MOBILE-ID
Anytime, Anywhere

TRUSTED HUB

SCVP Appliance

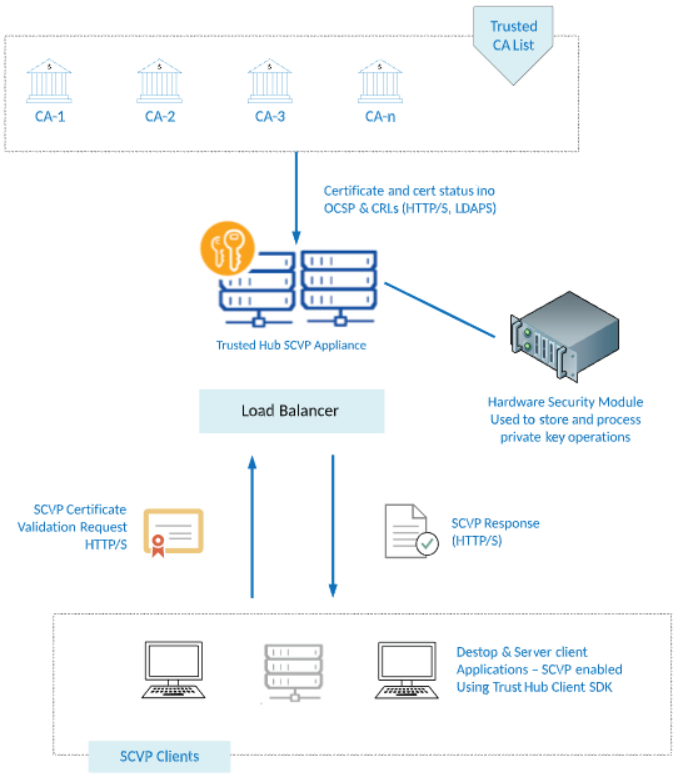
RFC 5055 Validation Authority using Advanced Path Discovery and Validation

Validating the trustworthiness of digital certificates can be complex and it normally requires sophisticated client-side logic. The RFC 5055 Server-based Certificate Validation Protocol (SCVP) standard was created to allow relying parties to be less aware and delegate all aspects of certificate validation to a trusted server.
The Mobile-ID™ Trusted Hub Appliance is a multi-function server offering a range of trust services for certificate validation and also digital signature creation and verification, eID validation, time stamping and long-term archiving. The Trusted Hub Client SDK provides a very effective SCVP client.

Trusted Hub SCVP Appliance meets the RFC 5055 SCVP standard for full path validation of X.509 eID certificates and is FIPS 201 certified (APL #692). 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. Trusted Hub SCVP Appliance makes it very easy for one or multiple relying parties to delegate the whole trust decision process to a fast, reliable SCVP Validation Authority server with just a few lines of code.



Why use Trusted Hub SCVP Appliance

- 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
- Complies with IETF RFC 5055, including historic certificate validation and is FIPS 201 certified
- A great product for in-house deployment and as a solution for Managed Service Providers looking for fast, scalable, secure products featuring detailed logging, transaction log analysis and reporting
- 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 Trusted Hub CRL Monitor, a powerful watchdog CRL monitoring, retrieving and alerting module
- Supports strong hash algorithms SHA-256, SHA-384 and SHA-512, RSA 2048 to 8192 bits, ECDSA 256 to 512 bits. Supports FIPS 140-2 HSMs
- Provides detailed transaction logs, with effective viewing, searching, reporting and archiving options.
- Includes the Trusted Hub 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

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 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.

Want Backs: Trusted Hub SCVP Appliance 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: Trusted Hub SCVP Appliance 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 Trusted Hub SCVP Appliance 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. Trusted Hub SCVP Appliance 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 Trusted Hub Appliance is extremely easy to administer.

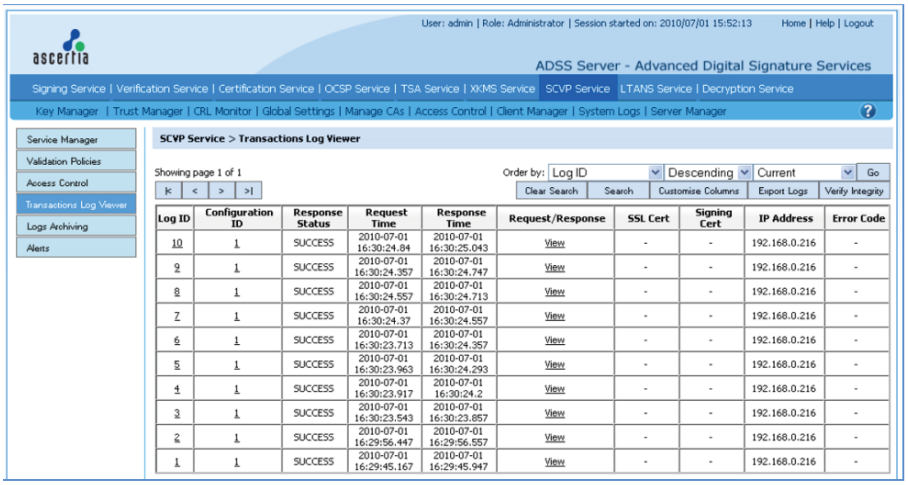
Advanced Functionality: Trusted Hub SCVP Appliance has many advanced features such as mandating that SCVP requests are signed, supporting multiple certificates within a single validation request and support for name validation algorithm.

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

Client APIs & Test Tools: Mobile-ID™ provides Trusted Hub Client SDK which offers a high-level API for SCVP in both Java and .NET. An Trusted Hub Appliance 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.

Ask us for further details on Trusted Hub SCVP Appliance and its sophisticated management options.



Trusted Hub SCVP Appliance 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, TLS/SSL
Back-end Interfaces:	OCSP (over HTTP/S), LDAP/S and HTTP/S for CRL Retrieval
Platforms:	Windows Server 2016/2012 R2/2012/2008 R2, Linux (RedHat, CentOS, SuSe, others), Solaris
Databases:	SQL Server 2016/2014/2012, Oracle 12c/11gR2/11g, PostgreSQL 9/8, MySQL 5.x (Percona & Oracle), Azure SQL
HSM Support:	PKCS#11 or CAPI/CNG compliant HSMs, smartcards or tokens, Gemalto/SafeNet, Thales, Utimaco, Cloud HSMs including Azure Key Vault, Amazon AWS Cloud HSM
Operator interface:	Mutually-authenticated HTTPS secure web-interface for administrators, plus email, SMS, SNMP & syslog alerting