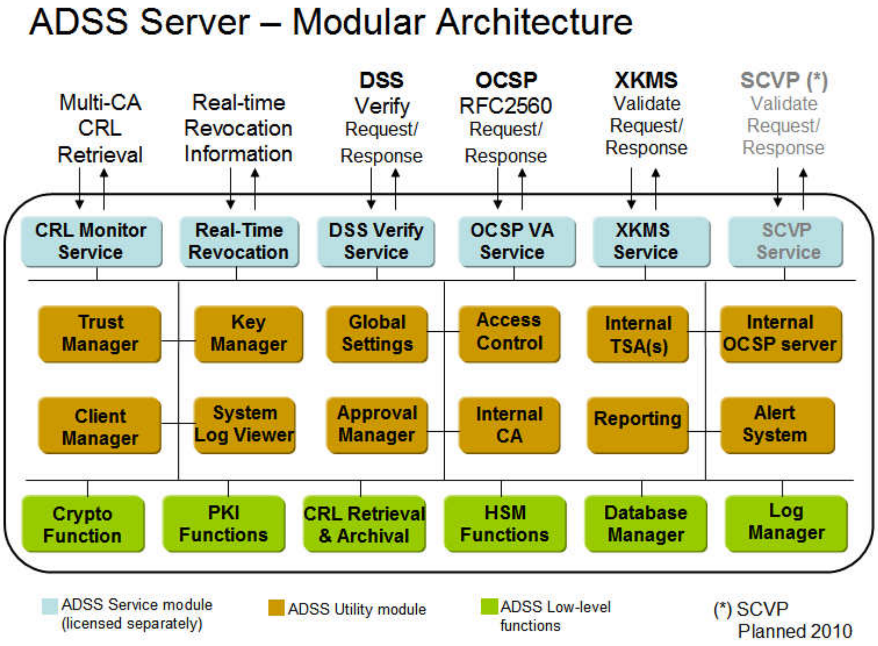
Certificate Verification Solutions for e-Business

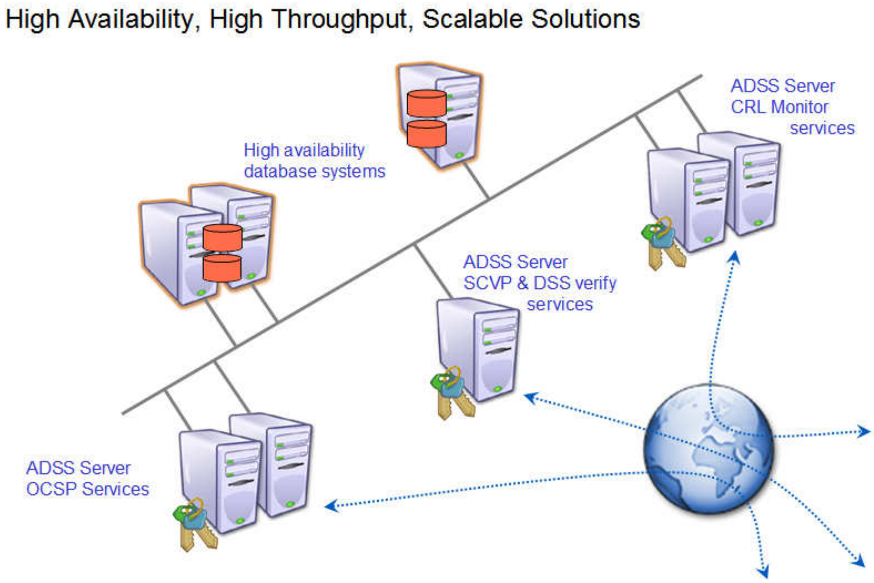
Certificate verification can be a complex area. Ascertia offers one of the most advanced product based solutions in this area to verify certificates as well as signatures. Key criteria in selecting a verification solution should include security management, flexibility, standards compliance, investment protection and the ability of the underlying product to evolve to meet both older and newer standards and usage requirements.



Ascertia's ADSS Server offers the advantage of a well designed architecture and well-proven implementations for large enterprises and major managed service providers. The verification services architecture of ADSS Server is shown to the right.

The modular services and existing certificate path building and validation functionality allows new service protocols such as SCVP to be added very easily.

ADSS Server supports both HTTP/S based services (for OCSP, XKMS and in future SCVP) as well as web-services for OASIS DSS Signature Verification requests. CRL Monitor offers very advanced CRL management features. Each CA has a defined validation policy, specifying where the CRLs can be obtained from. Of course new CRLs will be fetched at the specified nextUpdate date and time, however CRL manager can also poll for any emergency or over-issued CRLs as defined by an administrator. High availability is assured using two or more watch-dog CRL Monitor services on separate platforms.



High Availability, High Throughput, Scalable Solutions
High availability database systems
ADSS Server CRL Monitor services
ADSS Server SCVP & DSS verify services
ADSS Server OCSP Services

Scalability: For maximum flexibility, availability and throughput each ADSS Server service can be implemented on a different server. Using a high availability database the configuration details, trust anchor information, validation information are made available to all active servers. Event and transaction logs are also recorded centrally. This allows some severs to be dedicated to CRL Monitoring, whilst others handle OCSP Services, separated from SCVP, XKMS requests and even DSS signature verification web-services. The production solution can therefore be easily adapted to suit changing loading conditions using the in-built flexibility of the product. Additional servers can be utilised to run more OCSP services and thus handle greater loads. Similarly SCVP, XKMS and even DSS verification services can be added as needed on the same or different production servers. All verification servers can be used in active - active mode behind a standard network load balancer. CRL Monitor ensures that the most up-to-date validation information is available to all ADSS Server services. The OCSP service is also able to act as a proxy where required to refer to other external OCSP responders when CAs do not publish CRLs externally.

CRL Monitoring: Multiple CAs can be monitored, the limit is determined by the size of the network bandwidth and the processing power required to download and process the CRLs. Some national CRLs are extremely large and are updated every few minutes - imposing a reasonable load just for one CA. CRLs can be downloaded from HTTP, HTTPS, LDAP and LDAPS locations. CRLs are checked in detail - a CRL freshness check is implemented and the structure, integrity, signature, validity of the CRL is confirmed with email and/or SMS alerts being sent if issues are discovered. Full CRLs and Indirect CRLs are all supported. If for some reason the master CRL Monitor service fails then the next slave on the list of available slaves servers realises that the master instance has ceased normal operations and will promote itself to master status. If the old master then recovers it will in turn see that its status is now slave and will wait for its automatic turn to become master. Admin staff can change the master / slave status if required. Since only one instance of CRL Monitor can be used at a time a multi-CPU system is recommended, e.g. a 2 or 4 CPU quad core Xeon system should cope with many tens of CAs. An enhancement could be considered to split the processing of various CAs into groups, each process group having its own CRL Monitor.

CRL Data Management: When CRLs are downloaded they are checked and then expanded into a certificate validation database for the relevant CA. The CRLs are also (a) archived for historical certificate validation and (b) copied to a local folder if this is configured. The main database engine is thus responsible for the local caching of certificate status information, archived CRLs and in fact all the event and translation log information for the CRL Monitor service. The high availability watchdog processing depends on the database environment being available and reliable.

Historic Certificate Verification: If a historic certificate verification request is made for a specified date and time then the last archived CRL that covered this period is recovered and is checked to determine the certificate status. A grace period can be manually calculated when requesting a historic check.

Real Time Certificate Information: Where required Ascertia can also offer real-time revocation updating – this information can be provided by any suitable authority, for example a CA, an RA, an Identity Management application or card management system. ADSS Server takes this real-time update and over-rides the CRL data until a new CRL is published. Currently a real-time file based system is used but a CMP or CMC handler could be added as an enhancement if required. All these options provide the ability to offer certificate white & black listing for on a real-time basis outside of the usual revocation cycle. The validity period could be optionally extended to live beyond the next CRL. ADSS Server itself offers controlled access to its services based on (a) IP address white and black list, (b) Client SSL certificate white and black list (c) request signing.

OCSP Validation: ADSS Server offers world-class OCSP Validation Authority (OCSP Responder) services. Using the underlying power of the CRL Monitor described above a fully compliant RFC2560 on-line certificate status protocol service is offered to:

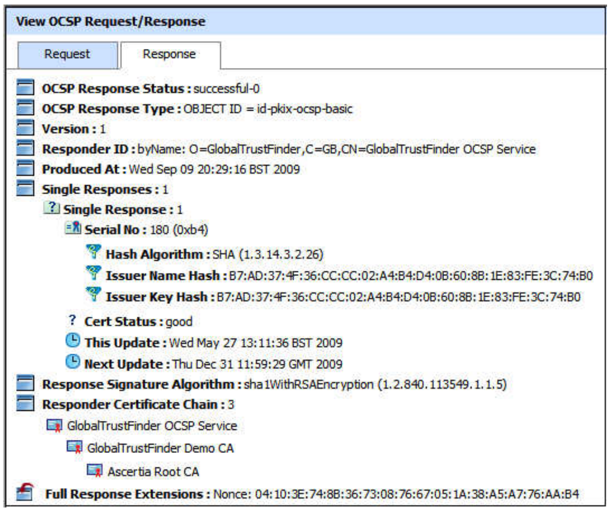
(1) Check the inbound request to see if it can be authenticated and authorised using (a) no checks or (b) IP address, (c) Client SSL certificates, or (d) OCSP request signature

(2) Check the CA that it needs to respond for and create a response consistent with the standard and the certificate status data in its CRL / real-time databases

(3) Sign the response message using the correct response signing key and certificate for the selected CA (uses separate keys/cert for each registered CA)

It is designed to meet the requirements of schemes such as IdenTrust, the DoD JITC and CWA 14167-1. ADSS server has been tested with Microsoft Certificate Server, UniCERT, Entrust Authority, RSA KEON and other CAs. Any standards-compliant OCSP client can be utilised.

ADSS Server OCSP services offer the in-built load-balanced high availability and scalability described before. Detailed logs are kept of all requests and responses. English language diagnostic utilities form part of the standard product to help security administrators rapidly analyse requests (and responses) to allow issues to be quickly resolved within minutes. See the later section on transaction reporting.



```
OCSP Response Status : successful-0
OCSP Response Type : OBJECT ID = id-pkix-ocsp-basic
Version : 1
Responder ID : byName: O=GlobalTrustFinder,C=GB,CN=GlobalTrustFinder OCSP Service
Produced At : Wed Sep 09 20:29:16 BST 2009
Single Responses : 1
  Single Response : 1
    Serial No : 180 (0xb4)
      Hash Algorithm : SHA (1.3.14.3.2.26)
      Issuer Name Hash : B7:AD:37:4F:36:CC:CC:02:A4:B4:D4:0B:60:8B:1E:83:FE:3C:74:B0
      Issuer Key Hash : B7:AD:37:4F:36:CC:CC:02:A4:B4:D4:0B:60:8B:1E:83:FE:3C:74:B0
    Cert Status : good
    This Update : Wed May 27 13:11:36 BST 2009
    Next Update : Thu Dec 31 11:59:29 GMT 2009
Response Signature Algorithm : sha1WithRSAEncryption (1.2.840.113549.1.1.5)
Responder Certificate Chain : 3
  GlobalTrustFinder OCSP Service
    GlobalTrustFinder Demo CA
      Ascertia Root CA
Full Response Extensions : Nonce: 04:10:3E:74:8B:36:73:08:76:67:05:1A:38:A5:A7:76:AA:B4
```

Certificate Verification Solutions

XKMS Validation: XKMS removes the complexities of handling certificates locally by delegating this to a server based application. ADSS Server is such an application and it is responsible for delegated path building and validation according to the W3C XKMS X-KISS standard. The delegation of certificate status handling using an XML/SOAP protocol to ADSS Server makes the client a lot simpler and delegates more functionality to the server, which is now more sophisticated. ADSS Server handles XKMS services in the same highly scalable, well managed, controlled, logged / reported way it does other services such as OCSP.

SCVP Validation: SCVP is somewhat similar to XKMS in that client systems delegate certificate validation checking to a server such as ADSS Server. Delegated path discovery and validation needs to be performed. The RFC5055 protocol is based on ASN.1 rather than XML/SOAP. An SCVP service has not yet been delivered due to lack of market demand for this protocol. It can be committed for delivery in the first half of 2010 as part of a project order. ADSS Server will handle SCVP services in the same highly scalable, well managed, controlled, logged and well reported way it does other services such as OCSP. It will reuse its current low-level path discovery and validation logic already implemented for XKMS service.

Web-Service Verification: ADSS Server is able to offer certificate verification services using an HTTP/S and XML/SOAP web-services interface. An optional high-level Java and .NET API is also offered to enable business applications to make such requests very easily in a few lines of code. The certificate verification web service is essentially another protocol interface that ADSS Server offered to allow a certificate or certificate chain to be checked, its trust status determined using the same path building and path validation technology used before. In addition ADSS Server is able to set filters to assign the CAs that should be used as trust anchors for each business application trust based on the requesting client. Also ADSS Server is able to return a trust rating – essentially a numeric code that can identify the level of trust associated with a particular issuer CA. This can be useful in determining the CAs that can be trusted for certain transactions, e.g. Qualified Certificate Issuers, other high trust CAs as compared with free email CAs. Business applications will be able to mandate or assess the trust level of CAs easily using this approach.

In detail the certification verification web service can check (a) the final Trust Anchors which are to be trusted by this client, b) the default minimum certificate trust rating for this application, c) a list of acceptable certificate policy OIDs for this client, d) Key Usage extension bit settings and e) how the Basic Constraints extension in the signer's certificate should be set to be considered valid.

Security Management: ADSS Server has been designed to offer well-managed security services from one product. The security management is highly effective and offers:

a) A secure web-browser Interface – to provide effective management from anywhere
b) Operator Authentication using client SSL certificates and role based access control to service management features – provides strong privacy and prevents MITM and session take-over attacks
c) Optional dual control to make and then authorize any changes to the configuration data
d) Client application authentication & authorisation to ensure that access to the relevant services, policies CAs, keys and certificates is effectively controlled
e) Secure event and transaction log creation and reporting – to ensure that all system events and all requests & responses are logged and protected using sequenced HMACs to prevent tampering
f) Auto-archiving keeps the database size small and all archived records are digitally signed
g) Management reporting in summary or detail as required for analysis or feeding data to billing systems,
h) Effective key management using PKCS#11 or PKCS#12 specifications, trust anchor management and algorithm management (e.g. supports SHA-2 already and large key lengths)
i) Database integrity management using HMACs to protect all important database information, including automated system integrity checking.

Effective Documentation: ADSS Server has been widely praised for the high quality of documentation including installation guides, quick guides and source code samples that is provided as standard. Check this yourself - the admin guide is available here:

https://www.ascertia.com/helpconsole/ADSS-Admin-Guide-3p7/default.aspx

Effective Reporting: ADSS Server offers excellent management reporting features – review these here:

https://www.ascertia.com/helpconsole/ADSS-Admin-Guide-3p7/default.aspx?pageid=Service_Separate