ADSS Server - Release Notes

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

ADSS Server v8.2 July 2023

New Features

- **New ADSS Server Access Control restrictions – (ADSS-7597)**
  A new ADSS Server access control module allows operators to assign administrators with access to specific Managed CA's and Certification Profiles. This helps managed service providers and enterprises create CA's with a specific set of operators and ensures CA operators can only access CA's they have permissions to see and manage.

- **Support for General Name attributes – (ADSS-8386)**
  ADSS CA Server has been enhanced to support General Name attributes in both Subject Alternative Name (SAN) and Issuer Alternative Name (IAN) extensions.

  Expanded General Name Support:
  - Adds support for all General Names as defined in RFC 5280.
  - General Names now include options such as otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, and registeredId.

  UserPrincipalName as SAN Value:
  - Added the ability to set UserPrincipalName as a SAN value.
  - UserPrincipalName is commonly used in smartcard logon and authentication projects involving certificates.

- **Support for DigiCert One – (ADSS-17463)**
  ADSS Server now supports DigiCert One as an external CA. Customers can now use ADSS Server to perform full certificate lifecycle management of certificates issued by the DigiCert One Certification Authority.

- **Support For Entrust CA Gateway – (ADSS-18506)**
  ADSS Server now support Entrust CA Gateway (**v2.7.10)** as an external CA. Customers can now use ADSS Server to perform full certificate lifecycle management of certificates issued via the Entrust CA Gateway to Entrust Security Manager.
  Note: The Entrust CA Gateway does not support certificate enrolment where the subject distinguished name contains "Title", this is a known issues and will be updated in a future release.

- **Support for IDP and Explicit based authentication in ADSS Signing Server – (ADSS-18570)**
  ADSS Signing server has been enhanced to support IDP and Explicit(PIN) based authentication for user in remote signing via RAS

New Enhancements

- **Support of CDP extension for Self-Signed Certificates – (ADSS-15842)**
  This enhancement allows CA Operators to add the CDP extension for self-signed Certificates.

- **Enhanced Azure Key Vault to support RSASSA-PSS signature scheme - (ADSS-14857)**
  ADSS Server has been enhanced to support RSASSA-PSS Signature Scheme and EC NIST-P 384 and 521 key sizes for Azure Key Vault Crypto Sources.

- **Support for the Legal Person Semantic Identifier extension in qualified certificate - (ADSS-10444)**
  Organization Identifiers (OI) is now supported in the Subject DN according to the format outlined in ETSI TS 119 412-1 v1.4.1.

- **Detection of ROCA and ECC Vulnerabilities – (ADSS-12464)**
  ADSS Server has been enhanced to detect ROCA and ECC vulnerabilities when certifying the keys via ADSS Manual Certification or ADSS Certification Service.

- **Support for SHA-3 Hash Algorithm in ADSS Server – (ADSS-15096)**
  ADSS Server has been enhanced to support the SHA-3 hash algorithm for all services.

- **Updated JDK Version - (ADSS-17724)**
  The JDK version has been updated to 11.0.19.

- **Apache Tomcat version upgrade - (ADSS-17725)**
  Apache Tomcat has been upgraded to version 9.0.76.

- **Jar file updates - (ADSS-17726)**
  Third party jars have been updated.

Discontinued Features

- **Percona XtraDB Cluster v5.x Support**

  ADSS Server no longer supports Percona XtraDB Cluster v5.x

Note

- **Symantec MPKI CA Support**

  This will be the last version of ADSS Server to support the Symantec MPKI CA external CA connector.

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 Ubuntu 20.x, 22.x

Tested Database Servers

Database Servers	Tested Version(s)
Microsoft	SQL Server 2022, 2019, 2017, 2016 (Express, Standard and Enterprise Editions) Azure SQL Database (Database-as-a-service)
Oracle	12c, 19c (Standard Edition, Enterprise Edition)
MySQL	8.0.x
Percona	XtraDB-Cluster 8.0.23
Postgres	14, 13, 12, 11

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 12.81.2
Thales Luna	7.7.0.0-317	7.7.0	10.3

	7.7.1-188	7.7.1	10.4 10.5
Thales Protect Server	• PTK 7.1 Client Software for ProtectServer 3 • PTK 7.0 Client Software for ProtectServer 3 • PTK 5.9 Client Software (ProtectServer Client Software 5.9.1)		
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	8.2, 8.1, 8.0, 7.1
ADSS Client SDK - .Net	8.2, 8.1, 8.0, 7.1
ADSS Go>Sign Desktop	8.2, 8.1, 8.0, 7.1
ADSS Auto File Processor	8.2, 8.1, 8.0, 7.1

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

*** End of Document ***