ADSS OCSP Server

Common Criteria Certified Validation Authority

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

OCSP Overview

Digital certificates provide individuals, organisations, applications, and devices with trustworthy digital identities for use within the digital world. However, these digital identities can expire, be revoked, or can be stolen. In order for digital identities to be used in everyday business life, there must be trust and confidence that the digital identities of third parties are still valid and trusted for the transaction being conducted.

There are two approaches when it comes to validating a digital identity, Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP).

CRL's are created by Certification Authorities and are a single signed list of certificate serial numbers that are no longer considered to be trusted, CRL's need to be downloaded by end entities and processed to check for serial numbers of certificates that are no longer trusted. In this approach a CRL file can grow to an unusable size in a deployment with thousands of digital identities.

OCSP provides end entities a far more scalable and efficient means for end entities to check to see if a digital identity is still trusted. With OCSP, and end entity makes a request to an OCSP Server to check the validity of a certificate. This request checks the specific certificate serial number with a trusted Certificate Authority and an OCSP response is sent back with a response of either 'good', 'revoked' or 'unknown'. In this approach the end entity constructs a simple efficient OCSP query and in milliseconds receives a response instead of having to download and process potentially large CRL files (tens of seconds).

OCSP provides the additional benefit of providing real-time revocation information from a Certification Authority and the ability to check to see if the Certification Authority issued the certificate in the first place!

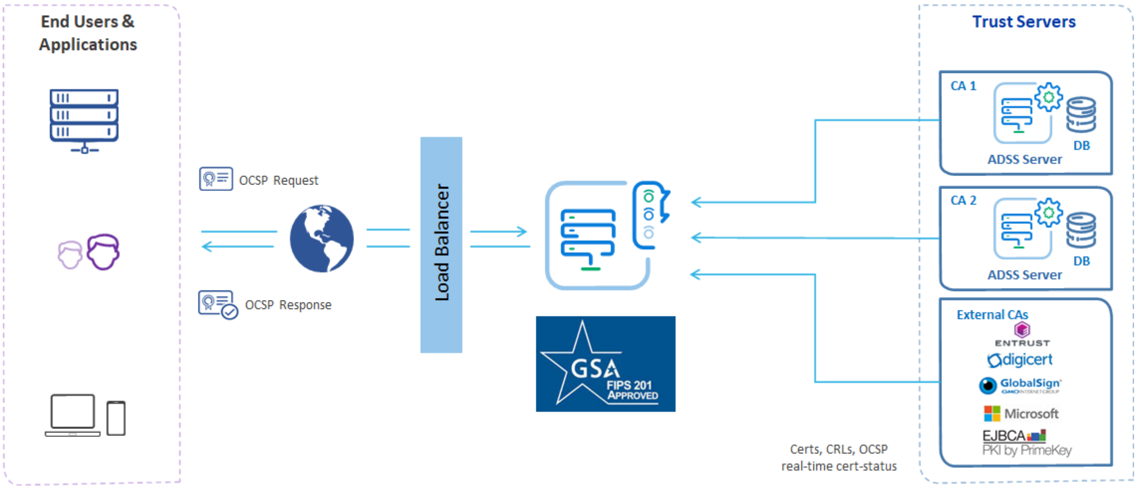
Key Features

- **Standards Compliance**: Fully compliant with RFC 6960, RFC 5019, and RFC 8954, has undergone FIPS 201 certification.
- **Third Party Certifications**: Common Criteria EAL 4 certified, meeting the requirements of the NIAP Protection Profile for Certification Authorities Version 2.1 (2017)
- **Interoperability**: Tested with Microsoft Active Directory Certificate Services, Entrust Security Manager, Primekey EJBCA, and other CAs that publish CRLs to HTTP/S or LDAP/S locations. A white-list revocation checking and certificate status option is also available for CAs that support this.
- **Advanced CRL processing**: 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**: 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.
- **Distributed Architecture:** 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. Customers may also take advantage of ADSS OCSP Gateway as an option to protect multi-Tier datacentres

ADSS OCSP Server Architecture

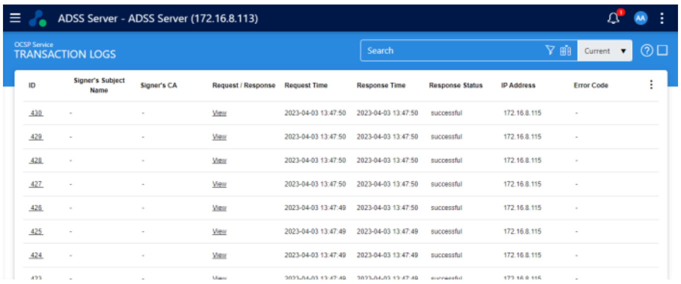
ADSS OCSP Server is a high performance, robust and reliable OCSP Validation Authority that complies with the RFC 6960 and RFC 5019 standards. It is FIPS 201 Certified (APL #1411 replacing APL #583) confirming that it meets all the requirements and is approved for use by US federal agencies for their 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. ADSS OCSP Server can also able to be used as a secure front-end OCSP Server for third party OCSP Servers that have to be positioned close to the issuer CA.

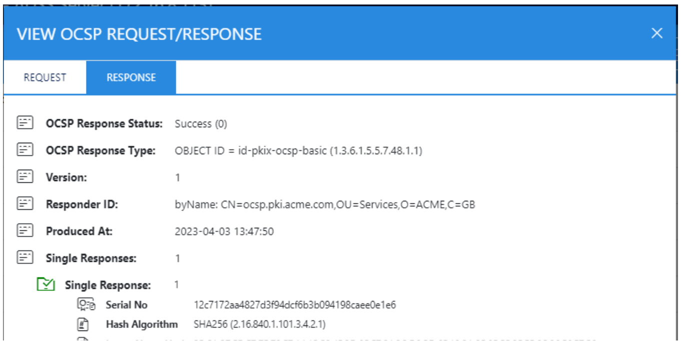


Ease of Use

Product installation is simplified by using a wizard to guide 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.



ID	Signer's Subject Name	Signer's CA	Request / Response	Request Time	Response Time	Response Status	IP Address	Error Code
430	-	-	View	2023-04-03 13:47:50	2023-04-03 13:47:50	successful	172.16.8.115	-
429	-	-	View	2023-04-03 13:47:50	2023-04-03 13:47:50	successful	172.16.8.115	-
428	-	-	View	2023-04-03 13:47:50	2023-04-03 13:47:50	successful	172.16.8.115	-
427	-	-	View	2023-04-03 13:47:50	2023-04-03 13:47:50	successful	172.16.8.115	-
426	-	-	View	2023-04-03 13:47:49	2023-04-03 13:47:50	successful	172.16.8.115	-
425	-	-	View	2023-04-03 13:47:49	2023-04-03 13:47:49	successful	172.16.8.115	-
424	-	-	View	2023-04-03 13:47:49	2023-04-03 13:47:49	successful	172.16.8.115	-



OCSP Response Status: Success (0)
OCSP Response Type: OBJECT ID = id-pkix-ocsp-basic (1.3.6.1.5.5.7.48.1.1)
Version: 1
Responder ID: byName: CN=ocsp.pki.acme.com,OU=Services,O=ACME,C=GB
Produced At: 2023-04-03 13:47:50
Single Responses: 1
Single Response: 1
Serial No 12c7172aa4827d3f94dcf6b3b094198caee0e1e6
Hash Algorithm SHA256 (2.16.840.1.101.3.4.2.1)

Advanced Features

Secure Logging: Every request and response is securely logged to enable operators to quickly review transactions in detail and resolve issues in minutes.

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.

Performance Tuning: ADSS OCSP Server provides the ability to fine tune the deployment to make best use of the platform on which the product is operating, this in turn enables organisations to tune OCSP performance to meet the needs of their business.

Advanced Features (Cont.)

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.

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.

Ascertia provides a Performance Management tool to enable 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 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.

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 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