ADSS Server - Release Notes

This document provides a high-level description of the new features offered in each release of ADSS Server. Only the main features in each release are identified.

ADSS Server v6.7 — July 2020

- Ascertia's ADSS Server now includes support for the issuance and management of digital certificates in support of both Basic Access Control (BAC) and Extended Access Control (EAC) ePassport PKI solutions.

  ADSS Server's Basic Access Control solution includes - Country Signing CA (CSCA), Document Signer (DS), Master List Signer and National Public Key Directory (NPKD) components.

  ADSS Server's Extended Access Control solution includes - Country Verifying CA (CVCA), Document Verifier CA (DVCA), issuance of Inspection System Certificates and Single Point of Contact (SPOC).

  The ADSS Server client SDK now also supports the issuance and management of Inspection System certificates which enables developers to integrate BAC and EAC into border management solutions.

  ADSS Server's ePassport solution is fully compliant with:

  a) ICAO 9303 7th Edition part 12 for Basic Access Control

  b) BSI TR-03139 v2.2 for Extended Access Control

  c) BSI TR-03129 - Protocols for the Management of Certificates and CRLs

  d) BSI TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents

  e) CSN 36 9791 - Country Verifying Certification Authority Key Management Protocol for SPOC

  These components are accessed when enabled via the ADSS Server license.

- Multiple enhancements were identified by sophisticated security tools that have been made part of this release.

ADSS Server v6.6.0.9 — June 2020

- ADSS Verification Service has been enhanced to support the legal entity identifier and role information in the verification response via its HTTP interface.
- Resolved an issue related to advance path building using certificate's AIA extension in SCVP Service.
- Resolved an issue related to OCSP Service -> Management Reporting -> Service Statistical Report.
- Resolved an issue in RAS Service related to OAuth token.

ADSS Server v6.6.0.8 — June 2020

- Fixed a problem where the upgrade of v5.8 to v6.6 failed because ADSS Server setup fails to get database password.
- Resolved test connection functionality issue for External CA.
- Resolved an issue related to signing operation in RAS Service.
- Resolved an issue related to Arabic characters for Entrust Authority Security Manager (EASM).

ADSS Server v6.6.0.7 — June 2020

- Resolved an issue related to TLS authentication while communicating with Symantec MPKI external CA.
- Resolved an issue related to certificate import in Key Manager.

ADSS Server v6.6.0.6 — May 2020

- This release adds support DigiCert PKI v8.0 as an external CA in ADSS Server. Customers can now use ADSS Server to perform full certificate lifecycle management of certificates issued by DigiCert PKI version 8.0.

  For further reference, Click Here.

ADSS Server v6.6.0.5 — May 2020

- Resolved an issue related to TLS authentication while communicating with Symantec MPKI external CA.
- OCSP Service has been enhanced to use the ArchiveCutOff extension, with the archiveCutOff date set to the CA's certificate "valid from" date.
- Resolved an issue in Certification Service related to renewal of certificate.
- Resolved an issue when saving changes in Global Settings > Notification Settings.
- Resolved an issue where user is unable to delete a certificate having (+) sign in it.
- Resolved an issue in CSP Service related to user authentication using refresh token.
- Resolved an issue related to RDNs where certificate issuance failed for qualified natural person semantics.
- Resolved an issue related to checkbox in Manage CAs > Local CAs > Keep expired revoked certificates in the CRL.
- Resolved an issue related to OCSP Service -> Management Reporting -> Service Statistical Report for linux platform.
- Resolved an issue related to Signing Service -> Management Reporting -> Service Stats Report.
- Resolved an issue related to Large Size CRL generation and CRL import.
- Enhanced character limit for Organization field in Manage CA > External CA.
- Enhancement has been done in Audit Log Events for ADSS Core, Console and Service Instance.

ADSS Server v6.6.0.3 — April 2020

- Resolved issues related to the display of signatures being generated by the ADSS Server Signing Service related to multilingual characters. These now display correctly when viewed in signed PDF documents.

ADSS Server v6.6.0.2 — April 2020

- This patch upgrades the Apache Tomcat server used by ADSS Server to release 9.0.33, by default the AJP connectors for the ADSS Server Console and Service instances are disabled. Customers who need to use the AJP connector to support Go>Sign or SigningHub use cases should use the steps defined in the following link to enable and secure access to the AJP.

  Connectors:http://faqs.ascertia.com/display/ADSS/Tomcat+Configurations#TomcatConfigurations-ConfigureADSSServertomcatforsecureAJPcommunication.

ADSS Server v6.6.0.1 — March 2020

- Multiple enhancements were identified by sophisticated security tools that have been made part of this release.

ADSS Server v6.6 — March 2020

- Upgrades to third party libraries have been made to enhance security of ADSS Server.
- ADSS Server documentation now provides guidance on system hardening and security, full details are available in the ADSS Server installation guide.
- This release resolves issues reported in Approval Manager for some operations under dual control.

ADSS Server v6.5.0.3 — January 2020

- Resolved multiple issues related to management reporting in OCSP Service.
- Resolved an issue when saving changes in Verification Service profile.
- Logic for Schedule restart thread has been improved in ADSS Core, Console and Service instances.

- Several enhancements done for NTP monitoring in load balance environment along with logs improvement.
- Resolved an issue in RAS Service related to Arabic characters.
- Resolved an issue in OCSP Service related to appearance of preferred signature algorithms in request/response viewer.
- Resolved an issue in ADSS Signing Service related to performance optimisation.
- Resolved an issue related to incorrect validity period while generating certificate for Entrust CA.
- ADSS RAS Service has been extended to support concurrent requests in bulk.
- Resolved an issue about logs directory access from help menu on ADSS Server console home screen.

ADSS Server v6.5.0.2 — January 2020

- Certification Service has been enhanced to support UID as a new RDN.
- Resolved an issue in SAM Service related to authorization of signing request.
- Resolved an issue in Key manager related to crypto profile.
- An issue related to database connections has been resolved when performing archiving operation.

ADSS Server v6.5.0.1 — December 2019

- Resolved an issue of status checking for QuoVadis External CA.

ADSS Server v6.5 — November 2019

- ADSS RAS Service now supports OAuth v2.0 to enable remote authorised signing following the Cloud Signature Consortium (CSC) specification.
- ADSS CSP Service now supports OAuth v2.0 to authenticate users registered in Active Directory and Azure AD.
- CA Service has been enhanced to request certificate issuance with serialNumber and UID in support of multi-valued RDNs from Entrust Authority Security Manager (EASM).
- The Manage CA module now supports the manual processing of Name Constraints extension.
- The Certificate Template Viewer has been enhanced.
- ADSS Signing Service has been enhanced to support the Reference identifier for XML Signatures via its HTTP/S interface.
- ADSS OCSP Service has been enhanced to support ADSS OCSP Gateway functionality.
- ADSS RAS Service can now return the list of devices registered to a client token.
- An email alert is now sent when ADSS Server time deviates from HSM time as defined in Global Settings.
- Certificate Templates module has been enhanced to add new custom extensions.

ADSS Server v6.4 — September 2019

- The ADSS Signing Service has enhanced support for ETSI PAdES/CAdES/XAdES formats.
- The ADSS Signing Service API can now receive and process user certificates for remote signing.
- The ADSS Signing Service Management Reports have been enhanced to show monthly and yearly statistics.
- The ADSS CSP Service has a new API call to retrieve CSP Advance Settings.
- Support for the MariaDB connector for MySQL databases and Microsoft JDBC driver for SQL Server databases has been added.
- Auditing for data encryption key changes has been enhanced.
- The Manage CA module now supports the CRL extension IssuerAltName.

ADSS Server v6.3.0.9 September 2019

- Resolved an issue in Trust Manager regarding CRL download.

ADSS Server v6.3.0.8 September 2019

- Resolved an issue for XML and MS office Signatures concerning hashing algorithm selection.
- Resolved an issue where ADSS Server failed to send SMS OTP that is required in the device registration process for Remote Authorised Signing.

ADSS Server v6.3.0.7 September 2019

- Resolved an issue in Certification Service related to Arabic characters for Entrust Authority Security Manager (EASM).
- Resolved an issue related to self-signed key configuration when OCSP Service is used as a gateway.

ADSS Server v6.3.0.6 August 2019

- Resolved an issue related to database connections when processing real-time revocation database requests.
- Resolved an OCSP Service issue in handling of OCSP response headers when nextUpdate is not available.
- Resolved an issue in SAM service related to renewal requests while using new key pair for external CAs.
- Resolved an issue related to Certificate Signing Request (CSR) in Key Manager.
- Enhanced the RAS Service to ensure CSC interoperability.
- Resolved an issue of "Test SMS" feature in Global Settings > Notification Settings module.

ADSS Server v6.3.0.5 August 2019

- Resolved an issue related to import and deletion of large size archived transaction logs in OCSP Service.
- Resolved an issue in CA Service related to RDNs in Subject DN for Entrust Authority Security Manager (EASM).

ADSS Server v6.3.0.4 August 2019

- Resolved an issue when upgrading a v5.x slave instance to a v6.x slave instance in load balanced mode.
- Resolved an issue working with Thales/Gemalto Luna HSMs when generating key pairs and using bulk signing.

ADSS Server v6.3.0.3 July 2019

- Enhanced the SAM Service to ensure CSC interoperability.

ADSS Server v6.3.0.2 July 2019

- Resolved an issue of key pair generation with Gemalto SafeNet Luna HSM in FIPS mode.

ADSS Server v6.3.0.1 July 2019

- ADSS Server CA Service has been enhanced to request certificate issuance with various supported RDNs in Subject DN from Entrust Authority Security Manager (EASM).
- Certificate policies shows on certificate viewer.
- Update in CMC request/response viewer.

ADSS Server v6.3 July 2019

- ADSS Verification Service can now act as a front-end gateway to back-end services.

- ADSS RAS Service can now act as a front-end gateway to back-end services.
- CSP Proxy Server now logs back-end requests and responses.
- Manage CA module now supports the CRL extension ExpiredCertsOnCRL as required by WebTrust.
- Global Settings > Advanced Settings has a new option to bypass CRL expiry checking for certain operations.
- WebRA can send Renew and Re-key requests for a certificate using a specified Certification Profile.

ADSS Server v6.2 June 2019

- ADSS Server CA Service has been enhanced in various ways:
    f) Supports CA/B Forum and Web Trust guidelines for certificate issuance.
    g) Key Manager and Certification Service now supports Arabic and French characters in the Subject Distinguished name.
    h) Multiple AIA extensions are now supported within a certificate.
    i) Name Constraints for a certificate can now be requested.
    j) Short life certificates can now be requested from Entrust Authority Security Manager (EASM).
- ADSS Server RA Service SCEP Protocol handler has been enhanced to meet the latest device certificate requirements.
- Key Manager supports the latest ECDSA curves.
- Security has been enhanced with form validation rules enforced to check and validate input data.
- A Generic SMS Connector is now provided to rapidly enable the use of local SMS providers.

ADSS Server v6.1 May 2019

- The Certification Service and Go>Sign Service have been enhanced to support new WebRA functionality.
- The RAS and SAM Services have been enhanced allow third party products to handle device registration and the RAS Service now supports QR Codes.
- The CSP Service has been enhanced to handle extended character sets.
- Various upgrades to third party libraries and frameworks have been made to enhance functionality and security.
- A HMAC Service has been added as a licensed option using JSON calls to compute HMACs for business application such as SigningHub.
- Go>Sign Desktop now supports ECDSA key generation.

ADSS Server v6.0 November 2018

- This is the ADSS Server EN 419 241-2 Common Criteria compliant version that supports EU eIDAS Regulation for Remote Qualified Signatures. These are server-side signatures, which meet the Sole Control Assurance Level 2 (SCAL2) requirements to prove that a centrally held signing key was only used for signing under instruction from its owner.

  The Ascertia ADSS Server SAM Appliance which is a tamper-protected hardware remote Qualified Signature Creation Device (QSCD) uses this version.

  ADSS Server 6.0 is qualified to work against Utimaco CP5 EN 419 221-5 Common Criteria certified HSMs. These new HSMs provide the extra security required for eU eIDAS compliant remote Qualified Signatures. ADSS Server has been integrated with the new Key Authorisation interfaces to strictly control all aspects of key generation and usage.

  The ADSS Server SAM Service module specifically is the Target of Evaluation for EN 419 241-2 certification.

ADSS Server v5.10.0.4 December 2018

- An ADSS OCSP Service Gateway license option is now supported to force OCSP forwarding from a Tier 1 ADSS OCSP Gateway to a Tier 2 ADSS OCSP Server.
- Resolved an issue in Trust Manager regarding the display of Request Signing Certificates.
- Resolved an issue in the TSA client "test connection" feature in Global Settings > Timestamping module.

ADSS Server v5.10.0.3 December 2018

- Resolved an issue accessing certain CSP service profiles.
- Resolved an issue with HMAC verification reporting in the SAM Service.
- Resolved an issue displaying a sub-module of a service on the Admin Console.
- Resolved an issue whereby SAM user ID was not correctly saved when using PostgreSQL database.

ADSS Server v5.10.0.2 December 2018

- Resolved an issue where ADSS Server failed to generate an OTP that is required in the device registration process for Remote Authorised Signing.
- Resolved a problem where the upgrade of v5.9 to v5.10 failed because the Master Key components were not copied to the new directory.

ADSS Server v5.10.0.1 December 2018

- Resolved an issue with Certification Profile for certificates used in Remote Authorised Signing. The profile expected a password to protect the private signing key.
- Resolved an issue where HMAC verification failed in Server Manager after adding a new Crypto Source to Key Manager.
- Resolved an issue of an orphaned key in HSM when certificate renewal operation with a new key pair failed.
- Resolved an issue where some ADSS Server external communications were not using the configured proxy.

ADSS Server v5.10 October 2018

- A new Cryptographic Service Provider (CSP) Service is now available as a licensed option. ADSS Server now offers Virtual CSP (VCSP) support for Windows Desktops to support remote signing, i.e. where keys and certificates are held centrally. It works in conjunction with the VCSP Plugin installed locally and enables any Microsoft or third party CAPI/CNG applications to conduct remote signing seamlessly. VCSP has been tested for remote signing with a range of applications including Microsoft Word, Outlook and Adobe Acrobat®.

ADSS Server v5.9.0.5 November 2018

- Enhanced Signature Activation Data (information sent to user's mobile device to request authorisation for a Remote Signing Operation) schema to allow a message of up to 500 characters to be sent. This is the message that is displayed on the user's mobile device.
- Resolved an issue that logged Operators out of the ADSS Server Console unexpectedly.
- Resolved an issue related to TLS communication between RAS and Certification Services.
- Resolved an issue where OCSP Responder URL was not displayed on Trust Manager -> Validation Policy page for a trusted CA.

ADSS Server v5.9.0.4 October 2018

- Resolved an issue with user login while working with UTIMACO HSM.

ADSS Server v5.9.0.3 October 2018

- Improved the performance of full certificate status checking for OCSP Service by modifying the database searches.

- Resolved an issue related to notifications in Key Manager for certificate expiry whereby the settings were not saved, and hence followed correctly.
- Resolved an issue related to the verification of PAdES-LTA signatures.
- Resolved an error when using MS SQL Server for full certificate status checking for OCSP Service.

ADSS Server v5.9.0.2 September 2018

- Resolved issues related to the upgrade of load balanced slave instances.

ADSS Server v5.9.0.1 September 2018

- Resolved an issue related to re-compute HMAC utility.

ADSS Server v5.9 September 2018

- New Signature Activation Module to support Remote Authorised Signing for end users. eIDAS Regulation compliant solution against EN 419 241 – 2. This operates within the same framework but supports use of a standard PKCS#11 HSM. Fully Common Criteria EAL4+ certified version of SAM is currently undergoing the certification process.
- New Remote Authorization Service (RAS) to support Signature Activation Module (SAM) for Remote Authorised Signing operations. RAS provides support functions to business applications and end user mobiles, and is the interface to SAM. It allows registration of users and mobile devices and authorization of user signing requests. RAS supports both Ascertia proprietary protocols and Cloud Signature Consortium remote signing. RAS also supports Push notifications for Remote Authorised Signing requests to end user mobile phones.
- ADSS Server RA Service enhanced to support business applications in the use of RAS/SAM. It acts as the interface for business applications to register users and their mobile devices.
- ADSS Server has been enhanced to support:

  (a) Clickatell RESTful API to provide the most reliable SMS delivery to end users.

  (b) Alert and ultimately deny usage of ADSS Server if the default Operator certificate is not changed.

  (c) Twilio SMS Gateway for SMS delivery of Operator alerts.

  (d) Security review and enhancements to ensure the highest levels of security for ADSS Server.
- Underlying JRE updated as per Oracle recommendations. Now uses version jdk1.8.0_171.
- Underlying Tomcat server upgraded as per Apache recommendations to version 9.x.
- Third party library upgrades where required by vendors for bugs, features, and potential security vulnerabilities.
- Struts upgrade program for ADSS Server Console. Phase one.

ADSS Server v5.8.0.5 September 2018

- Resolved an issue related to time out in Entrust CA.
- The ADSS RA Service has been enhanced to support all possible RDNs.

ADSS Server v5.8.0.3 July 2018

- Resolved an issue related to the PKCS#11 test utility to generate the log file.
- Resolved an issue related to Approval Manager while approving TSA policy changes.

ADSS Server v5.8.0.2 July 2018

- Some improvements in ADSS Server real time revocation status checking mechanism.

ADSS Server v5.8.0.1 May 2018

- Resolved an issue related to key generation in Luna HSM when ADSS Server is upgraded from an older version.

ADSS Server v5.8 — May 2018

- Support Symantec MPKI v7.5 as an external CA in ADSS Server. This includes full certificate lifecycle management via Certification Service.
- Enhancements to integration with Entrust Authority Security Manager as an external CA in ADSS Server.

ADSS Server v5.7.0.2 — May 2018

- Resolved an issue related to key generation in Thales HSM when ADSS Server is upgraded from an older version.
- Resolved an issue in Trust Manager console related to Real-time certificate status settings when ADSS Server is upgraded from an older version.

ADSS Server v5.7.0.1 — April 2018

- Some ADSS Server Console GUI enhancements.

ADSS Server v5.7 — April 2018

- ADSS Go>Sign Service has been enhanced to:

  (a) Allow the local signing certificate filter to also use the Subject Alternative Name (SAN) extension when automatically filtering for certificates.

  (b) Optionally allow the display of the native hardware vendor PIN/Passphrase entry dialog.
- The Key Manager module has been enhanced to:

  (a) Support the AWS CloudHSM service.

  (b) Allow the inclusion of otherName and iPAddress within the SAN extension of X.509 Certificates
- The ADSS Certification Service has been enhanced to allow the entry of iPAddress within the SAN extension of X.509 Certificates.
- A few third party libraries have been upgraded as part of our regularly security improvement review cycle.

ADSS Server v5.6 — February 2018

- Support Entrust Authority Security Manager as an external CA in ADSS Server. This includes full certificate lifecycle management via Certification Service.
- Support GlobalSign High Volume Issuing CA as an external CA in ADSS Server.
- Client Manager enhanced to support multiple client TLS certificates per client.
- ADSS Server Signing service enhanced to work with other central signing / sealing servers (ADSS Server Gateway version).
- Installer enhanced to support Windows Authentication at deployment time.
- Windows Authentication support for full certificate status checking database login.
- Support for PostgreSQL 10.x database.
- PSS signature padding scheme support for all signature operations.
- Performance improvements for full certificate status checking.

ADSS Server v5.5.0.10 — January 2018

- Some improvements in ADSS LTANS Service related to archive data export and verification.

ADSS Server v5.5.0.9 — January 2018

- Some improvements in ADSS Server real time revocation status checking mechanism.

ADSS Server v5.5.0.8 — January 2018

- ADSS Server has been enhanced to provide better handling of timeouts in case of external communication failure.
- Various stability enhancements.

ADSS Server v5.5.0.7 November 2017

- ADSS Server has been enhanced to support latest Postgres database v10.x.

ADSS Server v5.5.0.6 November 2017

- Go>Sign Service and Go>Sign Desktop have been updated to enhance security handling.
- ADSS Client SDK has been updated.
- ADSS Server HSM management has been updated to handle different vendor key wrapping options.

ADSS Server v5.5.0.5 October 2017

- ADSS Server OCSP Service reporting has been enhanced.
- Minor issues in the ADSS Server Manage CAs module have been resolved.

ADSS Server v5.5.0.4 September 2017

- A SQL Server upgrade issue resolved.

ADSS Server v5.5.0.3 August 2017

- Now supports multiple PKI Disclosure Statements in Certificate Templates.

ADSS Server v5.5.0.2 August 2017

- Signature verification issue resolved for SigningHub Mobile Apps.

ADSS Server v5.5.0.1 July 2017

- RA Service has been enhanced to return DER encoded X.509 certificate in SCEP response.

ADSS Server v5.5 July 2017

- A new Authorised Remote Signing (ARS) Service is now available as a licensed option. The ARS Service provides a secure way for users to authorise the use of their centrally-held user signing keys. The ARS Service meets the EU eIDAS Regulations requirements for remote Qualified Signatures, in particular it ensures up to Level 2 Sole Control over the signing keys according to the standard EN 419241-2 Protection Profile. Each user must use the new Ascertia “Go>Sign Mobile” app to register their mobile device and then they can participate in the secure authorisation protocol for their server-side signing actions. The Go>Sign Mobile app is available for iOS 9+ and Android 7+ devices.

  When the user needs to sign a document or transaction, the ARS Service sends an authorisation request via separate data channel to the user’s Go>Sign Mobile app and the user is asked to authorise the transaction using their Touch ID. If the user is authenticated successfully the Go>Sign Mobile app creates a signed authorisation response using a device-specific private key held within their mobile device’s Secure Element/Enclave. The signed authorisation is verified by the ARS Service before it requests the use of the user’s centrally-held Qualified, AATL or similar high trust signing key. Note the user’s signing keys are protected using a suitably certified centrally held HSM, for remote Qualified Signatures this must meet the standard EN 419221-5 Protection Profile.

  The ADSS ARS Service provides a set of APIs that allow business applications to (a) register users, (b) send hash signing requests, (c) check the status of a pending signing requests and (d) fetch the signed hash values as a PKCS#1 signature. The ADSS Signing Service can extend this basic signature type to any supported basic, timestamped or long-term ETSI PAdES, XAdES, CAdES signature format.

- ADSS Server has been enhanced to support;

  (a) AES GCM ciphers for TLS/SSL communication as specified in RFC 5084 and RFC 5288.

  (b) A new Key Encrypting Key (KEK) management service for Data Encryption Key (DEK) encryption/decryption.

ADSS Server v5.4.0.6 — May 2017

- Resolved an issue with generating KEK protected keys while working with Gemalto SafeNet Luna SA5 HSM.

ADSS Server v5.4.0.5 — May 2017

- Resolved an issue with sending OCSP Monitor email alerts.

ADSS Server v5.4.0.4 — April 2017

- Resolved an issue with creating PDF signature appearance profiles.

ADSS Server v5.4.0.3 — March 2017

- Updates applied to the Qualified Seal management process.

ADSS Server v5.4.0.2 — March 2017

- Enhanced Key Manager to add Key Usage and Extended Key Usage extensions in Certificate Signing Request (CSR).

ADSS Server v5.4.0.1 — February 2017

- Enhanced Azure Key Vault HSM management.
- Updated ADSS Server Console to reduce system resource requirements.
- Enhanced OCSP response processing for authorised OCSP responders.
- Updated certificate validity checking for whitelist database.

ADSS Server v5.4 — January 2017

- ADSS Server has been enhanced to:

  (a) Support TLSv1.2 as default protocol for TLS/SSL communication;

  (b) Support IPv6 network addresses;

  (c) Support RSA keys of length 8192;

  (d) Support SNMP v3 traps in order to improve performance, flexibility and security;

  (e) Provide management summary statistics for the Signing, TSA and OCSP services.
- The ADSS Certification Service has been enhanced to optimise performance.
- ADSS OCSP Service has been enhanced to:

  (a) Support CertHash and Archive Cutoff extensions in OCSP response according to German Common PKI and RFC 6960;

  (b) When using full certificate status processing the nextUpdate interval can be configured on per CA basis for non-issued certificates.
- New alert messages have been added to ADSS OCSP Monitor.

ADSS Server v5.3.0.4 — January 2017

- Resolved an issue in OCSP Service response signing when the key is in Azure key vault.
- Concurrent request handling has been enhanced in the ADSS LTANS Service.

ADSS Server v5.3.0.3 — December 2016

- Resolved an issue related to handling of special characters when used in crypto source PIN.

ADSS Server v5.3.0.2 — December 2016

- Resolved an issue related to headless installation of ADSS Server on Linux OS with Microsoft Azure SQL Server database.

ADSS Server v5.3.0.1 December 2016

- Go>Sign Desktop is now multilingual and also supports colors handling for the PKCS#11 PIN dialog.

ADSS Server v5.3 November 2016

- The ADSS Signing Service has been enhanced to:

  (a) Provide SigningHub with services that comply with EU eIDAS Regulation requirements to create Qualified Remote Signatures using server-held keys and certificates in accordance with CEN/TS 419241;

  (b) Set an ADSS Server user or application inactive if the supplied security credentials fail to verify for a configurable number of times;

  (c) Send an alert message if a signing operation fails because the signature operation fails as opposed to system failures.

- ADSS TSA Service has been enhanced to:

  (a) Support the RSA PSS v2.1 padding scheme;

  (b) Manage the size of the service logs by selecting only those transactional details that are required so that the database overhead is reduced for high throughput systems;

  (c) Allow the transaction logs to be searched by nonce value, message imprint value and timestamp serial number.

- ADSS Go>Sign Viewer has been enhanced to allow a user to sign all assigned fields in one click.

- ADSS Server has been enhanced to:

  (a) In the OCSP Service, return “tryLater” if the Full Certificate Status Database (whitelist data) becomes unavailable;

  (b) In Trust Manager, enable CRL polling at nextUpdate as a default setting when configuring a CA’s validation policy;

  (c) Enable an ADSS Server operator to configure connection pool settings for HSMs;

  (d) The default database connection pool settings have updated to provide enhanced performance.

ADSS Server v5.2.0.4 September 2016

- Resolved a Signing Service issue related to the formatting of the emails after signing.

ADSS Server v5.2.0.3 September 2016

- Resolved a Go>Sign Applet issue to return the valid certificate chain.
- PDF Signature verification is enhanced as well as the correct timestamp signature algorithm is now returned by the Verification Service.

ADSS Server v5.2.0.2 August 2016

- Resolved a Go>Sign Service issue in producing XAdES signatures.
- Resolved a Certification Service issue related to certificate issuance from QuoVadis as an external CA.
- Resolved an OCSP Service issue in handling of OCSP response headers when nextUpdate is not available.

ADSS Server v5.2.0.1 August 2016

- Resolved a Go>Sign Service issue related to loading of certificates from windows keystore when using JDK 1.8.0 update 101.
- License expiry as well as NTP Monitoring alerts have been optimized.

ADSS Server v5.2 July 2016

- The ADSS Signing Service has been enhanced to meet the EU eIDAS Regulation requirements to:

(a) Create Qualified Signatures using server-side (remote) signing in accordance with CEN/TS 419241;

(b) Create Qualified eSeals using server-side (remote) signing with user authorisation in accordance with CEN/TS 419241.

- ADSS TSA Service has been enhanced to meet the EU eIDAS Regulation requirements specified in ETSI EN 319 422.
- ADSS Go>Sign Viewer has been enhanced to show PDF certified signature restrictions.
- ADSS Server now supports Microsoft Azure SQL Database (SQL database as a service).
- ADSS Server can now send license expiry alerts to designated operators

ADSS Server v5.1.0.2 June 2016

- Resolved a signing service issue related to adding the issuer CA name, having special characters in subject DN, correctly in the signed xml file while generating XAdES signatures

ADSS Server v5.1.0.1 June 2016

- ADSS TSA Service has been enhanced to optionally include timestamp authority name in the timestamp token.

ADSS Server v5.1 April 2016

- The ADSS Server Certification Service has been enhanced to:

  (a) Allow the same certificate alias to be used independently by multiple clients – Internally ADSS Server now appends the Client Originator ID to each Certificate Alias to provide internal separation;

  (b) Allow attribute certificate issuance requests to be rejected if the CA certificate validity constraints are violated.

- ADSS Server now supports the EU eIDAS Regulation No. 910/2014 and allows all possible RDNs and QC statements when generating qualified certificates.
- The ADSS Server Go>Sign Service has been enhanced to support the Microsoft Edge browser.
- The ADSS Server LTANS Service no longer stores the ERS data if the archive data cannot be published to the defined URL.

ADSS Server v5.0.0.7 April 2016

- Resolved a Go>Sign Applet issue related to returning the signed document.

ADSS Server v5.0.0.6 March 2016

- Enhanced the TSA Service access control filter to support Serbian characters in the SSL Client certificate subject DN.
- Resolved an issue in OCSP Service Management Reporting related to Daily Request Report.

ADSS Server v5.0.0.5 March 2016

- Resolved an ADSS Server upgrade issue when installed with Oracle database.
- Resolved an OCSP Service issue related to full certificate status checking for non-issued certificates.
- Resolved a change password issue in Certification Service.
- Resolved an issue related to generating KEK using KEK utility.

ADSS Server v5.0.0.4 February 2016

- Resolved an issue in OCSP Service Management Reporting for daily request report.

ADSS Server v5.0.0.3 February 2016

- Resolved an issue in loading OCSP Service Transaction logs and management reports.

- Resolved an issue in deleting a TA from Trust Manager when ADSS Server is installed in load-balanced configuration.

ADSS Server v5.0.0.2 — February 2016

- ADSS Go>Sign Viewer has been enhanced to support hand signature drawing on surface tablet/touch screens.
- ADSS Go>Sign Service AJAX calls have been changed to support only synchronous mode.

ADSS Server v5.0.0.1 — January 2016

- LTANS Service has been enhanced to send ArchiveID in the HTTP response header when archive data is published to a URL.
- Resolved an issue related to backward compatibility with AFP v4.x.

ADSS Server v5.0 — December 2015

- ADSS Go>Sign Service can now sign using a new Go>Sign Desktop local signing application that does away with the problems of signed Java Applets. Go>Sign Applet is still available but its use is gradually being affected by restrictions in browsers such as Chrome. Go>Sign Desktop must be installed locally but then works with any HTML5 browser using JavaScript interactions. Go>Sign Desktop offers the same functionality as Go>Sign Applet and is currently available for Windows Desktops, version for MacOSX and Unix will follow.
- ADSS Signing Service now supports signing multiple documents in a single HTTP/S (high speed protocol) request. Multiple documents were always supported using the slower OASIS DSS protocol.
- ADSS Signing Service and ADSS Go>Sign Service now support signing using selected elements within an XML document that are explicitly defined in the signing profile or within an referenced XPath expression.
- ADSS Certification Service now supports asynchronous certificate request and response processing. This is useful where vetting of a certificate application must take place prior to certificate issuance.
- ADSS OCSP Service now supports "NextUpdate" field in OCSP responses for non-existent certificates during white list checking. The Management Reporting section offers a new Daily Request Report feature that provides a line graph display for the period requested.
- ADSS Server now supports the choice of hash algorithm to be used while sending requests to other OCSP responders.
- For various services within Management Reporting, the display of transaction logs is much faster.
- ADSS OCSP Server and ADSS SCVP Server are being submitted for recertification under the FIPS 201 standard to provide PIV card validation services that comply with HSPD-12.

ADSS Server v4.8.6.4 — December 2015

- Resolved a Verification Service issue related to PDF Signature Verification.
- Resolve a Certification Service issue related to change password call when the issued certificate resides in the HSM.

ADSS Server v4.8.6.3 — November 2015

- Resolved a Certification Service issue related to unique serial number generation.

ADSS Server v4.8.6.2 — October 2015

- Resolved a Go>Sign Service issue related to local signing using Belgium eID cards.

ADSS Server v4.8.6.1 — October 2015

- Resolved an LTANS Service issue related to logging of Export transactions.
- Resolve an issue related to updating Go>Sign profiles.

ADSS Server v4.8.6 — September 2015

- ADSS Key Manager now supports the latest Microsoft Azure Key Vault APIs.
- ADSS Go>Sign Service now supports local signing using IntoIT middleware to support Belgian eID smartcards without using a local Java runtime.
- ADSS Go>Sign Service now supports mobile signing using AET Mobile ConsentID.
- The Manage CAs module now supports direct calls to GlobalSign's online Certificate Service.
- ADSS Server can now request certificates from a remote ADSS CA Server using a secure client/server TLS/SSL channel.

ADSS Server v4.8.5.5 — September 2015

- Resolved an RA Service issue related to approving Device Certificates by Security Officer.

ADSS Server v4.8.5.4 — September 2015

- Resolved an issue in OCSP Service while adding responder certificate in the OCSP response.

ADSS Server v4.8.5.3 — August 2015

- Resolved an issue in HMAC recompute utility.

ADSS Server v4.8.5.2 — August 2015

- Resolved an issue in Import/Export functionality.
- Resolved an issue related to headless installation in load-balanced mode.

ADSS Server v4.8.5 — July 2015

- ADSS Server now supports Distributed OCSP and complies with the new RFC 6960 and old RFC 2560 standards in this area.
- A new separately licensed ADSS Server OCSP Repeater Service is now available which works with a separate full ADSS Server OCSP Service to provide precomputed OCSP responses for local OCSP clients - this is valuable where local OCSP clients do not want to always rely on central but remote OCSP servers and/or where speed of response is vital such as in PACS/LACS (physical or logical access control systems).
- The Manage CAs module has been enhanced to support direct communication with the following external CAs:

  (a) Windows Server 2008 and 2012 CA;

  (b) QuoVadis CA.

  This is in addition to the current support for ADSS CA Server, GlobalSign CA and PrimeKey CA (EJBCA).
- The Signing Service has been enhanced to allow API calls to override the value for the “Signed By” field in a visible signature.
- Memory and database connections statistics can now be examined by clicking “System Health” in the Server Manager module and new operator alert messages can be configured for these items within the Global Settings > System Alerts page.
- Manual renewal of infrastructure certificates is now possible in Key Manager.
- An existing profile / or certificate template can be used as a base when creating a new profile or template for selected services.

ADSS Server v4.8.4.5 — June 2015

- Resolved an issue related to HTTP Headers in OCSP Service.

ADSS Server v4.8.4.4 — June 2015

- Resolved an issue related to KEK generation in Thales HSM.

ADSS Server v4.8.4.3 June 2015

- Resolved an issue related to publishing of large CRLs.
- Go>Sign Service has been enhanced based on the ETSI plug-test findings.

ADSS Server v4.8.4.2 May 2015

- Resolved an issue related to HSM connectivity on Linux OS.
- Resolved an issue related to deleting TAs from Trust Manager.

ADSS Server v4.8.4.1 May 2015

- Resolved an issue related to database connectivity.

ADSS Server v4.8.4 April 2015

- ADSS Server has been enhanced to utilise Java 8 (JDK 1.8.0u31) and Apache Tomcat 8 (8.0.20).
- The Key Manager module has been enhanced:
  (a) To support Microsoft Azure Key Vault using the software or HSM based keystore;
  (b) To allow automatic renewal of infrastructure certificates to be enabled or disabled.
- The JVM maximum memory parameters for the ADSS Core, Console and Service Windows services or UNIX daemons are now configurable via the installation wizard.
- The Manage CAs module has been enhanced to view and save the CRLs for local CAs and send alerts when automatic CRL publishing fails.
- The ADSS Signing Service has been enhanced to ensure that PDF document conversion and signing is PDF/A-1, PDF/A-2 and PDF/A-3 compliant and to also support centrally created signature location profiles.
- The ADSS Go>Sign Service has been enhanced to sign multiple fields assigned to the current user in one go.
- ADSS Server Console has been enhanced to manage and repair HMAC verification failures if these arise in the Transactions Log of any service;
- Microsoft SQL Server 2014 and PostgreSQL 9.4 have been added to the list of supported databases.

ADSS Server v4.8.3 February 2015

- The HSM key wrapping functionality has been enhanced to ensure that SSCD Type 2 (CWA 14169 PP) compliant signatures are produced.
- The ADSS Signing Service has been enhanced to allow the signing profile to define the PDF signature dictionary size - this enables operators to create profiles that allow larger (or smaller) signature data sizes to be successfully embedded in the PDF.
- The ADSS Verification Service has been enhanced to provide detailed information for PAdES Part 2 and PAdES Part 4 signatures.
- The Manage CAs module has been enhanced to be able to use EJBCA and GlobalSign CAs as online external Certificate Service Providers.
- ADSS Go>Sign Service has been enhanced:
  (a) To ensure that PDF document conversion is PDF/A-1, PDF/A-2 and PDF/A-3 compliant;
  (b) To create empty signature fields at predefined locations;
  (c) To allow Go>Sign Applet to reload in single page application without reloading the page.
- ADSS Go>Sign Viewer can now display and sign Microsoft Word 2013 and Word 365 documents.
- Configurations in the ADSS Server properties files have been moved to be within the Admin Console under Global Settings > Advanced Settings to ensure the settings are preserved during upgrade.

ADSS Server v4.8.2.2 January 2014

- Resolved an issue related to email alerts when sent using SMTPS (i.e. SMTP over TLS/SSL).

ADSS Server v4.8.2.1 December 2014

- ADSS Server Manage CAs now allows user key and certificate containers to be imported and used with document signing requests.
- The ADSS Go>Sign Service now allows ADSS Go>Sign Applet to be used in a web page with or without calling "OnPageLoad".
- An ADSS Certification Service issue seen when HolderEntityName contains "UniformResourceIdentifier" or "OtherName" elements in Attribute Certificates has been resolved.

ADSS Server v4.8.2 November 2014

- ADSS Signing and Verification Services have been enhanced to create and verify Microsoft Office 2013 and Office 365 signatures.
- The ADSS Certification Service has been enhanced to:
  (a) Support Certificate Transparency extensions within TLS/SSL server certificates compliant with RFC 6962;
  (b) Enable certificate issuance requests to be prevented if CA certificate constraints are violated.
- The ADSS Verification Service now supports embedding attribute certificates within digital signatures as part of verification and enhancement.
- Local Certificate Authorities and Attribute Authorities support the publishing of their issued certificates on a defined LDAP server.
- When exporting ADSS Server configuration data all dependent configurations are now automatically included.

ADSS Server v4.8.1 September 2014

- ADSS Server can now be scheduled to restart at a selected future time, typically a quiet time such as 02:00 so that any configuration changes and the subsequent restart do not affect processing during business hours.
- The ADSS SCVP Service has been enhanced to dynamically discover the chain for an OCSP Responder certificate when using advanced discovery settings.
- The ADSS Certification Service has been enhanced to allow certificate validity periods to be defined in units of minutes, hours, days, months and years to better support short life certificates.
- The ADSS Manage CAs module has a new licensed Attribute Authority option. This can issue and revoke attribute certificates for existing identity certificates. Various Attribute Certificate profiles can be defined and a Registration Authority can request attribute certificates through the web services interface.

ADSS Server v4.8 August 2014

- ADSS Server currently supports keys held permanently within an HSM. A new feature allows keys to be exported under an HSM held and managed Key Encrypting Key (KEK) and held securely within the ADSS Server database where HSMs allow this functionality. This means that large numbers of users can now be enrolled within ADSS Server and have their own unique keys and certificates.
- The ADSS Certification Service now integrates with Active Directory to create user keys & certificates.
- ADSS Signing service and ADSS Verification Service have been enhanced:
  (a) Stand-alone PDF document timestamps can be created and verified;
  (b) XAdES v1.4.1 is now supported.
- ADSS SCVP Service now supports validation fall-back options using CDP and AIA based addresses.
- The Key Manager module has been enhanced to support Windows CAPI/CNG software or CAPI/CNG based HSMs.

- The Manage CAs module has been enhanced to allow the CRL publishing period to be set independently of the CRL expiry date to allow over-issuance. In addition all issued certificates can have their expiry dates limited to the issuer CA certificate expiry.
- ADSS Server Console has been enhanced:
  (a) All load balanced ADSS Server systems are shown on the Admin screen home page;
  (b) To simplify manual OCSP routing configuration management multiple CA certificates can be imported at once from a system folder entered in the Service > Manual Routing page. This is valuable for large scale PKIs with routers that do not use the service locator extension;
  (c) To allow the ADSS Server hostname/IP address to be changed in the Server Manager module. This is valuable when the hostname/IP is changed after the ADSS Server installation.
- The configuration settings “Import” feature now enables an operator to choose to overwrite or skip configuration data that already exists in the target installation when importing saved configuration data.
- New operator alert messages are produced for the Core and Console services or daemons when in high availability mode and the “Slave” instance takes over from the “Master” instance.

ADSS Server v4.7.7.3 June 2014

- The Certification Service now supports the custom Subject Alternative Name extension within the SOAP XML protocol.
- ADSS CRL Monitor can now download the CRLs from a URL that contains a '+' sign.
- An issue in the Certification Service CMC protocol has been resolved.

ADSS Server v4.7.7.2 May 2014

- Resolved an issue handling special characters within certificate DNames.

ADSS Server v4.7.7.1 May 2014

- Resolved a licensing issue affecting XML signatures in the ADSS Verification Service.

ADSS Server v4.7.7 May 2014

- ADSS Signing Service and ADSS Go>Sign Service now feature a new HTML based “Signature Appearance” designer.
- The ADSS Verification Service now shows signature enhancement failures in the Transactions Log Viewer.
- The ADSS TSA Service has been enhanced to optionally use time obtained directly from the NTP servers configured in the NTP Time Monitor.
- ADSS Server Core instance now uses a high availability architecture on load-balanced systems.
- The default view on the ADSS CRL Monitor > CRL Details page now shows just those CAs whose Validation Policy is ‘Local CRL Cache’ or where automated polling is enabled for the CA.
- New system wide alerts are provided in the Global Settings > System Alerts page to alert operators about issues in database connections, certificate expiry and configuration change events.
- The Trust Manager module has been enhanced such that:
  (a) The OCSP Request Signing certificate is now configurable from the Validation Policy tab, previously it was on Back-end Certificates tab;
  (b) Trust Manager only shows the options related to the licensed services.
- ADSS Go>Sign Service has been enhanced to:
  (a) Support signed attributes in AdES signatures;
  (b) Support EPES signatures;
  (c) Use a hand signature image and/or company logo image provided by the business application.
- A new test case has been added to the PKCS#11 test utility to check the support for internal clock in the HSM.
- A new Trace Logs Utility is added which collects the product trace logs and appropriate ADSS Server information in a zip file. This assists in gathering the log information in one operation and will speed up the customer support process.
- ADSS Server Admin Console has been enhanced in these ways:
  (a) In Key Manager a hardware crypto profile can now be set as Active/Inactive;
  (b) In Global Settings Import/Export of Operators and Roles is now supported;
  (c) You can now search the Transactions Log Viewer using the Log ID value in each service;
  (d) The Verification Service > Signature Settings tab only shows the licensed signature types;
  (e) Management reports now default to show the last month’s data;
  (f) In OCSP Monitor and CRL Monitor an event count threshold is now available to not send alerts until the defined threshold is reached;
  (g) An on-screen alert has been added to identity certificates that have expired or are about to expire.
- Database drivers for all supported databases have been upgraded to the latest available versions. SQL Server driver (JTDS) stays at v1.2.2. Hibernate has been upgraded to the latest available version (v4.3.1). Database connection pool management has been enhanced.
  (a) ADSS Server now supports these databases versions: PostgreSQL 9.3; Oracle 12C; MySQL 5.6.

ADSS Server v4.7.6.1 February 2014

- Resolved an ADSS OCSP Service issue related to NextUpdate value in the OCSP responses when real-time certificate status database is used.

ADSS Server v4.7.6 January 2014

- ADSS Verification Service has been enhanced to support:
  (a) The OASIS DSS item “TimeStampContent” in the “VerificationReport” element of the response;
  (b) For historical validation, the CRL issued immediately before signing and the next CRL (after signing) are checked to see if the certificate was identified as revoked before the signing time.
- The ADSS Signing Service has a new HTML based PDF editor that is used to define blank signature field locations and manage signature appearances.
- ADSS LTANS Service enhanced to support:
  (a) A new optional HTTP protocol that delivers substantially better performance;
  (b) A new “renew” evidence request is supported via the HTTP interface - this is needed when ADSS Server only retains the original ERS and allows the original data to be sent once again to enable a new hash algorithm to be used within the LTANS profile.
- Log Archive management has been enhanced to:
  (a) Write all archived logs in zipped format to save the disk space;
  (b) Archived logs are now imported using a fast bulk-processing mode for better performance.
- ADSS OCSP Service has been enhanced to:
  (a) Allow smaller transactions logs to be created by deselecting certain transaction viewer columns, thus reducing the database overhead for heavily used systems;
  (b) A separate flag now identifies records processed using full certificate white list checking;
  (c) Non-issued certificate requests can now be searched for within the transactions log viewer;
  (d) OCSP responses can be set to “unknown” or “unauthorized” as required for certificates not issued by defined Trust Anchors;
  (e) OCSP response nextUpdate fields can now be set to contain a value even when using real-time whitelist data to meet RFC 5019 section 4 requirements;
  (f) HTTP header attributes have been implemented to meet RFC 5019 section 5 requirements that enable client OCSP caching.
- ADSS Go>Sign Service has been enhanced to:
  (a) Support local bulk document signing;
  (b) Go>Sign Profiles can now define multiple certificate issuers within the certificate filter criteria;
  (c) Browser cache management has been improved for Go>Sign Viewer/Applet;
  (d) Detect and report if the Java plugin is missing or not enabled on MAC OSX.
- ADSS Server now supports CRL and OCSP response caching for CAs registered in Trust Manager using CDP and AIA options (this was already supported for non-registered CAs).
- The term PAdES-A has been retired and is now referred to as a PDF Document Timestamping.
- ADSS Server now uses SHA-256 as the default hash algorithm when creating PKCS#10 requests.
- ADSS Server Access Control now allows Operators to be deleted in addition to being set as inactive.
- The ADSS Server sample data has been updated.

ADSS Server v4.7.5.1 October 2013

- An issue within HMAC verification related to DB connection pool exhaustion has been fixed.
- PAdES Part 4 LTV signatures have been enhanced to improve industry interoperability

- ADSS Go>Sign Service / Go>Sign Applet has been enhanced to add the extra manifest attributes required to support recent JRE 7 updates.
- ADSS Client Manager has been enhanced to fix a number profile management issues

ADSS Server v4.7.5 October 2013

- ADSS Server has been enhanced to utilise Java 7 update 25 and Apache Tomcat 7.0.42
- ADSS Verification Service has been enhanced to optionally use the current CRL for historical validation when it contains historic data.
- ADSS CRL Monitor has been enhanced to confirm that:
  (a) The CRL data has been expanded successfully in the ADSS Server database and;
  (b) Optionally generate an alert when the CRL number of the downloaded CRL does not have the next sequential number from the previous CRL.
- ADSS SCVP Service has been enhanced:
  (a) Smart Card Logon and Any Purpose bits are now shown in the Extended Key Usage list;
  (b) If multiple EKUs are provided in the profile, then the target certificate must contain all these EKUs;
  (c) The list of validated OIDs is shown in the transaction logs.

ADSS Server v4.7.4.6 August 2013

- Resolved an issue in the ADSS Verification Service handling certificates with UTF-8 encoding in the subject DN.
- Fixed an issue with handling special characters when using username and password to authenticate to external TSAs.

ADSS Server v4.7.4.5 August 2013

- ADSS Signing Service now supports Universal Business Language (UBL) signatures.
- The ADSS Server setup script has been enhanced for headless mode operation.
- Issues related to:
  (a) empty signature field creation;
  (b) SCVP Service for policy mapping, and;
  (c) OCSP relayed requests have been fixed.

ADSS Server v4.7.4.4 August 2013

- ADSS LTANS Service performance has been enhanced for LIST_IDs service requests.

ADSS Server v4.7.4.2 July 2013

- Resolved a Trust Manager issue related to updating the registered trusted authorities.

ADSS Server v4.7.4.1 July 2013

- The ADSS Certification Service has been enhanced to these ways:
  (a) Added option to include multiple distribution points in the issued certificate's CDP extension;
  (b) All issued CRLs will now contain AKI extension;
  (c) Added option to include AIA extension in the issued CRLs.

ADSS Server v4.7.4 July 2013

- ADSS OCSP Service has been enhanced to enable compliance with RFC 6960 whitelist checking.
- The ADSS Certification Service and ADSS RA Service protocols have been enhanced to add SAN extensions rfc822Name and dNSName in addition to allowing this within Key Manager.

- ADSS Server now supports username/password based authentication to external TSAs.
- The ADSS Verification Service has been tuned for better performance and an issue fixed when upgrading an XAdES signature to a long-term format if it is created using a SHA-2 hash.
- The ADSS LTANS Service has been modified such that when the hash algorithm is changed within a profile only the ERS archives that have their Archive Data stored locally will be automatically refreshed.

ADSS Server v4.7.3 June 2013

- The ADSS Go>Sign Service has been enhanced in these ways:
  (a) Documents and data are now hashed within the Go>Sign Service to optimise performance and security, Go>Sign Applet now creates PKCS#1 signatures so that the signature format can be finalised on the server and extended to timestamp or long-term format as required;
  (b) Business applications can now send just the hash of XML or text file for XML/XAdES or PKCS#7/CMS/CAdES signatures to be signed by Go>Sign Applet;
  (c) NSS key stores are now supported.
  (d) Real time PIN handling for PKCS#11 devices is supported using errors returned by the device.
- The Go>Sign Document Viewer has been enhanced in these ways:
  (a) Document Viewer settings now have a new profile tab called “Viewer Settings”;
  (b) Document conversion now uses licensed technology from Apose instead of OpenOffice;
  (c) Automatic generation of field name can be enforced by profile settings;
  (d) A top bar shows the overall status of the signatures in the open document;
  (e) A nice certificate viewer has been added to show the detail of signer certificates;
  (f) WACOM and Signotec tablets now show a rectangle to maintain the signature image aspect ratio.
- The ADSS Verification Service has been enhanced such that each verification profile can define the policy for allowed hash algorithms, key algorithms and key lengths.
- ADSS Server HMAC verification process has been improved to separately identify missing HMAC values in the HMAC verification report instead of reporting such records as HMAC verification error

ADSS Server v4.7.2 April 2013

- The Manage CAs module has been enhanced to configure the ADSS Server as an external CA.
- The ADSS Signing Service now supports certificate revocation checking for BES signatures.
- The ADSS Server admin console has been enhanced to help the administrator/operator when the database is not available.
- The ADSS Go>Sign Service has been enhanced to:
  (a) Embed the certificate chain when creating a local signature;
  (b) Draw empty signature fields with same aspect ratio as the signature appearances and create hand signature images with the same aspect ratio as the signature appearances;
  (c) Improve localisation by adding new language options for different info, error and warning messages;
  (d) Provide a dialog box that displays the hand signature image drawn on the tablet device;
  (e) When signing a document with a profile that requests a certifying PDF signature, any subsequent signature operation will ignore the ‘certify’ request since this can only be applied once;
  (f) Reason, Location and Contact info can be marked as mandatory;
  (g) The Go>Sign transaction log contains entries for each individual action taken in the Document Viewer;
  (h) Certificate revocation checking is performed for BES signatures;
  (i) Go>Sign profiles can now control the use of the “draw, text and upload” tabs for hand signature images within the document viewer.

- The Go>Sign Document Viewer has been enhanced to:
  (a) Provide support for PDF form fields;
  (b) Provide a cancel button to cancel the signing operation;
  (c) Resolve issues related to page scrolling and message dialog displacements;
  (d) Optionally show tooltips on the Open and Finish buttons to guide new users;
  (e) Improve the information display on the signature verification dialog;
  (f) Move a new signature field by attaching it as the mouse pointer and then dropping it on the document when the mouse is clicked;
  (g) Provide feedback to a business application so it can perform new operations based on the user action, e.g. reload the web-page using a different Go>Sign profile;
  (h) Enforce the signing of fields in incremental way based on the field name and number;
  (i) A new interface can show error messages in any language that is provided.

ADSS Server v4.7.1.10 — April 2013

- Resolved an ADSS Go>Sign Service issue when signing with PKCS#11 tokens.

ADSS Server v4.7.1.9 — April 2013

- Resolved an issue with user sessions across multiple load-balanced ADSS Go>Sign Service instances.

ADSS Server v4.7.1.8 — April 2013

- Resolved an issue with user sessions across multiple load-balanced ADSS Go>Sign Service instances.
- Resolved an issue when enhancing a basic signature to an advanced format in ADSS Verification Service.
- Resolved an issue with CRL polling status when using multiple load-balanced ADSS CRL Monitor Service instances.

ADSS Server v4.7.1.7 — March 2013

- Improved support for user sessions across multiple load-balanced ADSS Go>Sign Service instances.
- Resolved an issue related to email alerts when sent using SMTPS (i.e. SMTP over TLS/SSL).
- Resolved an issue in OCSP Monitor related to daily test scenario execution.

ADSS Server v4.7.1.6 — March 2013

- PKCS#11 support provided in the Go>Sign Service for Linux and MAC operating systems.

ADSS Server v4.7.1.5 — February 2013

- A Go>Sign Service PKCS#11 PIN caching issue has been fixed.

ADSS Server v4.7.1.4 — February 2013

- Resolved Go>Sign Service issues:
  (a) when handling multiple signatures within the same session;
  (b) avoiding an additional upload when the document source is set to server.

ADSS Server v4.7.1.3 — February 2013

- Resolved a Go>Sign Service signature appearance issue.

ADSS Server v4.7.1.2 — February 2013

- Homepage alerts will now be supressed for inactive profiles, operators and certificates to avoid unnecessary messages.

- Resolved an issue in Verification Service related to use of the configured grace period when operating in HTTP mode.
- Go>Sign Service has been improved:

  (a) To support space characters and custom defined values in the Certificate Alias display pattern;

  (b) To prevent signing using older v1 UAE EID cards which do not contain hand-signature images;

  (c) Signing dialog has been enhanced to show the remaining number of retries for the PKCS#11 device PIN.

ADSS Server v4.7.1.1 — January 2013

- ADSS Go>Sign Service has been enhanced to support:

  (a) User sessions across all load balanced instances;

  (b) Business applications can now dynamically set certificate filter criteria;

  (c) Application requests that contain just the document/data hash for signature;

  (d) Server-side signing using the document viewer - a signing passphrase dialog is now available;

  (e) Resolved an issue relating to Icelandic characters support in the Go>Sign Document Viewer.
- Key Manager HMAC key generation has been enhanced to offer additional key sizes
- ADSS Go>Sign Applet has been enhanced to work with the UAE eID cards

ADSS Server v4.7.1 — January 2013

- ADSS Server Certification and RA Services have been enhanced to support the CAB Forum EV SSL requirements.
- An option is introduced in ADSS Certification Service profile to reject the request if requested Subject DN does not match the Subject DN pattern configured in certification profile.
- ADSS Certification Service has been enhanced to handle the Names Constraint in Subject DN.
- ADSS Server certificate templates now supports the Acrobat Authentic Documents Extended Key Usage (EKU) option.
- ADSS Certification Service profiles now allow the selection of the crypto profile for the keys and certificates created.
- ADSS Go>Sign Service has been enhanced to provide tight integration with UAE eID card features

ADSS Server v4.7 — December 2012

- A new ADSS RA Service is now available as a licensed option. This service manages certification and revocation requests from end-users, applications, servers and SCEP protocol devices.
- ADSS Go>Sign Service and ADSS Go>Sign Applet have been enhanced to support local key generation and CSR handling for the ADSS RA Service.

ADSS Server v4.6.1.5 — November 2012

- Resolved an issue related to Certificate Viewer within ADSS Server Console.

ADSS Server v4.6.1.4 — November 2012

- The ADSS Go>Sign Service has been enhanced by providing support for Wacom signature tablets on both Citrix and non-Citrix environments.
- An issue related to behaviour of “Cancel” button on signature tablet dialog has been resolved in the ADSS Go>Sign Service.
- Signature tablet disconnection handling in the ADSS Go>Sign Applet has been enhanced.

ADSS Server v4.6.1.3 — November 2012

- The ADSS Go>Sign Applet now provides transaction status when Finish button is clicked.
- Implementation for “OK” and “Cancel” buttons on signature tablet dialog has been enhanced in the ADSS Go>Sign Applet.
- The ADSS Go>Sign Applet signing dialog has been enhanced – now it does not show hand signature options when the associated signature appearance profile does not include the hand signature.

ADSS Server v4.6.1.1 November 2012

- A few issues related to hand signature image in signature appearance have been resolved when using Signature tablet device.

ADSS Server v4.6.1 October 2012

- The ADSS Go>Sign Service has been enhanced by providing support for Signotec signature tablets on both Citrix and non-Citrix environments.
- An issue related to publishing of CRLs by local CA has been resolved in Manage CAs.

ADSS Server v4.6.0.2 October 2012

- An issue related to unnecessary increase in size of PDF documents upon signing has been resolved in ADSS Go>Sign Service.
- The ADSS Go>Sign Service has been improved to allow generating multiple signatures using a PKCS#11 device in a single session.
- The ADSS Go>Sign Service has been improved to resolve interoperability issues when accessing the Go>Sign demos in Firefox, Chrome and IE internet browsers.

ADSS Server v4.6.0.1 October 2012

- The ADSS Go>Sign Service has been improved to require business applications to request the signed document back from the ADSS Go>Sign Service.

ADSS Server v4.6 September 2012

- A new ADSS Go>Sign Service is now available as a licensed option. This service updates and enhances the way Go>Sign Applet works with business applications. The ADSS Go>Sign Service allows multiple profiles to be created to select and control the functionality of Go>Sign Applet. A new server component, ADSS Go>Sign Viewer provides powerful PDF display, navigate, and signing features.
- Multiple PKCS#11 drivers are now supported in the new Go>Sign Service. This allows Go>Sign Applet to work in environments where multiple smartcards/USB tokens are deployed and users need to be able to sign with the token type they have been given.
- A new OCSP Monitor Service is now available as a licensed option. It fully replaces the current OCSP Monitor desktop product and is valuable in monitoring the correct functioning of one or multiple OCSP servers/ OCSP responders.
- The CRL Monitor Service has been enhanced with an advanced reporting option and new reports and alerts are available.

ADSS Server v4.5.7.3 September 2012

- An issue related to verification of archive files stored on the file system in LTANS Service has been resolved.

ADSS Server v4.5.7.2 August 2012

- An issue related to Accuracy settings in TSA Service profiles has been resolved.

ADSS Server v4.5.7.1 July 2012

- An issue related to Turkish characters’ support has been resolved.

- An issue related to use of optimized HTTP protocol in Verification Service has been resolved.

ADSS Server v4.5.7 July 2012

- ADSS Verification Service manager now has a setting to define if the input signed data objects/documents are stored in the database.

ADSS Server v4.5.6.2 June 2012

- An issue related to editing Signing Service profiles has been resolved.
- Resolved a couple of issues related to CRL Monitoring Service debug logging.

ADSS Server v4.5.6.1 June 2012

- An issue related to LTANS archive validity has been resolved when the archive renewal time was set to a value above 68 years.
- An issue related to Signing Service has been resolved when signing documents using existing keys imported from an HSM.
- Database connection leakage issues have been resolved in ADSS Server Console and Service components.

ADSS Server v4.5.6 May 2012

- ADSS Verification Service profiles have been enhanced to allow one or more selected Time Stamping Authorities (TSAs) to be configured and used when enhancing a basic signature to include a timestamp.
- The ADSS Verification Service can now optionally use an optimised HTTP protocol to substantially improve performance over OASIS DSS web services, the selection is done using a protocol flag in the ADSS Client SDK.
- Email, SMS and SNMP alerts have been enhanced by introducing general alerts when the database or optional HSM(s) become disconnected or become available again.
- SHA-256 is now the default hashing algorithm when configuring ADSS Server services.

ADSS Server v4.5.5.2 May 2012

- An issue related to database connections has been resolved when processing large number of OCSP Service requests.

ADSS Server v4.5.5.1 April 2012

- Process has been enhanced to cache the latest CRL in memory for high speed OCSP responses.

ADSS Server v4.5.5 April 2012

- ADSS TSA Service now supports Microsoft Authenticode timestamp requests.
- ADSS Signing Service now supports PDF Permissions and can thus set copying, printing and commenting rights. The signature appearances designer has been enhanced to allow much greater control of signature appearances for new or existing signature fields.
- ADSS CRL Monitor has been enhanced to factor the CRL freshness policy into the calculation of when the CRL Next Update time has arrived. There is also a new option that allows just the latest CRL to be retained to improve database size management for one or multiple CAs with very large CRLs. The Transaction Log viewer has been enhanced.
- ADSS Trust Manager has been enhanced to enable a Time Stamp Authority to be associated with a particular CA so that local signatures can be extended using the appropriate TSA when using a common signature profile.
- The ADSS Console starts quicker than before with any alerts shown after the home page has loaded.

ADSS Server v4.5.4.2 March 2012

- Certificate path building has been enhanced in various ADSS services to support non-English characters in certificate subject name.

ADSS Server v4.5.4.1 March 2012

- Resolved an OCSP service issue related to loading CRLs in memory for high speed OCSP responses.

ADSS Server v4.5.4 March 2012

- ADSS CRL Monitor has been enhanced to allow all prior CRLs to be deleted and thus reset CRL information for a particular CA.
- ADSS CRL Monitor can now import revocation information from multiple partitioned CRLs stored in an LDAP repository as a feed for the OCSP service.
- ADSS LTANS Service has been enhanced such that (a) LTANS profiles now define the Signing and Verification authority addresses to be used and (b) greater control is offered over the inclusion of meta-items when computing the XMLERS and notary signatures and during subsequent storage.
- ADSS Signing and Verification services now support PDF collections.
- The ADSS Signing Service PDF signature appearances designer has been improved.
- Following a successful ETSI PAdES plug test a number of enhancements have been integrated.
- The Certification Service now supports the deletion of valid keys and certificates via the API.
- PostgreSQL 9.1 has been tested and added to the list of supported databases.
- Solaris 11 has been tested and added to the list of supported operating system.

ADSS Server v4.5.3.3 February 2012

- Resolved a CRL Monitoring issue related to CRL polling.

ADSS Server v4.5.3.2 February 2012

- Resolved an issue related to XML signature verification in ADSS Verification Service.
- ADSS Server installation wizard has been enhanced to resolve a problem with inserting sample data

ADSS Server v4.5.3.1 January 2012

- Path validation has been enhanced in XKMS, SCVP and Verification services to support dynamic path building using NIST LDAP repository. PKITS test cases pass when test data is imported manually and also when data is discovered dynamically from NIST LDAP repository.

ADSS Server v4.5.3 January 2012

- The ADSS Signing service higher speed HTTP interface has been enhanced to support signing attributes and PDF signature appearance profiles (these were already supported within the OASIS DSS interface).
- The OCSP service and Timestamp service response messages now support signing using the GOST algorithm.
- ADSS Server has been updated to use Java EE 6 release 29 (jdk1.6.0_29).

ADSS Server v4.5.2.2 January 2012

- An issue related to database connection pool management has been resolved.

ADSS Server v4.5.2.1 November 2011

- Handling of longer key aliases is enhanced for the keys imported from hardware crypto devices.

ADSS Server v4.5.2 — November 2011

- To respond to the recent attacks on trusted CA services ADSS Server can be licensed to enable Trust Manager to mark a CA as revoked so that all signature and certificate validation requests receive revoked responses for any issued certificate. Also CRL Monitor now allows individual certificates to be marked as revoked to allow a fraudulent certificate that was not legitimately issued to be treated as revoked.
- The Certification Service has been enhanced to allow an option to set the “Valid From” date/time for a new certificate to be in the future.
- The OCSP Service has been updated to provide an option to check if a good target certificate (i.e. not identified within a CRL) was actually issued by the issuing CA (only if the ADSS Local CA was the certificate issuer).

ADSS Server v4.5.1.3 — February 2012

- Path discovery has been enhanced in XKMS, SCVP and Verification services to avoid manually configuring additional LDAP repositories and CRLs for Trust Anchor certificates.

ADSS Server v4.5.1.2 — January 2012

- Path validation has been enhanced in XKMS, SCVP and Verification services to support dynamic path building using NIST LDAP repository. PKITS test cases pass when test data is imported manually and also when data is discovered dynamically from NIST LDAP repository.

ADSS Server v4.5.1 — October 2011

- The Verification Service has new options when checking a long-term signature that does not have an embedded timestamp: (a) the signature can be checked at the current time, or (b) an error can be returned.
- The Signing, Verification, XKMS, LTANS, Certification and Decryption Services now allow profiles to be referenced by Profile Name as well as by Profile Id.
- The OCSP Service has been updated to allow the OCSP response signature to include its certificate alone or the full certificate chain.
- The Signing Service now allows signature appearances to be overridden if this option is enabled.

ADSS Server v4.5.0.2 — October 2011

- The HSM automatic reconnection feature has been enhanced.

ADSS Server v4.5.0.1 — October 2011

- An issue related to database connection pool management has been resolved.
- Handling of revoked target certificates is enhanced in the ADSS XKMS Service.

ADSS Server v4.5 — August 2011

- Support for the Russian GOST algorithm has been added.
- Support for reason based segmented CRLs has been added.
- Certificate validation has been enhanced within the SCVP, XKMS and Verification services to include:

  a) LDAP referrals are now supported in DPD (Delegated Path Discovery);

  b) Indirect CRLs support is enhanced to satisfy PKITS DPV and DPD test cases;

  c) Information on non-registered CAs and their CRLs found within DPD processing is now cached.

ADSS Server v4.4.4.2 (Patch release) — August 2011

- An issue related to signing PDF on multiple pages has been resolved.

ADSS Server v4.4.4.1 (Patch release) August 2011

- HSM auto reconnection logic has been enhanced.

ADSS Server v4.4.4 July 2011

- The ADSS Signing Service can now use configuration settings to manually allocate and optimise the space for PDF signature dictionaries.
- The Certification Service and Manage CAs modules now support custom Subject Alternative Name and Issuer Alternative Name extensions and the Manage CAs module can now publish CRLs to an LDAP directory.
- The transaction logs viewer in the Verification, XKMS and SCVP service modules now provides full details of an expired CRL within the signer certificate chain.
- The ADSS Server console now automatically connects to multiple load balanced ADSS Server instances.

ADSS Server v4.4.3 June 2011

- The performance of ADSS Server Delegated Path Discovery (DPD) has been substantially increased and timeout values in seconds can now be set.
- ADSS SCVP Service now supports an easy to understand structured view of the SCVP request and response messages.
- Certificate distinguished name default configurations have been moved from Global Settings to the Key Manager module.
- A separate support utility has been added that can be used to verify the full functionality of a PKCS#11 HSM device during interop testing or fault finding.

ADSS Server v4.4.2.1 (Patch release) June 2011

- An ADSS Verification Service long term signature verification issue has been fixed as has a key quality issue when verifying PDF signatures.
- The ADSS Signing service has been enhanced by extending support for detached PAdES signatures according to ETSI TS 102 778 V1.1.1 (2009-07) PAdES profiles.

ADSS Server v4.4.2 May 2011

- ADSS Signing Service has been enhanced by:

  (a) Supporting “ISO 8601” date formats in PDF Signature appearance;

  (b) Extending support for special language characters;

  (c) Providing new settings, that can prevent a label with no value being shown for a PDF signature field when no value is supplied, e.g. (Reason: /Location: /Contact:).
- ADSS Signing and Verification services have been enhanced by providing support to generate and verify counter signatures.
- ADSS Verification Service has been enhanced by adding support for enhancing the PAdES signatures to part 3 and part 4.
- Added support for “CRL Entry Extensions” within OCSP response messages.
- SHA2 and RipeMD hashing algorithms are now supported ADSS CA Service CRL publishing.
- The ADSS TSA Service has been enhanced by:

  (a) Adding an allowed hash algorithm list;

  (b) Adding an option to reject a TSA request if it does not contain the 'certReq' flag.
- ADSS SCVP Service has been enhanced to support further RFC 5055 options, e.g. scvpServer and scvpClient EKUs are now supported in request / response signing certificates respectively.

- NTP time monitoring has been enhanced to generate an alert and stop ADSS Services when none of the configured NTP servers can be connected.
- Added support to generate certificates with multiple RDNs.

ADSS Server v4.3.4 (Patch release) — May 2011

- An ADSS SCVP Service path verification issue with Self-Issued certificates has been fixed.
- An ADSS Verification Service long term signature verification issue has been fixed. Also resolved an XML verification issue when the signer is revoked.

ADSS Server v4.3.3 (Patch release) — April 2011

- An ADSS SCVP Service FPKI path building issue has been fixed.
- An ADSS Verification Service long-term signature issue has been fixed.

ADSS Server v4.3.2 (Patch release) — April 2011

- The ADSS TSA Service now supports a list of allowed algorithms.
- An ADSS Signing Service issue relating to the handling of images within signature appearance profiles has been fixed.
- An upgrade issue relating to the default HMAC key has been resolved.

ADSS Server v4.3.1 (Patch release) — March 2011

- Resolved a trust chain issue affecting OCSP Service start-up.
- Resolved a location issue relating to blank signature field creation.
- Resolved an issue relating to email address parsing.

ADSS Server v4.3 — February 2011

- ADSS Signing and Verification services have been enhanced by:

  (a) Providing support for PAdES signatures based on ETSI PAdES standard (TS 102 778);

  (b) Providing extended support for XAdES and CAdES specifications;

  (c) Supporting the creation of PDF signature fields using X/Y coordinates (OASIS DSS-X profile).
- ADSS Signing, Verification, XKMS, Certification and LTANS services have been extended to support SOAP v1.2.
- ADSS Verification and XKMS services have been enhanced to support enveloping XML signatures in request and response messages. The ADSS XKMS Service additionally supports detached XML signatures in request and response messages.
- ADSS Verification, SCVP and XKMS services have been extended to support PKITS compliant path discovery and path validation. The Verification and XKMS services have also been enhanced to extend support for detailed PEPPOL requirements.
- A new ADSS Verification Gateway Service has been introduced as a licensed option within ADSS Server. This new service replaces the original ADSS Gateway software. Managed service providers need such Verification Gateways to allow clients to protect their data privacy by extracting the document signatures and sending only these for external verification.
- The ADSS TSA Service has been enhanced to support ESSCertIDv2 Update for RFC 3161.
- A new time drift check facility allows ADSS Server to check that server system time is acceptably accurate by cross-checking with a list of trusted NTP servers. If predefined thresholds are exceeded then ADSS Server (a) warns operators about the unacceptable time drift and can then (b) stop all services.
- ADSS Server home screen alerts have been enhanced such that the hyperlink only shows those records which are relevant to the specific alert.

- Management reports have been added to the XKMS, SCVP and LTANS service modules which provide different levels of graphical and tabular reports on service usage in real-time. Reports can be exported in PDF format or as CSV files.
- The ADSS Server installation wizard now installs three different ADSS Server components, namely (a) the Core service, (b) the Console service and (c) selected Service modules. Each of these components uses a separate Java Virtual Machine to provide better resource management for high performance systems. Administrators can choose to install these components on just one single system or on separate physical or virtual machines.
- The ADSS Trust Manager module has been enhanced in these ways:

  (a) When deleting a CA, if the CA is used elsewhere then the references to it are shown so that an administrator can confirm or cancel the delete request;

  (b) Validation policy configurations can now allow the real-time downloading and caching of CRLs and use them to validate certificates issued by a registered CA – this is particularly relevant when checking certificates issued by Entrust CAs that feature partitioned CRLs;

  (c) When registering a new CA, the Friendly Name offered uses CA certificate common name by default to save time and mistakes - the default value can be used or changed as required;

  (d) When adding CRL resource addresses for a CA, a certificate it has issued can be identified so that all the CDP addresses are automatically read and added to the CRL resource list - this saves operator time and prevents typing mistakes;

  (e) A hierarchal view of registered CA certificates is now provided that shows chained certificates in a tree structure. The old classic view is still available if required.
- When deleting a key within Key Manager, if the key is used anywhere within the ADSS Server, the references to it are shown so that an administrator can confirm or cancel the delete request.
- CRL Monitor now allows the administrator to manually update a CRL without first turning off CRL polling within Trust Manager – this saves operator time when configuring a system.
- Wild card search is now available in various ADSS Server modules.

ADSS Server v4.2.9 (Patch release) — February 2011

- Resolved an issue relating to external Time Stamping Authorities with a space in their DName.

ADSS Server v4.2.8 (Patch release) — January 2011

- Support for ECDSA has been added to meet FIPS201 requirements.
- HMAC computation has been enhanced to handle network HSM disconnections.

ADSS Server v4.2.7 (Patch release) — December 2010

- The Key Manager HSM connection test has been enhanced.
- The System Log Viewer has been enhanced. It now shows a Log ID column in the Operational Logs and an issue with importing archived logs has been fixed.
- XAdES/CAdES plug test enhancements have been integrated.

ADSS Server v4.2.6 (Patch release) — November 2010

- Key Manager key importing has been enhanced.

ADSS Server v4.2.5 (Patch release) — October 2010

- Resolved a CRL Monitor issue associated with CRL 'certificateHold' entries that have no 'holdInstructionCode'.

ADSS Server v4.2.4 (Patch release) — October 2010

- Resolved a CRL Monitor issue with handling delta CRLs.

- Resolved a Verification, XKMS and SCVP services PKIX validation issue.
- Improved the way Key Manager displays certificate templates and imports PFX/PKCS#12 files.

ADSS Server v4.2.3 (Patch release) September 2010

- The ADSS Verification Service has been extended to support an additional OASIS DSS VerifyInfo attribute “Id”.
- Resolved an issue with the loading of historic CRLs in ADSS Verification Service.

ADSS Server v4.2.2 (Patch release) September 2010

- Resolved an issue in Verification service profile handling.
- Resolved an issue with CRL Monitor email alerting when polling for multiple CRL addresses.
- Resolved an issue with headless installation on non-Windows platforms.

ADSS Server v4.2.1 (Patch release) August 2010

- The ADSS SCVP Service has been extended to meet the GSA FIPS 201 test case requirements.
- The PKIX implementation has been extended in the XKMS, SCVP and signature verification services to meet more of the PKITS test cases.

ADSS Server v4.2 July 2010

- The ADSS Signing Service now includes support for signed attributes in CAdES and XAdES signatures as an option during OASIS DSS signing operations. Signing profiles now allow a signature grace period to be configured which defines how long the ADSS Server should wait after the signing time (shown in the timestamp or otherwise the signer's local system time) before converting the basic signature to an advanced ETSI AdES signature.
- The ADSS Verification Service has been extended to support additional DSS-X verification reports, such as returning authenticated and unauthenticated attributes and the verification of the full chain for CRLs and OCSP responder certificates. In addition the Verification Service profiles have been extended to support signature grace periods. These define how long the ADSS Server should wait after the signing time (shown in the timestamp or otherwise the signer's local system time) before verifying a signature. PEPPOL optional inputs are now supported as is the configuration of a peer XKMS server to determine revocation information for certificates whose issuer is not locally trusted on ADSS Server.
- The ADSS XKMS Service has been extended to support PEPPOL extensions. XKMS Service profiles have been introduced to allow greater granularity of the configuration options in such areas as Trust Anchors and certificate validation options. The transaction logging has also been enhanced for better presentation of the certificate validation process information.
- The ADSS SCVP Service has been extended to support Delegated Path Validation (DPV) with optional validation policy attributes in the response & support for multiple certificates in a request.
- The ADSS Verification, XKMS and SCVP services now support these features:

  (a) PKIX algorithm based validation of the certificate chains;

  (b) Transaction logging has been enhanced to also store the validation profile configuration at the time of verification to allow a later audit review of the ADSS Server decisions.
- The ADSS OCSP Service has a new feature to allow high speed OCSP response processing by optionally not storing the OCSP transactions and caching the latest CRL in memory.
- The number of internal ADSS Server “local CAs” has been extended. A new ADSS Server “Manage CAs” module has been created to allow multiple Root and issuer CAs to be configured if required. Configuration for all local and external CAs has been moved to “Manage CAs”.
- A new alerting system has been introduced to display alerts on the ADSS Server home page for various events such as license expiry, certificate expiry (includes CAs, clients and end user certificates), unused service profiles and uncertified keys within the Key Manager.

- The ADSS Access Control module has been enhanced to allow greater control over operator roles. Each service module and its sub-modules can be controlled whether to allow Add, Delete, or Modify operations and enabling dual control is now possible at a sub-module level.
- All ADSS Server services can now be configured to retry connections with external OCSP, TSA and CRL addresses when there is a connection failure.
- The ADSS Server Global Settings module has been enhanced to support client authentication when communicating with a TSA Server running over SSL with client authentication.

ADSS Server v4.1.4 (Patch release) June 2010

- Resolved an issue with SNMP alerting to include ADSS Server IP address.

ADSS Server v4.1.3 (Patch release) June 2010

- Resolved an issue with handling Unicode characters within the signature appearance designer.
- Resolved an issue with repeated optional output elements within DSS verification response.

ADSS Server v4.1.2 (Patch release) May 2010

- Enhanced the proxy handler to support NTLM authentication.
- Enhanced the PDF signature appearance designer to allow signature labels to be modified.
- Resolved an issue with handling remote file paths within LTANS service request messages.

ADSS Server v4.1.1 (Patch release) May 2010

- Fixed an issue with handling Operator CA certificates that contain a quotation character.
- Fixed an issue related to terminating the ADSS Server process when stopping on UNIX platforms.
- Fixed an issue with creating signed and timestamped Verification Service response messages.

ADSS Server v4.1 April 2010

- The ADSS Signing Service has been extended to support the enhancement of basic signatures to more advanced ETSI AdES formats as an option during OASIS DSS signing operations. In addition signature appearance attributes are now supported in the signing request as defined in the OASIS DSS-X Visible Signatures profile. Signing profiles now allow even greater configuration flexibility including the option to select alternate signing keys/certificates – this is valuable when load balanced servers need to sign using a key/certificate held within their own local PCI HSM where cloning of HSM keys and certificates is not allowed by the trust scheme, e.g. Adobe CDS Certificates.
- The ADSS Verification Service has been extended to support the enhancement of basic signatures to more advanced ETSI AdES formats as an option during OASIS DSS verification operations. OASIS DSS-X Verification Reports are supported and PEPPOL trust ratings are now available to determine signature and certificate quality. The Verification Service profiles have been extended to allow greater granularity of the configuration options in such areas as Trust Anchors, signature formats and certificate validation options. CRLs can now be optionally retrieved in real-time from the CDP contained in the target certificate – useful for partial CRLs. Finally the transaction logging has been enhanced for better presentation of the signature verification and certificate validation process information.
- The ADSS TSA Services has been extended to support RipeMD160 and SHA 224 hash algorithms. A new option is provided to use the HSM internal time clock when generating timestamp tokens provided this is supported by the target hardware.
- The ADSS LTANS Service has been extended to include a range of new features such as:
  (a) supporting application supplied meta data attributes within the generated evidence record;
  (b) searching meta data attributes to select evidence records;
  (c) return XMLERS data back if requested within export transactions;
  (d) verify archived evidence records before they are returned in export transactions;
  (e) able to select whether to store the original data within the archive, file system or to post to a configured URL and allowing the option to only store the evidence record and not the data;
  (f) archive profiles can configure how to verify signed data objects before they are archived;

(g) archive profiles can control the deletion policy for archived information;
(h) Support is provided to read and write large data objects via network paths.

- A new ADSS SCVP Service is now available as a licensed option. This follows the recently ratified RFC 5055 Server-based Certificate Validation Protocol standard. Delegated Path Validation (DPV) has been implemented in this release.
- The ADSS OCSP Service has been enhanced to support real-time revocation information for the local ADSS Server CA and support additional hash algorithms.
- The ADSS CRL Monitor service has been enhanced to be able to optionally monitor and check all CRL resources for a defined CA. Alerts can be sent if any of the CRL resources are seen to have trust issues within them. Delta CRLs are now also supported.
- Within all ADSS Server services the transactions log viewer screens have been enhanced to allow operators to select which columns they wish to show on the screen. Extended character set certificates and CRLs can now be used within ADSS Server. SNMP (Simple Network Management Protocol) based alerts are also now available.

ADSS Server v4.0.4 (Patch release) — March 2010

- Added msvcr71.dll redistributable to avoid ADSS Server Windows service startup problems. This avoids operators having to copy this DLL manually.

ADSS Server v4.0.3 (Patch release) — March 2010

- PKCS#11 enhancements have been made to better handle existing keys and certificates.
- Certificate templates now use an updated country list.
- Oracle 11g has been added to the list of supported databases.
- The ADSS LTANS Service has been enhanced to better handle the evidence renewal process
- Fixed a bug relating to external Time stamping Authorities with a space in their DName.

ADSS Server v4.0.2 (Patch release) — February 2010

- Enhanced the HMAC feature to work with a broader range of HSMs.
- Enhanced the policy controls for CRL based validation in the signature verification service.
- The Certification Service can now use the full PKCS#10 subject DN attributes.
- CRL handling within the Trust Manager and the CRL Monitor service has been enhanced.
- CRL Monitor now supports digest authentication when downloading CRLs for configured CAs.
- Stale connections to a MySQL database are now automatically recovered.

ADSS Server v4.0.1 (Patch release) — January 2010

- The ADSS Server certificate viewer now supports Qualified Certificate statement extension details.
- Navigation on the ADSS Server Global Settings > Certificate Templates page has been enhanced.
- Indirect CRLs resources can now be successfully tested from within the ADSS Trust Manager when registering a CA.
- The optional sample test data that can be used at installation time has been enhanced.

ADSS Server v4.0 — November 2009

- Added the following features as part of the CEN CWA 14167-1 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements) compliancy audit:

  (a) Check the expiry of certificate before use in any ADSS service (e.g. Signing, Verification, Certification, TSA, OCSP etc.);

(b) Perform revocation checking for back-end SSL/TLS server authentication certificates, ADSS infrastructure certificates and back-end TSA certificates;

(c) Ability to issue emergency CRLs at the time of receiving a revocation request within ADSS Certification Service;

(d) Support for IETF CMC protocol for processing certificate generation and certificate revocation requests from CMC-compliant clients, e.g. RA systems like AET BlueX. CMC over SSL/TLS is also supported for client authentication;

(e) Ability to terminate the SSL session upon log out or session timeout; in both the cases operator needs to re-launch the ADSS Server console in a new browser instance in order to re-login to ADSS Server;

(f) Support the generation of the ADSS Server Tomcat SSL Server Authentication key inside PKCS#11 devices e.g. HSM;

(g) Support the generation of system integrity checking HMAC keys in PKCS#11 devices e.g. HSM, Also included the ability to update the HMAC key;

(h) Dual control facility is extended within Approval Manager to also cover generation/import of keys in Key Manager and import of configurations in the Global Settings module;

(i) Provides a built-in certificate viewer capable of showing the certificate's fingerprint and the related fingerprint algorithm;

(j) Support for ETSI Qualified Certificate profile (TS 101 862) within the ADSS Certification Service module. A built-in certificate profile template is added for this purpose;

(k) Ability for administrators to enable Tomcat's SSL debug logging to record login failures attempts performed by ADSS operators.

- The Certification Service module now supports manual certification by importing an external PKCS#10/CSR (certificate signing request) and issue certificate against the imported PKCS#10.
- The Certification Service module now supports creation of new certificate templates in addition to the default ones.
- ADSS Server can now be installed in headless mode i.e. without a GUI-based wizard. This option is provided to help administrators to remotely install ADSS Server on non-Windows machines.

*** End of document ***