ADSS Server - Release Notes

This document provides a high-level description of the new features in ADSS Server.

ADSS Server v8.0 — February 2023

ADSS PKI Server Common Criteria Release:

ADSS PKI Server is certified to Common Criteria EAL 4 against the 2017 National Information Assurance Partnership (NIAP) Protection Profile for Certification Authorities version 2.1, which is the latest protection profile available for Certification Authorities.

ADSS Server is a modular trust services platform that is core to providing digital trust and is used the world over by trust service providers, governments and global organisations. ADSS Server delivers a highly secure and scalable trust services product, upon which can be built services to issue digital certificates to people, devices and applications providing digital trust, the foundation of digital business.

ADSS PKI Server delivers all of the components required to issue, validate and manage X.509 and ISO 7816 Card Verifiable Digital Certificates. Ascertia's ADSS Server also provides a high performance OCSP solution for the validation of digital certificates, can provide real-time revocation and certificate whitelisting, and can be leveraged as a certificate validation hub for multiple CA's.

ADSS PKI Server is a next-generation PKI solution that manages the complete life cycle of public key certificates based on the X.509 standard and IETF Internet Standard protocols. It is suitable for Public and Private Trust Models, as well as National CAs, ePassport and Qualified Trust Service Providers (QTSPs).

New Features

- **ADSS Server CA support for Enrolment over Secure Transport (EST - RFC 7030) - (ADSS-15443)**
  The ADSS Server Certification Service has been enhanced to support RFC 7030 - Enrolment over Secure Transport**,** a REST interface used to generate, renew/rekey and revoke certificates.

- **Support for CA/B Forum 1.8.4 - (ADSS-10197)**
  ADSS Server has been updated to support CA/B forum guideline version to v1.8.4 for certificate issuance.

- **Enhanced implementation to access ADSS Server Console - (ADSS-15293)**
  ADSS Server has been enhanced to allow operators to access ADSS Server console, when operator's certificate revocation source is not available.

- **Security Banner for accessing ADSS Server Console - (ADSS-15291)**
  The ADSS Server has been enhanced to enable organisations to show a Security Banner prior to operators accessing the ADSS Server Console.

- **HMAC Verification Security - (ADSS- 15295)**
  ADSS Server HMAC verification will now terminate ADSS Server services if the HMAC verification process discovers any alteration to ADSS Server database records.

Tested Operating Systems

Operating System	Tested Version(s)
Microsoft	Windows Server 2016, 2019, 2022
Linux	RedHat 7.x, 8.x CentOS 7.x, 8.x SUSE

Tested Database Servers	Tested Version(s)
Microsoft	SQL Server 2019, 2017, 2016 (Express, Standard and Enterprise Editions) Azure SQL Database (Database-as-a-service)

Oracle	Database 19c (Standard Edition, Enterprise Edition) MySQL 8
Percona	XtraDB-Cluster 5.7, 5.8, 8.0.23
Postgres	13, 12, 11, 10

Tested Hardware Security Module(s)

HSM Vendor	HSM Firmware	HSM Software	HSM Client
Utimaco CP5 SE	5.1.0.0	N/A	5.1.1.1
Utimaco CryptoServer SE Gen2	4.45.3.0	N/A	4.45.3.0
Entrust nShield	12.60.15	N/A	12.70.4
Thales Luna	7.7.0.0-317	7.7.0	10.3 10.4
Thales Protect Server	Testing conducted using Protect Server Simulator v5.9		
Microsoft Azure Key Vault	N/A	N/A	N/A
Amazon Cloud HSM *	N/A	N/A	3.2.1
Notes: * Amazon Cloud HSM Tested on Linux only			

ADSS Server Product Compatibility

Product	Version(s)
ADSS Client SDK - Java	7.1, 7.0.2, 6.9
ADSS Client SDK - .Net	7.1, 7.0.2, 6.9
ADSS Go>Sign Desktop	7.1, 7.0.2, 6.9
ADSS Auto File Processor	7.1, 7.0.2, 6.9

For further details contact us on sales@ascertia.com or visit www.ascertia.com

*** End of Document ***