and Protect Server
Entrust nShield
Utimaco SS & CS CP5
Microsoft Azure Key Vault
Amazon AWS Cloud HSM (Linux Only)

M Hathaway

×

Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info

info@ascertia.com

www.ascertia.com