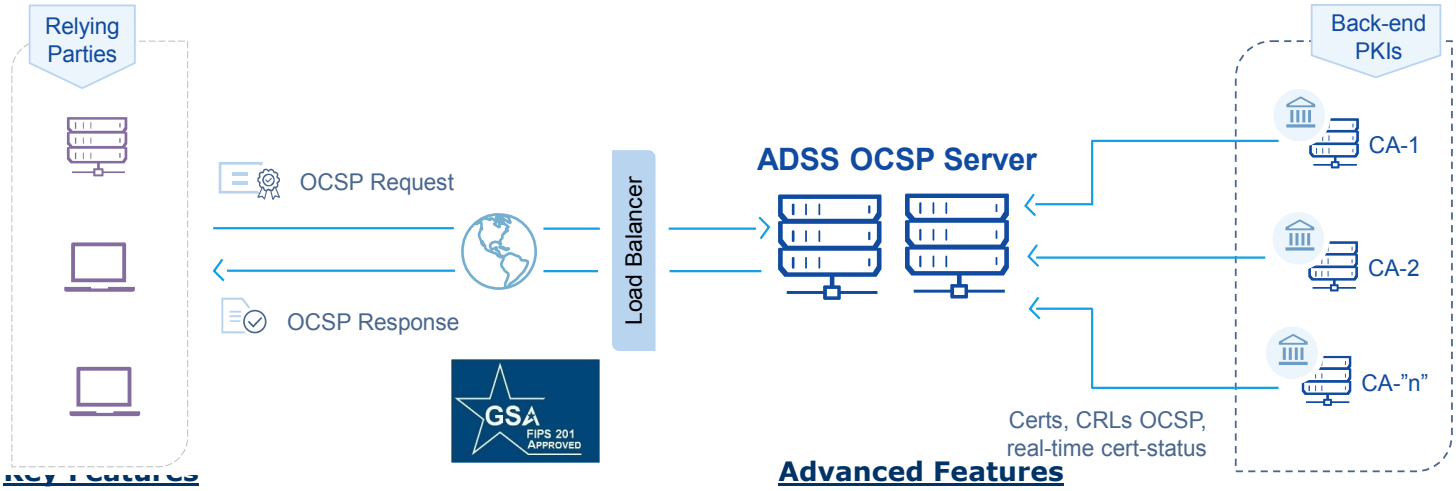
ADSS OCSP Server

FIPS 201 Certified Validation Authority

ADSS OCSP Server is a high performance, robust and reliable OCSP Validation Authority that complies with the RFC 6960 and RFC 5019 standards. It is FIPS 201 Certified (APL #1411 replacing the previous APL #583) confirming that it meets all the requirements and is approved for use by US federal agencies for HSPD-12 implementations. Ascertia stands out as the vendor that is still investing in their OCSP Validation Authority products and investing in GSA FIPS testing.

ADSS OCSP Server complies with the CEN Workshop Agreement CWA 14167-1 requirements and has been designed to operate as a robust validation hub solution, capable of providing OCSP certificate validation services for multiple Certificate Authorities (CAs) concurrently! Simple or sophisticated validation policies are supported for each individual CA and ADSS OCSP Server provides detailed transactional reporting and reviewing – essential for troubleshooting within managed service infrastructures or enterprise systems. Both OCSP Servers and distributed OCSP Repeaters are available.



Key Features

Standards Compliance: ADSS OCSP Server meets the IETF RFC 6960 and RFC 5019 standards. The product is FIPS 201 certified (GSA APL #1411). It also meets the CWA 14167-1 security requirements for trustworthy systems.

Interoperability: ADSS OCSP Server has been tested with Windows Certificate Server, Entrust Security Manager, Verizon UniCERT, Primekey EJBCA and other CAs. ADSS OCSP Server can be used with any standards based CA that publishes CRLs to HTTP/S or LDAP/S locations. A full certificate status (whitelist) checking option is also available.

Advanced CRL processing: ADSS OCSP Server includes a high-performance CRL Monitor service that imports and quickly processes large CRLs ensuring that the latest revocation information is always available. Multiple HTTP/S and LDAP/S CRL locations can be accessed and high availability is supported using watchdog processing. CRLs can be re-published to a defined location.

High-Availability: ADSS OCSP Server is easily configured to offer high scalability and availability to meet the most demanding infrastructure needs. Multiple load balanced servers can work concurrently and resilient secondary sites can also be established.

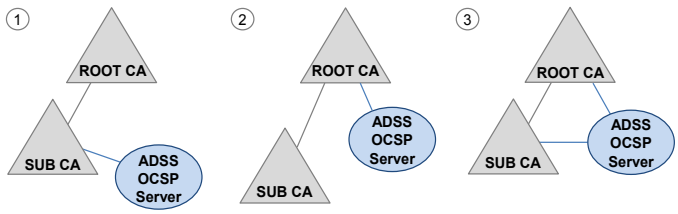
Advanced Management: The core services within ADSS OCSP Server can be split to allow separate back-end servers to process CRLs and front-end servers to handle pure OCSP requests and responses.

Advanced Features

Secure Logging:

Another key feature for operations staff is the ability to log all requests and responses and to allow an operator to quickly review a transaction in detail so that issues can be resolved in minutes. This is a must-have feature for any operations management team

Establishing Trust: ADSS OCSP Server supports multiple trust models as shown below. All common types of trust schemes can be supported, with ADSS OCSP Server certified by a Root CA or a subordinate CA, or both or even using a self-certified approach.



Intelligent OCSP Routing: ADSS OCSP Server supports both automated and manual routing of OCSP requests to peer OCSP responders. Automated routing requires support for AIA extension in certificates and since not all PKI certificates have this extension ADSS OCSP Server has a unique manual routing mechanism to ensure interoperability.

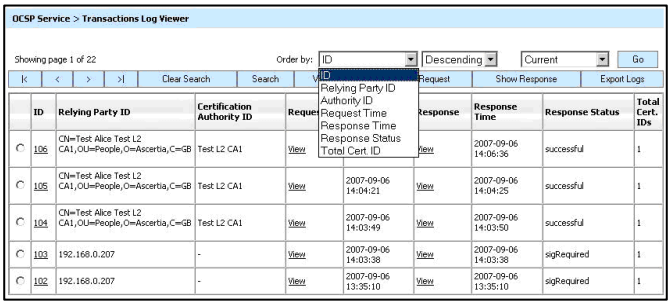
ADSS Server – High Trust OCSP Services

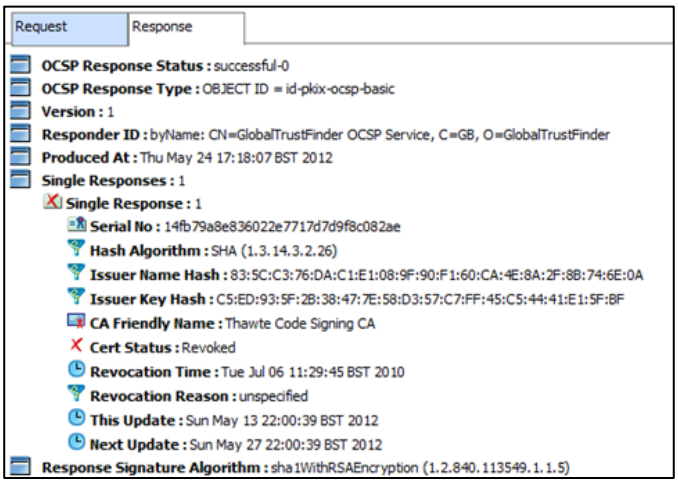
The Business Need

Digital certificates can provide individuals and companies with trustworthy identities for use within the e-commerce world. However, these digital certificates can expire, be revoked, or can be stolen. In order for digitally signed transactions to become a part of everyday business life, users must have trust and confidence that the digital identities of third parties are still valid and trusted for the transaction being conducted.

Ease of Use

The installation experience is simplified by using a wizard to help operators to configure the database, main operator account, trust model and HSM details, plus the CAs, their validation policies, the CRL monitoring and event reporting. The detailed reporting capability is highlighted below showing how privileged operators can drill into transactional details – in this case an OCSP response.





ADSS OCSP Server is an advanced OCSP responder that supports multiple CAs, multiple validation policies, 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.

Advanced Deployment Options

ADSS OCSP Server can be deployed in sophisticated ways to maximize performance. Logging levels can be controlled and CRLs used in memory to boost performance. The OCSP service, CRL Monitor service and database can all be deployed on separate servers. Distributed OCSP services and OCSP Repeater servers are available on request.

Management Control and Reporting

Detailed role based access controls make it easy to give staff the rights they need, for instance allowing help-desk staff to access log information so they can help customers whilst ensuring that they cannot view or change any configuration data.

ADSS OCSP Server creates detailed event and transaction logs that can be used to create usage reports and identify high demand users, certificates or IP addresses. Advanced management reporting is provided as a standard feature.

Related Test and Monitoring OCSP Products

OCSP Monitor is a valuable management application for monitoring one or more OCSP responders by sending test requests and checking if the correct response is provided. A number of scenarios can be configured to run on a frequent or infrequent basis. Alerts can be configured with an email sent to specified staff members when the responses are seen as either incorrect or off-line. OCSP Monitor can also send a daily summary to specified users to show the key statistics of the service.

The **OCSP Client Tool** ensures that OCSP systems are operating effectively and to specification. The tool is of value during PKI installation, operation & maintenance.

Ascertia **OCSP Crusher** is a useful tool for PKI administrators and testers involved in testing OCSP servers. It allows administrators to stress test an OCSP server with a selectable large number of OCSP requests, enabling operations managers to prove how their systems respond to varying load conditions.

ADSS OCSP Server Standards Compliance:

Certificate validation:	X509 v3 certificates, CRLv2, Real-time certificate status data and delta CRLs used with any standards compliant CA.
Certificate generation:	Generates PKCS#10 and accepts PKCS#12, PKCS#7, X.509v3 Certificates for signing responses, requests and logs
Algorithms and keys:	RSA 1024, 2048, 4096, 8192, ECDSA 256, 384, 521, SHA1, SHA-256, SHA-384, SHA-512, RIPEMD
Operating systems:	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
Interfaces:	HTTP and HTTPS communications for OCSP requests/ responses, HTTP/S and LDAP/S for CRL Monitoring
Operator interface:	Mutually-authenticated HTTPS secure web-interface for administrators, plus email, SMS, SNMP & syslog alerting

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 203 633 1177
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

Signed by: Rod Crook
Signed at: 2017-11-14 18:26:09 +00:00
Reason: I approve this document