ADSS Server - Release Notes

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

ADSS Server v8.3.3 — March 29, 2024

Release Summary:

The latest release of ADSS Server features the introduction of a new service “Unity Service” and a new Crypto Profile “Azure Managed HSM”. Significant performance improvements have been made to both the Signing Server and Verification Server. Additionally, various security enhancements have been implemented to strengthen the system’s robustness.

New Features

1. **ADSS Server Unity Service** – (ADSS-16929)

   ADSS Server has been enhanced to deliver a new service to simplify the integration of business applications with Ascertia products. The Unity Service supports the latest Cloud Signature Consortium (CSC) version 2 APIs and an initial set of Business APIs. This includes a new, /signDoc API, which enables the signing of entire documents, generating advanced digital signatures including PAdES, XAdES, and CAdES.

   The Unity Service also introduces a new system for managing short-term certificates, ensuring direct communication with the ADSS Server SAM Service. It encompasses all mobile APIs previously supported by the RAS Service, as well as client APIs for user registration. The ADSS Server Unity Service, facilitates direct interaction with other ADSS Server components and external service providers, including IDPs and SMS gateways.

   Access to Unity Console:
   The Unity Service is exclusively accessible through the Unity Console for ADSS Server Operators. Consequently, Operators will need to follow the instructions below to access the Unity Console:
   1) Open the ADSS Classic Console.
   2) On Classic Console dashboard, navigate to the top banner.
   3) Click on the Unity Console option, the user will be navigated to the Unity Console dashboard.

New Enhancements

1. **ADSS Server Certificate Templates Update** – (ADSS-21645, ADSS-21644)

   ADSS Server certificate templates have been updated to support the custom certificate extension “ext-valassured-ST-certs” as defined in ETSI EN 319 412-1 "5.2 Certificate Extensions regarding Validity Assured Certificate", this is used by CA’s when issuing short life certificates.

   ADSS Server certificate templates in Unity Console have also been updated to include the Subject Directory Attributes extension as defined by RFC 3739 to include “dateOfBirth” and “placeOfBirth” in certificates to ensure compliance with ETSI EN 319 412-1 “5.1.5 eIDAS eID Natural person semantics identifier”.

2. **Support for Azure Managed HSM** – (ADSS-20821)

   ADSS Server 8.3.3 introduces support for Microsoft Azure Managed HSM as a new Crypto Source in Key Manager. The updated Key Vault API is compatible with Azure Managed HSM, offering backup and restoration capabilities and support for key wrapping. Users can now back up keys from Azure Managed HSM, securely store them in the ADSS Server database, and then remove them from Azure Managed HSM. These keys can be restored to Azure Managed HSM later for signing operations.

3. **ADSS Signing Server Performance Improvement** – (ADSS-20818)

   ADSS Signing Server performance has been improved for signing profiles that support document hashes for CAdES detached signatures. Additionally, it has been updated to return the complete signature through a CallBack URL, rather than just the requestID. This is achieved by establishing a

secure, authenticated channel with the business application using OAuth 2.0 authentication, which enhances performance in the Remote Authorised Signing flow.

4. **ADSS Verification Server Performance Improvement** – (ADSS-20819)

   ADSS Verification Server performance has been improved to validate signatures using both the signature itself and the document or content hash. It now has the ability to verify multiple signatures within a single request. Performance enhancements have been achieved by reducing and optimizing database calls and by caching frequently used objects.

5. **ADSS RAS Server Secure APIs** – (ADSS-20604)

   ADSS Server has introduced a new security feature for its REST APIs provided by the ADSS RAS Service. This feature can be activated by turning on the BUSINESS_API_AUTHENTICATION setting in the RAS Server's Advanced Settings. The business APIs now operate in two modes: one that maintains compatibility with previous versions without requiring authentication, and another that uses OAuth 2.0 with ClientID and secret for secure, authenticated access.

6. **New API to retrieve all certificates from a given CA** – (ADSS-19980)

   The "Get Certificates" API in ADSS Server has been improved to provide a list of certificates from a specified Certification Authority (CA), which can be either local or external. Additionally, it now supports returning PKCS_10 and PKCS_12 formats in the response when these are specified in the 'respondWith' parameters.

7. **Support for new RDNS in ADSS Server** – (ADSS-19981)

   ADSS Server now includes support for the new Relative Distinguished Name (RDN) 'Domain Component' in the subject's distinguished name. ADSS Server based CA's can now issue certificates with DC= in the subject distinguished name which is required for interoperability for Microsoft Active Directory use cases.

8. **Upgraded Tomcat** – (ADSS-XXXXX)

   The ADSS Server has been upgraded tomcat from v9.0.83 to v9.0.85.

New OS and Database Support

- **RedHat v9.0 Support**
  ADSS Server now supports RedHat v9.0
- **AlmaLinux v9.3 Support**
  ADSS Server now supports AlmaLinux v9.3
- **Oracle v21c Support**
  ADSS Server now supports Oracle v21c
- **PostgreSQL Server Support**
  ADSS Server now supports Postgres SQL 15 and Postgres 16
- **MySQL v8.0.36 Support**
  ADSS Server now supports MySQL v8.0.36

Discontinued Features

- **PostgreSQL v11 Support**
  ADSS Server no longer supports PostgreSQL v11
- **CentOS v7.x and v8.x Support**
  ADSS Server no longer supports CentOS v7.x and v8.x

For full details of tested Operating System's, Databases, Hardware Security Modules and 3rd party component, please review the Ascertia Platform Support Report for ADSS Server:

https://www.ascertia.com/product-documentation/platform-support/

ADSS Server v8.3.2 January 2024

New Features

- **Introduced new installer for Regular Release – (ADSS-20751)**

  Introducing ADSS 8.3.2 with a streamlined installation option for regular releases, allowing users to seamlessly install incremental updates comprising improvements and bug fixes. This version offers increased adaptability through simplified procedures, such as automated backup, smooth file replacement, executing database scripts, guaranteeing a frictionless installation flow and the ability to revert changes in the event of failures.

New Enhancements

- **Migration from .NET framework 4.5 to .NET Core 8.0 – (ADSS-20454)**
  ADSS Server has been migrated from .NET framework (4.5) to .NET core (8.0)

- **Upgraded Tomcat – (ADSS- 20782)**
  The ADSS Server has been upgraded tomcat from v9.0.76 to v9.0.83

- **Upgraded OpenJDK – (ADSS- 20783)**
  The ADSS Server has been upgraded OpenJDK from 17.44+15 to 17.46+19

- **Enhanced flexibility of cache or deleting the key from the HSMs – (ADSS-20436)**
  A new functionality has been introduced in ADSS SAM Server to allow user to enable or disable the automatic removal of keys into the HSM after each eSeal signing operation

- **Enhanced functionality to reject duplicate pubic key – (ADSS-20289)**
  A new functionality has been added in the ADSS Certification Server to reject already certified public key in certificates created through certification service, key manager and manual certification.

ADSS Server v8.3.1 November 2023

New Features

- **ADSS Server Unity Console updates:**
  ADSS Server 8.3.1 introduces RAS and SAM Services within the new ADSS Server Unity Console, with plans for updating additional services in forthcoming releases. Operators can seamlessly switch between the ADSS Server Classic console and Unity console with a simple click

- **ADSS Verification Gateway document confidentiality – (ADSS-19291)**
  The ADSS Server Verification Gateway has been enhanced to achieve document confidentiality. The verification gateway will extract a document signature hash and send it to the verification server for signature verification and/or enhancement across all supported Signature Types (PAdES, CAdES, and XAdES).
  Verification Service within the ADSS Server Client SDK now possesses the capability to generate and verify timestamp tokens for provided hash or timestamp tokens, introducing a new signature format called Timestamp

- **Support for OpenJDK 17 – (ADSS- 14869)**
  The ADSS Server has been upgraded and enhanced to support OpenJDK version 17.44+15.

- **Import Signature Appearance – (ADSS- 17424)**
  ADSS Server now supports the ability to import signature appearances that have been created and exported from ADSS Server instances.

- **Go>Sign installation directory selection – (ADSS-15172)**
  Go>Sign Desktop installation process now enables users to select their preferred installation directory.

- **Support to provide an option CUSTOM_DATE in SAM Profile – (ADSS- 19286)**
  ADSS Server has been enhanced to incorporate a custom date setting this enables administrators to set a specific date within SAM profiles for SAD expiry.

- **Support of external authorization servers (IdPs) for service authorization in ADSS RAS Server – (ADSS- 17261)**
  The ADSS RAS service has been enhanced to support external authorization servers (IdPs) for service authorization via SAML or OpenID Connect.

New Enhancements

- **Enhanced ability to disable "Compute final hash at signing time" option when use padding scheme PSS – (ADSS-17762)**
  ADSS SAM Server console has been enhanced to support the disabling of the "compute hash at signing time" checkbox when the PSS padding scheme is selected. This modification enables the ADSS SAM Server to accept the both **Hash** and **signAlgoParam** parameter as a result of this change

- **Enhanced OpenID Connect User Identification in RAS/SAM via Custom Attributes – (ADSS-19387)**
  ADSS RAS/SAM server has been enhanced to enable user identification through custom attributes within assertion data via OpenID Connect IdP for external remote authorization

- **Enhanced RAS/SAM with separate Authorization Request expiry and SAD Request expiry – (ADSS-18888)**
  ADSS RAS/SAM Server now supports separate settings for SAD expiry and authorization request expiry, facilitating the management of expired authorization requests separately

- **Enhanced support of JSON-Based SAD for RAS/SAM Authorization – (ADSS- 19288)**
  ADSS RAS/SAM Server now supports JSON-based SAD for credentials authorization in RAS/SAM services.

- **Enhanced ADSS TSA Server to specify the list of supported Hash Algorithms – (ADSS- 13861)**
  Administrators can now specify a list of supported hash algorithms for the ADSS Server TSA service.

- **Enhancement of storage of data-to-be-displayed distinct from the SAD – (ADSS- 19289)**
  The ADSS Server now facilitates the separate storage of data-to-be-displayed distinct from the (SAD). This not only reduces the size of the SAD but also significantly enhances performance

- **Enhanced validation checks for Certificate generation – (ADSS- 17505/ ADSS- 17504)**
  Enhanced validation checks for reserved IP Address and Internal Names according to WebTrust and CA/B Forum guidelines in certificate generation for SSL and EV-SSL certificates

- **Enhanced integration with Thales Luna HSM for ADSS SAM Server – (ADSS- 19431)**
  The Thales Luna integration with ADSS Server has been upgraded improve the performance of key handling for remote authorised signing.

- **Enhanced the functionality to list all the pending requests – (ADSS- 18887)**
  ADSS Server now exposes an API to retrieve and display a list of all pending requests for a user

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

*** End of Document ***