ADSS Server 8.3.7

November 2024

This document provides information about Ascertia ADSS Server. Browse through the following topics to find out about new features, product enhancements, improvement, known issues, and limitations for this release.

For information related to tested 3rd party components such as operating systems, database servers, and Hardware Security Modules, please review Ascertia Platform Support, this can be found here: https://www.ascertia.com/product-documentation/platform-support/

Ascertia ADSS Server has successfully completed Common Criteria certification at the EAL4+ Assurance Level. For details, visit https://www.commoncriteriaportal.org/products/index.cfm, under Key Management Systems.

New Features

- **TSA Support for additional ISO/IEC Standards:**

  Jira ID – (ADSS- 18126)

  The ADSS TSA Server has been enhanced to comply with the ISO/IEC 18014-1 and ISO/IEC 18014-2 standards for the generation and verification of timestamp tokens. To enable this functionality, users are required to activate the 'ENABLE_ISO_IEC_18014_COMPLIANT_TSA' property within the Advanced Settings section under the TSA module, located in the Global Settings submodule.

- **ADSS Server CSP Service:**

  Jira ID – (ASAC-1734)

  The Ascertia Unity in ADSS Server introduces new modules such as CSP Service, 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.

Product Enhancements

- **Allow ADSS Core to Delete SAM Signed ARQs Regardless of Expiry**

  Jira ID – (ADSS- 22862)

The ADSS SAM Service has been enhanced to ensure that Authorized Requests (ARQs) with a "SIGNED" status are deleted prior to their expiry. This improvement effectively reduces database size and enhances overall performance.

User Signing:

- In User Signing, an Authorized Request (ARQ) is used only once for signing, and the user must generate a new Signed Authorization Data (SAD) for each subsequent signing operation.

- The core thread is responsible for removing ARQs with the "SIGNED" status once they reach their expiry, ensuring that expired ARQs are properly cleaned up to maintain system performance.

E-Seal Signing:

In e-Seal Signing, users can extend a transaction by reusing an old SAD and obtaining a new one. The new SAD is linked to the previous one through TransactionID chaining.

- When a user sends the old SAD to extend the transaction, a new ARQ is inserted into the database. The previous ARQ status is updated to "SIGNED," enabling the core thread to identify and delete it once it expires.

- After a successful signature in the sign API, the ARQ request is updated with the "SIGNED" status. However, for E-Seal Signing, the status is updated to "SIGNED_EXT_ALLOWED," indicating that the transaction can be extended.

This approach ensures efficient handling of ARQ records, supports seamless transaction extensions in E-Seal Signing, and optimizes resource management by removing expired ARQs as needed.

- **Support for Proxy Settings Across ADSS Server**

  Jira ID – (ADSS- 22886)

  The ADSS Server now fully supports proxy settings across all modules that make HTTP calls to external resources. While proxy configurations were previously available in most parts of the server, this enhancement ensures that proxy settings are applied uniformly throughout. This update improves connectivity management and strengthens security by consistently routing all HTTP traffic through the configured proxy.

- **Support for IAIK PQC v2.0**

  Jira ID – (ADSS- 22341)

The ADSS Server has been upgraded from IAIK PQC v1.3 to the latest IAIK PQC v2.0, ensuring alignment with NIST's FIPS-203/204 standards. This upgrade enhances cryptographic strength and ensures compliance with the latest post-quantum cryptography standards established by NIST.

- **Transitioning from JKS Format to PKCS12 Format**

  Jira ID – (ADSS- 18713)

  This feature introduces a KeyStore format migration across the ADSS Server, Client SDK, Go>Sign Desktop, Test Tool, AFP, and OCSP Client Tool, moving from the JKS (Java KeyStore) format to the PKCS12 format. PKCS12, a standardized format based on Public-Key Cryptography Standards, enhances compatibility with non-Java applications and provides stronger cryptographic support.

  This transition improves security by leveraging the advanced cryptographic algorithms available in PKCS12, which surpass those in JKS. As a result, PKCS12 is now set as the default KeyStore type for ADSS Server, Client SDK, Go>Sign Desktop, Test Tool, AFP, and OCSP Client Tool.

- **Support for Multiple Crypto Sources in ADSS SAM Service**

  Jira ID – (ADSS- 20858)

  This enhancement introduces the ability for operators to configure multiple crypto sources within a single ADSS SAM Service instance, providing load-sharing for user key generation and signing operations. A new configuration option in the ADSS SAM Service profile enables load-sharing for user key generation and signing operations across multiple crypto sources.

  - Operators can configure multiple crypto sources within a single ADSS SAM Service profile, allowing for efficient load distribution.
  - All configured crypto profiles must be of the same type to ensure compatibility and maintain operational consistency.
  - Configured crypto profiles must share the same Master Backup Key to support secure, seamless key management across sources.
  - Load distribution across crypto sources enhances the speed and reliability of key generation and signing operations.
  - This feature enables scaling cryptographic services through multiple sources without the need to deploy additional ADSS SAM Service instances.

Improvements

- **Enhanced APIs in RAS Service and Unity Service**

  Jira ID – (ADSS- 22411 /ADSS-22199)

The ADSS RAS Service and ADSS Unity Service have been enhanced to provide greater flexibility, allowing users to receive OTPs through their preferred communication channels. This enhancement improves efficiency and user experience for the Recover Password, Change Email, and Change Mobile Number APIs. Business applications can now dynamically determine whether to send OTPs via SMS, email, or both.

Security Improvements

- **Migration from Apache Oltu to Nimbus**

  Jira ID – (ADSS-22393)

  ADSS has successfully migrated from Apache Oltu to Nimbus (JOSE + JWT) and OIDC SDK. This migration was essential as Apache Oltu is no longer supported and contains multiple security vulnerabilities. Nimbus offers a more robust, secure, and up-to-date solution for handling JSON Object Signing and Encryption (JOSE), JSON Web Tokens (JWT), and OpenID Connect (OIDC). The transition to Nimbus ensures better security, improved performance, and continued compatibility with modern standards for authentication and encryption in ADSS services.

- **3rd party updates**

  Jira ID – (ADSS- 22888)

  Third party products supplied as part of ADSS Server have been upgraded.

- **Apache Tomcat version upgrade**

  Jira ID – (ADSS- 22887)

  Apache Tomcat has been upgraded to version from 10.1.25 to 10.1.28.

ADSS Server 8.3.6

August 2024

New Features

- **Support of Pre-Issuance Linting:**

  Jira ID – (ADSS-20374)

  ADSS Server v8.3.6 has introduced support for pre-issuance linting of certificates, CRLs, and OCSP responses. If the linting tool fails to validate any of these items, ADSS Server will block their issuance, log a detailed error, and send an alert to the operator, if configured. The integration includes the **PKILint** and **ZLint** tools as part of this update.

Product Enhancements

- **OAuth2 Client Authentication Now Supported in ADSS Certification Service**

  Jira ID – (ADSS-22264)

  TheADSS Certification Service now supports OAuth2 Client Authentication for secure communication with the ADSS RAS Server.

- **Enhanced validation checks for Certificate generation**

  Jira ID – (ADSS-21495/ ADSS-21566)

  The ADSS CA is now compliant with the updated CA/B Forum guidelines for the following certificate types:

  - **TLS Server Certificate:** Version 2.0.5
  - **EV TLS Server Certificate:** Version 2.0.1
  - **Code Signing and EV Code Signing Certificates:** Version 3.7
  - **S/MIME Certificate:** Version 1.0.3

- **Enhanced ADSS Verification Service**

  Jira ID – (ADSS-21320)

The ADSS Verification Service is now enhanced to verify only chosen signatures using X-Path in a document instead of whole document.

Improvements

- **API Updated and backward compatibility in Unity Service**

  Jira ID – (ADSS-22283)

  The (List Registered Devices) API has been enhanced to support user access tokens and the URI has been updated to remove the user-id query parameter.

  A new property has been introduced '**MOBILE_API_AUTHENTICATION'** when its value is TRUE the ADSS Server Unity Service will provide backwards compatibility.

Security Improvements

- **Tech Stack Migration in ADSS Server to Mitigate Security Vulnerabilities**

  Jira ID – (ADSS-21082)

  ADSS Server has migrated its major tech stack components, including Tomcat 10.1.x, JDK, Hibernate, and Spring Boot, to address security vulnerabilities.

ADSS Server 8.3.5

July 2024

New Features

- **Support of Post Quantum Cryptography**

  Jira ID – (ADSS- 17190)

  The ADSS server introduces support for Post-Quantum Cryptography (PQC) algorithms, ensuring robust security against both quantum and classical computing threats.

  ADSS Signing Server

  ADSS Signing Server performs server side signing and eSealing and will support CRYSTALS-Dilithium PKCS#1 and CMS signatures.

  ADSS SAM Service

  The ADSS SAM Service performs eIDAS compliant remote authorised server side signing and eSealing will support CRYSTALS-Dilithium PKCS#1 signature.

  ADSS PKI Server

  ADSS PKI Server can create CAs and issue X.509 certificates signed using the following Post-Quantum algorithms.

  - CRYSTALS-Dilithium
  - Classic McEliece
  - Kyber

  Note: Currently the PQC algorithms (Dilithium and Kyber) are provided to support proof of concepts (POC), subsequent releases will add further PQC capability as the NIST standards for PQC are finalised.

- **New Integration with Microsoft Active Directory Certificate Services (ADCS)**

  Jira ID – (ADSS- 21318)

The release of ADSS Server introduces a new integration with Microsoft Active Directory Certificate Services (AD CS) Enterprise CA's. ADSS Server now integrates via the Microsoft DCOM interface to provide a much tighter integration with Active Directory Certificate Services to offer full certificate lifecycle management, including issuance, renewal, rekeying, and revocation through the ADSS Server Certification Service.

- **Provided an 'Un-install' option for regular release**

  Jira ID – (ADSS-21057)

  ADSS Server 8.3.5 introduces a new un-install option for regular releases. This enhancement allows ADSS Server operators to easily roll back to previous versions. This offers greater flexibility with simplified un-installation steps, seamless file replacement, and a check to ensure manual database restore has taken place.

- **Performance statistics of Remote Signature via RAS-Demo**

  Jira ID – (ADSS- 20822)

  Case Number - ENH231101327

  The ADSS Server 8.3.5 introduces a new performance testing feature in the RAS-Demo web application. This feature provides flexible and simplified steps to calculate performance statistics for the remote signature flow when using an IDP. Additionally, the ADSS RAS Service has been enhanced to request credential/service authorization from the user only once, and the ADSS Signing Service has been updated to notify the business application (RAS-Demo) about duplicate responses from the IdP.

Product Enhancements

- **AWS Cloud HSM update**

  Jira ID – (ADSS- 21269)

  Case Number - ENH240101409

  The ADSS Server 8.3.5 now supports Client SDK v5 of AWS Cloud HSM for Windows and Linux systems.

- **Enhanced ADSS Signing Server to lock PDF documents**

  Jira ID – (ADSS- 20716**)**

Case Number - ENH231101295

The ADSS Signing Server has been enhanced to lock PDF documents against all changes upon the final signature. This lock prevents the PDF from being used for further digital signing, form-filling, or any annotation modifications.

- **Enhanced support in eSeal Signing through ADSS Signing Gateway**

  Jira ID – (ADSS- 20718)

  Case Number = ENH231101304

  ADSS Server now supports eSeal signing without requiring certificates and aliases to be configured in business applications. Certificates are configured on the eSeal server signing profile and are used automatically. For remote authorized signing, only the certificate alias needs to be passed, with the Signing Service retrieving the certificate from RAS for signature computation.

- **Entrust Proxy Update**

  Jira ID – (ADSS- 20777)

  Case Number = ENH231101322

  The ADSS Server Entrust Proxy has been enhanced to support for multiple middle names within in the Common Name (CN) field when generating certificates via the Entrust proxy, the Entrust Proxy will now include all users first, middle and last names when requesting a certificate.

- **Support HTTP v1 for Firebase Push Notifications**

  Jira ID – (ADSS- 21161)

  Case Number = ENH240101367

  Customers using Google Firebase for push notifications in ADSS Server to the Ascertia Go>Sign mobile app need to take immediate action to avoid notification interruption, Google FCM will start a gradual shutdown of deprecated APIs around July 22nd, 2024.

  Ascertia has upgraded to latest Firebase HTTP v1 API in its ADSS v8.3.5, so customers are advised to upgrade to ADSS v8.3.5 as soon as possible.

  With Firebase Push Notifications migrating from legacy FCM APIs to HTTP v1, users need to make the following changes after upgrading to the ADSS Server version 8.3.5:

1. Update the server address. i.e https://fcm.googleapis.com/v1/projects/[PROJECT_ID]/messages:send

2. Upload the service account file instead of the secret key.

Users can download the service account JSON file and the updated server address from the Google FCM Portal.

https://firebase.google.com/

Clients who are using Go>Sign Mobile APP can get latest JSON file from the following link or Ascertia Support Team.

- **Added Support of new Extended Key Usages**

  Jira ID – (ADSS- 21487)

  Case Number = ENH240201463

  ADSS Server now supports a new set of Extended Key Usages (EKUs). These EKUs can be selected from the Extended Key Usages available in the Certificate Template for inclusion in certificates. The added EKUs are:

  - 1.0.18013.5.1.2 (mdlDS) – Mobile Drivers License Document Signer Certificate
  - 1.0.18013.5.1.3 (mdlJWS) – Mobile Drivers License JWS Certificate
  - 1.0.18013.5.1.6 (IACA link certificates) – Mobile Drivers License Link Certificate
  - 1.0.18013.5.1.4 (mDL Reader authentication) – Mobile Drivers License Reader authentication and TLS client authentication Certificate
  - 1.3.6.1.5.5.7.3.36 (id-kp-documentSigning) – RFC 9336 Document Siging Certificate

  ADSS Server also enables operators to create custom extended key usages.

Improvements

- **API Updated and backward compatibility in RAS Service**

  Jira ID – (ADSS-21702)

  Case Number - ENH240401496

  The (List Registered Devices) API has been enhanced to support user access tokens and the URI has been updated to remove the user-id query parameter.

A new property has been introduced '**MOBILE_API_AUTHENTICATION'** when its value is TRUE the ADSS Server RAS Service will provide backwards compatibility.

- **Improvements in CRL Monitor Alerts**

  Jira ID – (ADSS- 16701)

  The CRL Monitor functionality has been enhanced to send alerts prior to the expiration of the CRL.

- **Improvements in Credential Info API**

  Jira ID – (ADSS- 21240)

  Case Number - ENH240101405

  The ADSS RAS Server has been enhanced to include the hashAlgorithm OID in the RAS CSC credential info API.

ADSS Server 8.3.4

June 2024

Product Enhancements

- **OAuth2/Authorize CSC API enhanced in Unity Service**

  Jira ID – (ADSS-22241)

  There is an authorization prompt shown to user on calling CSC API OAuth2/Authorize with “scope=service” in ADSS unity service. This seems unnecessary and may annoying users. Now in this enhancement, it is skipped and unity service directly delegate to external IdP.

- **API Updated and backward compatibility in RAS Service**

  Jira ID – (ADSS-21702)

  Case Number - ENH240401496

  The (List Registered Devices) API has been enhanced to support user access tokens and the URI has been updated to remove the user-id query parameter.

  A new property has been introduced ‘**MOBILE_API_AUTHENTICATION’** when its value is TRUE the ADSS Server RAS Service will provide backwards compatibility.

- **Credential Authorize API enhanced in Unity Service**

  Jira ID – (ADSS-22262)

  The Credential Authorize API (credentials/authorize) in Unity Service now incorporates out-of-band functionality similar to the oauth2/authorize API, aimed at reducing the need for multiple user authorization calls.

Security Improvements

- **Updated JDK Version**

  The JDK version has been updated from 17.0.9 to 17.0.11.

- **Apache Tomcat version upgrade**
  Apache Tomcat has been upgraded to version from 9.0.85 to 9.0.89.

ADSS Server 8.3.3

March 2024

New Features

- **ADSS Server Unity Service**

  Jira ID – (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.

Product Enhancements

- **ADSS Server Certificate Templates Update**

  Jira ID – (ADSS-21645, ADSS-21644)

  ADSS Server certificate templates in Unity Console 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”.

- **Support for Azure Managed HSM**

  Jira ID – (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.

- **ADSS Signing Server Performance Improvement**

  Jira ID – (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.

- **ADSS Verification Server Performance Improvement**

  Jira ID – (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.

- **ADSS RAS Server Secure APIs**

  Jira ID – (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.

- **New API to retrieve all certificates from a given CA**

  Jira ID – (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.

- **Support for new RDNS in ADSS Server**

  Jira ID – (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.

Security Improvements

- **Upgraded Tomcat**

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

ADSS Server 8.3.2

January 2024

New Features

- **Regular Release installer**

  Jira ID – (ADSS-20751)

  ADSS 8.3.2 introduces a streamlined installation for regular releases, allowing users to seamlessly install incremental updates comprising of new features, improvements and bug fixes. This offers simplified installation 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.

Product Enhancements

- **Additional policy controls for ADSS Server SAM Service HSM key storage**

  Jira ID – (ADSS-20436)

  A new policy control has been introduced in the ADSS Server SAM Service to allow user to enable or disable the automatic removal of keys into the HSM after each eSeal signing operation, this enables large volumes of eSeals to be used beyond a HSM storage capacity without requiring additional authorisations.

- **New Security Policy to reject multiple use of pubic keys**

  Jira ID – (ADSS-20289)

  A new security policy option has been added in the ADSS Server Certification Service to reject already certified public keys in certificates created through certification service, key manager and manual certification, this prevents a client from trying to request a certificate multiple times without first generating new public and private keys.

Security Improvements

- **Migration from .NET framework 4.5 to .NET Core 8.0**

  Jira ID – (ADSS-20454)

ADSS Server Client SDK has been migrated from .NET framework (4.5) to .NET core (8.0).

- **Upgraded Tomcat**

  Jira ID – (ADSS- 20782)

  The ADSS Server has been upgraded tomcat from v9.0.76 to v9.0.83.

- **3rd party updates**

  Jira ID – (ADSS- 20783)

  Third party products supplied as part of ADSS Server have been upgraded.

ADSS Server 8.3.1

November 2023

New Features

- **ADSS Server Unity Console new features:**

  The Ascertia Unity in ADSS Server 8.3.1 introduces new modules such as RAS Service and SAM Service, 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.

- **Support to achieve document confidentiality in ADSS Verification Gateway**

  Jira ID – (ADSS-19291)

  The Verification Gateway has been enhanced to achieve document confidentiality. Verification Gateway will not send the whole document to backend Verification Service, instead the verification gateway extracts the signature and hash and sends 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 in ADSS Server**

  Jira ID – (ADSS- 14869)

  The ADSS Server has been upgraded and enhanced to operate on OpenJDK version 17.44+15.

- **Support for Import Signature Appearance**

  Jira ID – (ADSS- 17424)

  Introduced a new feature has been introduced to streamline the importing of exported files into the PDF Signature Appearances list. This enhancement includes the integration of an "Import" button within the PDF Signature Appearances section, facilitating the management of signature appearances within PDF documents.

- **Support to install Go>Sign Service in preferred directory**

Jira ID – (ADSS-15172)

The introduction of a new feature in the Go>Sign Desktop installation process now grants users the flexibility to select their preferred directory, enhancing alignment with individual requirements during installation.

- **Support to provide an option CUSTOM_DATE in SAM Profile**

  Jira ID – (ADSS- 19286)

  The ADSS Server has been enhanced to incorporate a custom date setting option within the SAM Profile specifically for SAD expiry. Administrators now have the capability to select "CUSTOM_DATE" from the dropdown menu and subsequently input a precise date utilizing the provided date-picker interface.

- **Support of external authorization servers (IdPs) for service authorization in ADSS RAS Server**

  Jira ID – (ADSS- 17261)

  The ADSS RAS server has been enhanced to support external authorization servers (IdPs) for service authorization through the utilization of SAML or OpenID Connect.

Product Enhancements

- **Enhanced ability to disable "Compute final hash at signing time" option when use padding scheme PSS**

  Jira ID – (ADSS-17762)

  The ADSS SAM Service 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 Service 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**

  Jira ID – (ADSS-19387)

  The ADSS RAS/SAM service has been enhanced to enable user identification through custom attributes within assertion data when utilizing an OpenID Connect IdP for external remote authorization.

- **Enhanced RAS/SAM with separate Authorization Request expiry and SAD Request expiry**

Jira ID – (ADSS-18888)

The ADSS RAS/SAM Service has been updated to offer distinct 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**

  Jira ID – (ADSS- 19288)

  The ADSS RAS/SAM Service has been upgraded to accommodate JSON-based SAD for credentials authorization in RAS/SAM services, introducing a new property named "SAD_FORMAT" within the Global Settings > Advanced Settings under the SAM Tab. This property allows the selection between two values, JSON or XML, for SAD formatting.

- **Enhanced ADSS TSA Server to specify the list of supported Hash Algorithms**

  Jira ID – (ADSS- 13861)

  This enhancement empowers the TSA service with the capability to specify and add a list of supported hash algorithms.

- **Enhancement of storage of data-to-be-displayed distinct from the SAD**

  Jira ID – (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**

  Jira ID – (ADSS- 17505/ ADSS- 17504)

  Enhanced validation checks for reserved IP Address and Internal Name according to WebTrust and CA/B Forum guidelines in certificate generation for SSL and EV-SSL certificates.

- **Enhanced the functionality of private key retrieving from Thales HSM for ADSS SAM Service**

  Jira ID – (ADSS- 19431)

The ADSS Server has been upgraded to exclusively provide a private handle for retrieving the private key from the HSM, eliminating the necessity for the public key handle. This will improve the performance of utilization of key handling.

- **Enhanced the functionality to list down all the pending requests – (ADSS- 18887)**

  In this enhancement, we have included the capability to retrieve and display a list of all pending requests for a user.

Known Issues

List of known issues and workarounds if available.

https://www.ascertia.com/product-documentation/adss-server/

Technical Support

If Technical Support is required, Ascertia has a dedicated support team. Ascertia Support can be reached/accessed in the following ways:

Website	https://www.ascertia.com
Email	support@ascertia.com
Knowledge Base	https://www.ascertia.com/products/knowledge-base/adss-server/
FAQs	https://ascertia.force.com/partners/login

In addition to the free support services detailed above, Ascertia provides formal support agreements with all product sales. Please contact sales@ascertia.com for more details.

When sending support queries to Ascertia Support team send ADSS Trust Monitor logs. Use the Ascertia's trace log export utility to collect logs for last two days or from the date the problem arose. It will help the support team to diagnose the issue faster. Follow the instructions on how to run the trace log export utility

Premier Success Services

The Ascertia Premier Success team assists business around the world to design, deploy, and maintain Ascertia solutions. We offer a wide range of services to assist you with our e-business solution this includes, planning and systems architecture, installation, system integration, deployment support, and custom software development.

Whether you choose to operate your Ascertia solution on-premise, via an Ascertia Trust Service Provider, or via Ascertia Hosted Services, the Ascertia Premier Success Team can design and implement the right solution for you. For more information about Ascertia Premier Success please visit our Web site at: https://www.ascertia.com/

*** End of Document ***