ADSS Server - Release Notes

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

ADSS Server v7.0.2 April 2022

ADSS Server SAM Appliance Common Criteria Release:

This is the Common Criteria EAL4+ certified version of the ADSS Server SAM Appliance that supports the EU eIDAS Regulation (EU) 910/2014 requirements for Remote Qualified Signatures evaluated against the industry-standard EN 419 241-2 Protection Profile. This allows creation of server-side natural person Qualified signatures and legal entity Qualified eSeals, which meet the Sole Control Assurance Level 2 (SCAL2) requirements to prove that a centrally held signing key was only used for signing or sealing after the appropriate authorisation of its owner. Sole Control Assurance Level 1 is also supported in this version to support business requirements, which do not require the highest-level of trust.

The Ascertia ADSS Server SAM Appliance v7.0 is a Remote Qualified Signature Creation Device (QSCD) that runs within a tamper-protected hardware appliance designed to meet FIPS 140-2.

ADSS Server v7.0 is qualified to work with the EN 419221-5 Common Criteria EAL4+ certified HSMs from Entrust, Thales and Utimaco. These HSMs provide the extra security required for EU eIDAS compliant remote Qualified Signatures and eSeals. This version of ADSS Server also offers new key authorisation interfaces including SAML and OpenID connect to strictly control all aspects of key generation and usage.

ADSS Server 7.0.2 software can also be installed and operated on supported Windows and Linux platforms with an eIDAS certified HSM to use the ADSS SAM Service features if required. This is not a certified solution but it does support remote signing for other PKI solution requirements such as signing using AATL certificates. An HSM emulator can also be used for lower cost test and development environments.

Common Criteria Certified Features

These EN 419 241-2 remote signing features are Common Criteria certified to EAL 4+:

- **Support for nCipher HSMs certified to EN 419 221-5 - (ADSS-12874)**

  ADSS Server SAM Service now supports remote signature creation using Entrust nShield XC HSMs certified to ETSI EN 419 221-5
- **Support for Thales Luna HSMs certified to EN 419 221-5 - (ADSS-8345)**

  ADSS Server SAM Service now supports remote signature creation using Thales Luna HSMs certified to ETSI EN 419 221-5
- **Performance enhancement when using UtimacoCP5 HSM - (ADSS-5668)**

  The ADSS Server SAM Service has been enhanced to improve system performance when using Utimaco CP5 HSMs
- **IDP/IAM for authentication/authorisation of remote signatures- (ADSS-11472)**

  ADSS Server has now been enhanced to support external authorization servers (IdPs) for authentication/authorization of remote signatures using SAML or OpenID Connect
- **SCAL1, SCAL2 remote signing and eSealing in ADSS Server - (ADSS-12305)**

  ADSS Server supports eSeals authorised using Sole Control Assurance Level 2 (SCAL 2) and can now produce also signatures and eSeals using Sole Control Assurance Level 1 (SCAL1) in RAS/SAM services
- **Time tolerance configuration for device certificate validation in SAM service - (ADSS-8323)**

  The ADSS Server SAM Service now allows administrators to set a tolerance in seconds for the system to validate signature activation data where system clocks may not be fully synchronised
- **Maximum number of authorisation devices per user – (ADSS-9057)**

  The ADSS Server SAM service now allows operators to specify the maximum number of devices a user can use to authorise remote signing operations.
- **Enhanced the SAM Service to load eSealing keys to HSM's for configured intervals to support Bulk Signing use cases (ADSS-14915)**

  eSealing keys can be loaded into the HSM until the Signature Activation Data (SAD) provided by the owner expires or until the signature count configured in the SAM profile is reached. This helps to increase performance in bulk signing use cases by ensuring the eSeal key is available inside the HSM when needed but ensuring its removed based on time limit or after configured number of signatures.

New Features

- **Enhancements on Crypto Source screen in Key Manager (ADSS-14912)**
  A new type of "Other" crypto source has been added in the dropdown that will allow ADSS Server operators to configure custom crypto source settings.
- **Enhancements to Key Templates screen in Key Manager (ADSS-14913)**
  Key Templates in Key Manager have been enhanced by adding "PKCS#11" and “EN 419221-5” types to allow template management.

New OS and Database Support

- **RedHat v8.x Support**
  ADSS Server now supports RedHat v8.4 & RedHat v8.5
- **CentOS v8.x Support**
  ADSS Server now supports CentOS v8.3
- **Percona v8.0 Support**
  ADSS Server now supports Percona v8.0.23
- **MSSQL 2019 Support**
  ADSS Server now supports MS SQL Server 2019

Discontinued Features

- **PostgreSQL v9.5 Support**
  ADSS Server no longer supports PostgreSQL v9.5.
- **MySQL v5.5 and v5.6 Support**
  ADSS Server no longer supports MySQL v5.5 and v5.6.
- **Oracle 18c Support**
  ADSS Server no longer supports Oracle 18c

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 Database	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
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	6.9, 6.8
ADSS Client SDK - .Net	6.9, 6.8
ADSS Go>Sign Desktop	6.9, 6.8
ADSS Auto File Processor	6.9, 6.8

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

*** End of Document ***