ADSS PKI Server

Common Criteria Certified PKI Server

ADSS PKI 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.

Digital Trust Overview

Digital Business defines the transition of analog processes to the digital world, this global movement has seen the digitization, streamlining and improvement of digital interactions, everything from buying goods and services, conducting financial transactions, to streaming media and entertainment. In order to conduct digital business, you must be able to trust the identity of the person, application or service you are communicating with, this requires digital trust.

Digital trust is established by issuing and managing digital identities from trust infrastructures, these are built and operated by trusted third parties, trust services teams within an organization or commercial entities, a key part of the issuance and management process includes secure vetting processes, this ensures each and every identity that is created are issued to a real and verified businesses, servers or people.

ADSS PKI Server is core to providing digital trust, used the world over by trust service providers, businesses, and governments, ADSS PKI Server delivers a highly secure and scalable trust services platform upon which can be built services to issue digital certificates to people, devices and applications to provide digital trust, the foundation to digital business. ADSS PKI Server offers a robust certification authority service, which enables operators to build as many Trusted Certification Authorities as they need in order to create a simple or as complex trust infrastructures as their business requirements demand, ADSS PKI Server also offers a highly scalable and performant Online Certificate Status Protocol (OCSP) service which enables the validation of all digital identities issued by an ADSS Server based CA.

Digital identities issued from trust infrastructures are fundamental to security online, providing authenticity, integrity, protection of information, Public Key Infrastructure is a key foundation to securing digital business.

Key Features

- **Standards Compliance**: Fully compliant with RFC 5280, RFC 6960 and RFC 5019, has undergone FIPS 201 certification.
- **Third Party Certifications**: Common Criteria EAL 4+ ALC_FLR.3 certified, meeting the requirements of the NIAP Protection Profile for Certification Authorities Version 2.1 (2017)
- **Support for Classic and Quantum Resistant Cryptography:** ADSS PKI Server provides support for generating keys and certificates using the following algorithms:
  - RSA & ECDSA
  - FIPS 204 (CRYSTALS Dillithium)
  - FIPS 203 (Kyber)
  - FIPS 205 (SPHINCS+)
  - Classic McEliece
- **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:** ADSS PKI Server can be deployed with ADSS Web RA Server to offer a fully distributed digital trust issuance model.
- **Multiple PKI Support:** ADSS PKI Server enables multiple CA's to be run from a single installation of ADSS Server, this enables the consolidation of CA's to a Highly redundant installation to reduce PKI TCO.

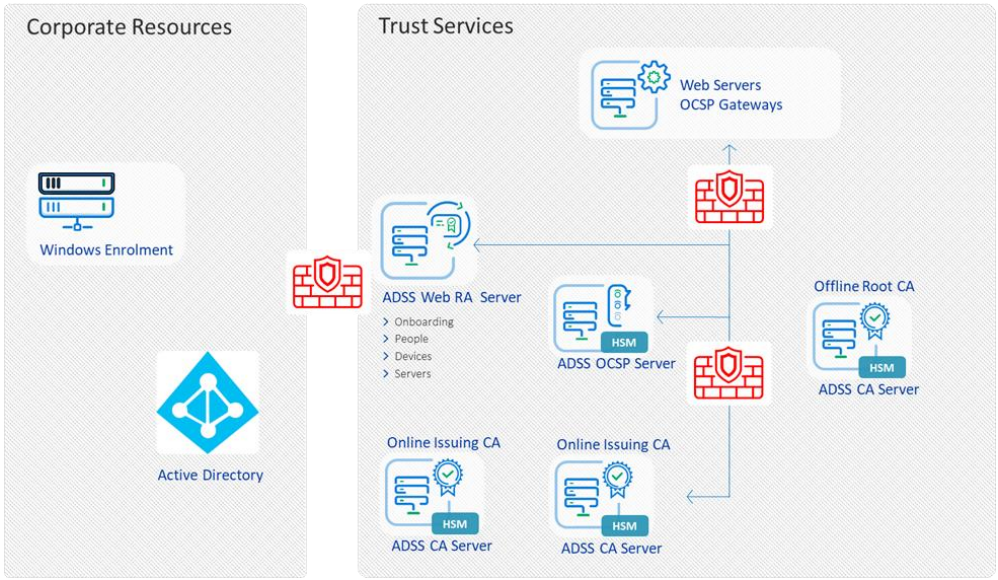
ADSS PKI Server Architecture

ADSS PKI Server includes both a Certification Authority (CA) Service and Online Certificate Status Protocol (OCSP) Service, that can be deployed by Trust Service Providers and Enterprise to meet a variety of digital business use cases. ADSS Server provides a high performance, robust and reliable CA and OCSP Validation Authority that complies with the RFC 5280, RFC 6960 and RFC 5019 standards. ADSS PKI Server is Common Criteria EAL 4 Certified and meets the requirements of the National Information Assurance Partnership Government Approved Protection Profile for Certification Authorities v.2.1 (2017), this means that ADSS PKI Server is certified to the very latest CA protection profile and to a high assurance level.

ADSS PKI Server provides support for the creation of a wide variety of certificate profiles to enable digital identities to be generated to support digital trust use cases and can enable be used by trust service providers and organizations to build multiple trust infrastructures on a single installation of ADSS Server, which can then be operated in a high availability, active \ active configuration, thus reducing the total number of servers required in a deployment.

ADSS PKI Server can provide 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.

When deployed with its sister product ADSS Web RA Server, ADSS PKI Server delivers the most comprehensive digital trust solution, enabling businesses and trust service providers to deliver certificate issuance and management across a wide selection of digital trust use cases.



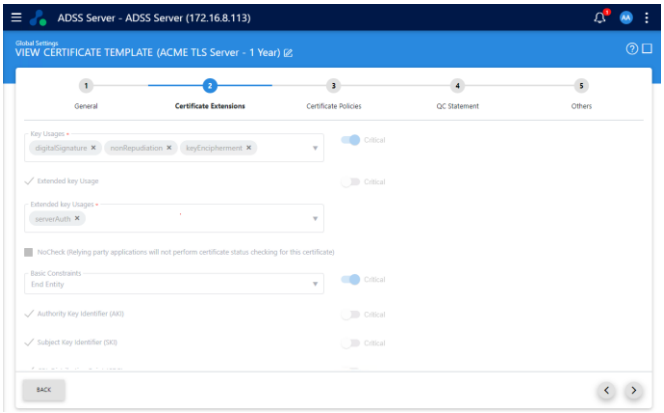
Ease of Use

Product installation is simplified, using a wizard to guide operators to configure the database, main operator account(s), trust model(s) and HSM details, plus the CAs, their validation policies, the CRL monitoring and event reporting.

Administration is provided by an intuitive browser-based administration console, each operator is authenticated via a client TLS certificate and only provided access to product functions according to their role within the product.

An example of a certificate template is shown opposite, operators can very easily create new certificate templates in a simple to use interface.

Certificate Template Management



Advanced Features

Performance Tuning: ADSS PKI 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 performance to meet the needs of their business.

ePassport Options: ADSS PKI Server not only supports the issuance and management of X.509 digital certificates, ADSS PKI Server also supports the issuance and management of **ISO 7816** Card Verifiable Certificates.

ADSS PKI Server can be deployed in support of Passive Authentication which is used during the verification of electronic machine-readable travel documents, ADSS PKI Server can act as a **Country Signing Certification Authority (CSCA)** and is fully compliant with **ICAO 9303**.

ADSS PKI Server can issue and manage digital certificates that can be issued to border control workstations in support of Extended Access Control (**EAC**), ADSS PKI Server can be operated as **a Country Verifying Certification Authority (CVCA)** or a **Document Verifying Certification Authority (DVCA)** to issue Inspection System Certificates to domestic border control systems or via the **Ascertia SPOC** to international DVCA's to enable domestic travel documents and their holders to be verified abroad.

Management Control and Reporting: Detailed role-based access controls makes 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 PKI 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.

ADSS PKI Server is an advanced trust services platform that supports multiple CAs and multiple OCSP Validation Authorities from a single instance. It can support 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, AlmaLinux

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 Security Server
Microsoft Azure Key Vault
Amazon AWS Cloud HSM (Linux Only)

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