

# ADSS Server v4.2.4 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.

<b>ADSS Server v4.2.4 (Patch release)</b>	<b>October 2010</b>
---	---------------------

- 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.

<b>ADSS Server v4.2.3 (Patch release)</b>	<b>September 2010</b>
---	-----------------------

- 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.

<b>ADSS Server v4.2.2 (Patch release)</b>	<b>September 2010</b>
---	-----------------------

- 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.

<b>ADSS Server v4.2.1 (Patch release)</b>	<b>August 2010</b>
---	--------------------

- 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.

<b>ADSS Server v4.2</b>	<b>July 2010</b>
-------------------------	------------------

- 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.

## ADSS Server Release Notes

---

- 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.

<b>ADSS Server v4.1.4 (Patch release)</b>	<b>June 2010</b>
---	------------------

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

<b>ADSS Server v4.1.3 (Patch release)</b>	<b>June 2010</b>
---	------------------

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

<b>ADSS Server v4.1.2 (Patch release)</b>	<b>May 2010</b>
---	-----------------

- 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.

<b>ADSS Server v4.1.1 (Patch release)</b>	<b>May 2010</b>
---	-----------------

- 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.

<b>ADSS Server v4.1</b>	<b>April 2010</b>
-------------------------	-------------------

- 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;

## ADSS Server Release Notes

---

- (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.

<b>ADSS Server v4.0.4 (Patch release)</b>	<b>March 2010</b>
---	-------------------

- Added msucr71.dll redistributable to avoid ADSS Server Windows service startup problems. This avoids operators having to copy this DLL manually.

<b>ADSS Server v4.0.3 (Patch release)</b>	<b>March 2010</b>
---	-------------------

- 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.

<b>ADSS Server v4.0.2 (Patch release)</b>	<b>February 2010</b>
---	----------------------

- 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.

<b>ADSS Server v4.0.1 (Patch release)</b>	<b>January 2010</b>
---	---------------------

- 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.

<b>ADSS Server v4.0</b>	<b>November 2009</b>
-------------------------	----------------------

- 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:

## ADSS Server Release Notes

---

- Check the expiry of certificate before use in any ADSS service (e.g. Signing, Verification, Certification, TSA, OCSP etc.)
- Perform revocation checking for back-end SSL/TLS server authentication certificates, ADSS infrastructure certificates and back-end TSA certificates.
- Ability to issue emergency CRLs at the time of receiving a revocation request within ADSS Certification Service.
- 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.
- 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.
- Support the generation of the ADSS Server Tomcat SSL Server Authentication key inside PKCS#11 devices e.g. HSM.
- 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.
- 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.
- Provides a built-in certificate viewer capable of showing the certificate's fingerprint and the related fingerprint algorithm.
- 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.
- 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.

<b>ADSS Server v3.8.1 (Patch release)</b>	<b>November 2009</b>
---	----------------------

- Improved auto-upgrade facility when upgrading from previous releases of the ADSS Server.
- Resolved an issue related to HMAC verification.

<b>ADSS Server v3.8</b>	<b>October 2009</b>
-------------------------	---------------------

- The Signing Service now supports CAdES-C, XAdES-C and XAdES-X type2 signature formats.
- The Signing Service can now accept basic signatures and enhance them by embedding timestamp and certificate status information using the relevant PDF, CAdES and XAdES profiles.
- The Signing Service now supports the production of German SigG standard compliant signatures using RipeMD160 hash and RSA 1024 keys in conjunction with services from www.SignTrust.de.
- ADSS GoSign Applet now supports local hashing. GoSign Professional is now available and provides licensed options for PDF viewing, timestamped and long-term signature support. GoSign Applet functionality is now controlled by use of a license.xml file.
- The Certification Service now supports roaming credentials. These credentials generated by ADSS GoSign Applet and are stored within a secure container on the ADSS Server. They are delivered to users needing to sign a document within the new ADSS GoSign Professional applet.
- The XKMS Service module can now return certificate status information for the full certificate chain of the target certificate, OCSP responder and the CRL issuer certificates within a single request/response call.
- A controlled option is available to support the decryption of XML documents using an OASIS DSS-X Encryption Profile compliant Decryption Service module. The encryption of the target data within an XML structure is possible using a special licensed option of the ADSS GoSign Professional Applet - ask for further details.

## ADSS Server Release Notes

---

ADSS Server v3.7.3 (Patch release)	October 2009
------------------------------------	--------------

- Resolved an issue in Certification Service module when configuring local CA.

ADSS Server v3.7.2 (Patch release)	September 2009
------------------------------------	----------------

- Resolved an issue in Trust Manager to allow the use of validation policy OCSP then NONE.

ADSS Server v3.7.1 (Patch release)	August 2009
------------------------------------	-------------

- Resolved an issue in the OCSP Service module when handling suspended certificates.

<b>ADSS Server v3.7</b>	<b>August 2009</b>
-------------------------	--------------------

- ADSS Server can now accept and process one or more hash values within ADSS Signing Service using the OASIS DSS protocol. Thus client applications do not need to send whole PDF documents for signing. This increases performance substantially for large PDF documents. To support this feature the ADSS Client SDK has been updated to provide local hashing and signature object embedding for PDF documents.
- ADSS Signing Service now supports the use of authorisation profiles. These require one or more end users to sign an authorisation control file requesting that one or more documents be signed with a server-held signing key. This is useful in high-trust workflows where important documents need to be signed by a Qualified Certificate or CDS Certificate. An audit trail of approvers is created, checked and available as audit or compliance evidence. An M of N scheme is implemented to ensure business workflow flexibility.
- Updated Tomcat & JRE versions. ADSS Server now uses Tomcat 6.0.18 and JRE 1.6.0\_13.
- The list of supported hash algorithms has been extended to include RipeMD128 and RipeMD160. These are needed to work with German SigG compliant signature service providers.
- The TSA Service has markedly better performance as a result of lower-overhead logging.
- A real-time certificate status checking feature has been added to ADSS Server. This can be configured for use with all validation i.e. OCSP, XKMS, Signing and Verification services. A special utility is provided to load real-time information from the Verizon Cybertrust UniCERT CA. Real-time information from other RAs and CAs can be integrated using this ADSS Server feature.
- New CRL Monitor alert events (using both email and SMS messages) have been added to cover circumstances when (a) the signature of a downloaded CRL cannot be verified and (b) when a downloaded CRL is not properly structured or has an incorrect format.
- CRL Monitor can now check that a CA that over-issues CRLs (e.g. creating a new CRL every three hours that is valid for 24 hours) is in fact meeting this policy. A new alert event has been created for circumstances when a CA fails to issue a CRL based on its over-issue policy - even if there is a valid CRL for that CA already present in the ADSS database.
- The CRL Monitor can now optionally publish downloaded CRLs to a local system after they are verified. This enables local CRL access for high security and high availability environments.
- HMAC recalculation for existing database records has been made optional when upgrading the ADSS Server. These are required to handle database schema changes from an older version to a new version. The process can now be run from a separate utility allowing an upgraded ADSS Server to start without interruption and with no delays.
- Added the option to configure two logging method for transactions in each ADSS Service module, to improve performance by reducing the number of database write transactions. Each service now has a specific configuration file for low-level system settings.
- Added a configuration option to enable the use of FIPS mode for HSMs and to enable the storage of generated certificates on to a PKCS#11 device (e.g. smartcard / USB token / HSM).

ADSS Server v3.6.3 (Patch release)	June 2009
------------------------------------	-----------

- Added support to generate asymmetric key pairs and subsequent PFX files within the ADSS Certification Service without the client application having to provide the password for the PFX file in the request message. A random password is generated automatically by the ADSS Server.
- Added support for the client application to retrieve the private key file (PFX) and the associated password from the ADSS Certification Service.

<b>ADSS Server v3.6.2 (Patch release)</b>	<b>May 2009</b>
---	-----------------

- Resolved a limitation in the Key Manager to handle longer key aliases.
- Resolved an issue regarding verification of XAdES-EPES signatures.

<b>ADSS Server v3.6.1 (Patch release)</b>	<b>May 2009</b>
---	-----------------

- Resolved an issue with image scaling in PDF signature appearances. Also provided a new facility to adjust the hand-signature and company logo image sizes whilst designing the signature appearance.
- Resolved an issue concerning the use of keys/certificates existing within a PKCS#11 device, where the key alias contains special characters.

<b>ADSS Server v3.6</b>	<b>April 2009</b>
-------------------------	-------------------

- A new OASIS Digital Signature Services (DSS) standard service module has been added to extend the range of signing and verification options available and continue Ascertia's commitment to standards compliance.
- An IETF LTANS (Long-Term Archiving and Notary Service) module has been added to provide standards based secure archiving and notarising for business documents. This LTANS module supports the IETF XMLERS and LTAP specifications.
- A W3C compliant XKMS (XML Key Management Specifications) service module has been added to extend the range of options available for validating X509 digital certificates.
- The Signing service transaction logging is improved to store and display the signing requests sent over the fast HTTP protocol (e.g. requests received from AFP) – this matches what is currently provided for web-services signing requests.
- Within the Admin interface a new PDF signature appearance designer applet is provided to offer fine control over exactly where the signature field should be positioned and how the signature appearance should look.
- Added the ability to select fall-back Time Stamping Authorities in the ADSS Signing and LTAN services, in case the primary TSA becomes unavailable.
- Added support for the SHA-256 hashing algorithm when signing PDF documents.
- Within the ADSS Verification service it is now possible to verify digital signatures according to the time of signing indicated by the signer.
- ADSS services can now be run from different machines e.g. an OCSP service can be deployed on one machine to process OCSP requests and the CRL Manager service can be running separately to download and manage CRLs to share the work-load.
- Added support for exporting / importing of selected ADSS Server configurations settings from one ADSS Server instance to another.
- Transaction logging is improved in all ADSS services to show error message for the failed transactions in the relevant transactions log viewer page. Previously these errors were only available in the debug log files.
- Default sorting order of the lists in all ADSS server modules is changed to show the most recent record at the top.
- Upon configuring the local timestamp authority (TSA), the relevant TSA certificate is automatically registered in the Trust Manager with the purpose of trusting timestamps.
- Provided ability to mark profiles (e.g. signing profiles) as active / inactive in all ADSS services.
- Provided ability to make requests over SSL with client authentication to the back-end OCSP responders and time stamp authorities.
- Added support for multiple hashing algorithms to be used for OCSP response signing.
- Restricted the ability to start ADSS services until at least the basic configurations are made e.g. ADSS verification will start only when at least one active verification profile is present.
- Added support to generate and store key pairs on smart cards and USB tokens and also save associated certificates directly on the smart card and USB tokens (rather than the database).
- Various improvements to the ADSS console GUI.

### ADSS Server v3.5.5 (Patch release)

April 2009

- Resolved a bug within TSA module when the service is stopped.

### ADSS Server v3.5.4 (Patch release)

February 2009

ADSS Server Release 3.5.4 is a unified patch release for all platforms; it merges updates for 32-bit and 64-bit Windows, Solaris and Linux. It includes:

- Enhance HSM signing service performance.
- Resolves an issue with MySQL databases requiring service restarts after Key Manager and TSA service changes.
- Resolves an issue in the setup to accept non-default database server ports.
- Resolves an issue in the display of signature appearance attributes (e.g. signing reason, location and date).

### ADSS Server v3.5.1 (Patch release)

January 2009

- Support for Linux Centos platform with support for MySQL database (embedded within Linux Centos).
- Support for Solaris sparc 10 64-bit platform.

### ADSS Server v3.5

November 2008

- Extends the ADSS verification service to check any ETSI AdES Explicit Policy-based Electronic Signatures (EPES) that are present. The service enables organisations to check whether the signature policy used by the signer is acceptable to them.
- Extends the message based alerting for all ADSS Services to include an SMS delivery option.
- Provides a new alert event and message (email and SMS) for situations when a master CRL Manager instance goes offline and is replaced by the next available slave instance.
- Enhancements have been made to the ADSS Server auto-archiving functionality so that records can be archived and copies kept in the database (i.e. enables archive back-ups to be made).
- An improved context-specific help facility is provided plus the ability to view online dynamic help for up-to-date information on the product.
- Extends support for HMAC integrity checking database records so that this can be checked automatically whilst being viewed by the operator.
- Extends the ADSS Certification Service to allow the issuance of OCSP responder certificates with a "NoCheck" extension.
- Extends the ADSS Certification Service CRL functionality to provide a manual CRL publishing option.
- For ease of operator use a system startup progress bar is now shown within the administration console as ADSS Service services are starting up.
- Adds an option in the ADSS OCSP Service to identify the Validation Authority using either KeyID or Distinguished Name within the OCSP response messages.
- The OCSP service can now be configured to optionally include or exclude the responder certificate chain in the OCSP response to either make chain building easier or reduce the size of the OCSP response for bandwidth-limited environments.

### ADSS Server v3.4

October 2008

- Support for multiple HSM / smart card / USB tokens has been added by using crypto profiles in Key Manager. Any existing keys and certificates on new hardware tokens introduced can be found and used. Both software and hardware keystores can be used at the same time.
- The Client Manager has been enhanced to control access rights for all ADSS Services.
- Adds support for specifying a signing certificate in the signing profile.
- It is possible to control which signing keys within the Key Manager are available to which clients.
- A new PDF signature location and appearance editor has been provided.

## ADSS Server Release Notes

---

- A new Auto File Processor client has been provided to replace the previous inbuilt watched folder signing implementation. This provides improved performance, flexibility, load-balancing and high availability capability to Watched Folder mode processing.
- An optimised HTTP protocol is supported in the signing service to improve performance.
- New support for ETSI XAdES and CAAdES EPES and ES-A format signatures.
- The Tomcat keystore password can be managed by ADSS Server.
- Extends support for certificate chain handling when signing and verifying documents and adds support for building certificate paths using intermediate CA certificates retrieved from the signature itself.
- Enables certificate revocation information to be embedded for the full chain of the signer, OCSP responder and timestamp authority certificates within long term signatures. Also supports PDF long-term signatures using Adobe Rooted CDS Certificates.
- Adds low-level IdenTrust specific certificate extension checks when signing/verifying documents.
- Adds support for defining the hashing algorithm to be used for signing when creating a new signing profile (supports SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 set of algorithms).
- Improvements are made in the debugging logs to record more clear and precise messages.
- Context specific help is provided for all ADSS Server modules to guide on using ADSS Server console for configurations.
- Enhancements have been made to archiving – auto archiving can now be performed on a frequent basis (days instead of months) and on demand archiving is supported.
- Multiple ADSS Server instances sharing the same database can be managed using the Service Manager module. The Service Manager can reload all ADSS Server configurations and restart selected ADSS Server service.
- A new default auditor role has been introduced. This role has privileges to access the transaction logs for all ADSS services plus the operational and event logs.
- Provides improved Management Reporting module for each service which can 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.
- Licensing strategy has been improved to support license expiry on specific date or after specific period from the start of use or after specific number of transactions.
- Adds ability to optionally perform revocation checking for the operator's and client's SSL authentication certificates.
- Adds support for automatically adding the CA certificates in the java keystore at the time a CA is registered or is marked active.
- Improved performance of the ADSS Server administration console when hardware crypto source is used.
- Adds ability to automatically upgrade the existing installation to the latest release of ADSS Server.

<b>ADSS Server v3.3.4 (Patch release)</b>	<b>September 2008</b>
---	-----------------------

- Resolves a CRL handling issue where an underlying API was not properly closing threads for LDAP addresses upon CRL timeout.
- Resolves a CRL Manager issue regarding redundant log messages.
- Supports interoperability between Opera browser OCSP client functionality and the ADSS Server OCSP service.

<b>ADSS Server v3.3.3 (Patch release)</b>	<b>August 2008</b>
---	--------------------

- Changes have been made to enhance the process of renewing Trust Manager CA certificates and also the processing of operator certificates.
- Supports non-standard version 2 CRLs that do not contain a CRL Number extension.
- A CRL handling issue within the CRL Manager Service has been resolved.
- A transaction logging issue has been fixed in the Verification service.
- A Trust Manager 'test connection' issue with PEM encoded CRLs has been resolved.

## ADSS Server Release Notes

---

### ADSS Server v3.3.2 (Patch release)

July 2008

- Adds support for using Safenet HSM running in FIPS 140-2 Mode.
- Provides facility for optionally embedding fonts to retain PDF/A compliancy of PDF/A-1a and PDF/A-1b documents.

### ADSS Server v3.3.1 (Patch release)

July 2008

- Adds support for importing PEM encoded CRLs.
- Provides facility for importing SSL Server Authentication certificates into the JVM key store using a SSL trust utility pre-bundled with the set-up.
- Adds support to include full certificate chain (if available) in PFX files exported from the Key Manager.
- Resolves a memory issue when archiving large number of big CRLs (e.g. several MBs).
- Resolves a CRL polling hang issue when using LDAP CRL resources.
- Resolves an issue where multiple instances of CRL Manager Service were started on the same ADSS Server instance when clicking start button multiple times.
- Resolves PFX file import issue on Windows XP platform for certificates generated by the ADSS Certification Service.
- Updates to algorithm.properties file to support a wider range of public key and hashing algorithms for computing signature quality levels in the ADSS Verification Service.
- Provides separate configurations settings for PKCS#7, CMS, CAdES, XML Dig Sig and XAdES signatures within the Signing Profiles.

### ADSS Server v3.3

March 2008

- Adds support for automated and manual authentication of database log records.
- Adds support for importing archived and expired CRLs for historic verification purposes.
- Adds Admin GUI support for Firefox browser plus enhanced Trust Manager Wizard.
- Enhances security for ADSS Server configuration data.

### ADSS Server v3.2.2

February 2008

- Resolves a memory leak issue when using an HSM.

### ADSS Server v3.2.1

January 2008

- Minor bug fixes related to verification service able to process large CRLs and fix OCSP detailed reporting.

### ADSS Server v3.2

January 2008

- Support for Solaris 10 on x86 platform with support for PostgreSQL v8.2.5 database (embedded within Solaris 10).

### ADSS Server v3.1.6

December 2007

- ADSS Server Verification service performance improvement.
- ADSS Server CRL Manager service performance improvement and adds option to immediately stop the CRL Manager service. CRLs cannot be manually imported while the polling is active for a particular CA.
- Adds a new email alert when the CRL Manager service downloads a valid CRL which already exists in the database. CRL statistics are provided for the event.
- Enhanced monitoring and re-establishment of database connection. Database monitoring debug logs provided in a newly file called hsm\_db\_monitoring.log.
- Issues related to CRL Manager service High Availability mode have been fixed.
- Support for verification of Acrobat 8 signed PDFs in ADSS Verification Service.

### ADSS Server v3.1.5

December 2007

- Support for digest authentication when downloading the CRLs for configured CAs.

### ADSS Server v3.1

October 2007

- Time Stamp Authority (TSA) Service, compliant with RFC3161, is added as a new service module.
- OCSP (Online Certificate Status Protocol) Responder Service, compliant with RFC2560, is added as a new service module.
- Adds Long Term Signature support (XAdES, CAdES and PDF) in Signing and Verification Services and updates verification schema.
- Internal CA now generates and publishes CRLs within the Certification Service.
- Enhanced email alert generation within ADSS Server.
- Support for the export and auto-archiving of transaction records in all ADSS services modules and System Log Viewer utility module.
- Support for Oracle 10g database.
- Support for SMTP user authentication.

### ADSS Server v3.0.1

June 2007

- Support for ADSS on Sun Solaris operating system with Oracle 10g database.
- Provision of ADSS Client SDK to simplify the ADSS integration process. The SDK provides both Java and .Net libraries and various samples, as well as GoSign applet developer info and demo applications.
- Optimization in signing and verification service.

### ADSS Server v3.0

April 2007

- Added Signing Service module to allow server-side signing of PDFs, XML DigSig and PKCS#7/CMS signatures on demand through Web Services.
- Added GoSign Applet support
- Added Certification Service module to allow applications to request server-side key generation and certification using either an inbuilt CA or external CA service provider.
- Renamed CA Manager to Trust Manager. This now allows registration of various different types of Trust Authorities (e.g. CAs, TSAs, OCSP responders, etc.). Separate modules for defining Validation Policies and OCSP settings are now removed and these policy settings are now configured when registering the CA.
- Changes to Access Control module to provide fine grained role based controls.
- A new Approval Manager module is provided for dual control purposes.
- Provided support for the ADSS services modules i.e. Signing, Verification, Certification and CRL Monitor to be deployed on different machines.
- Event logs contained only CRL based logs and thus it has been moved in CRL Manager Service. System log viewer shows all operations performed by operators on the system.
- Verification Web Service has been updated to support certificate validation also.
- Support for historical signature verification and certificate validation is now provided. This uses an archive of old CRLs managed by the ADSS CRL Manager Service to determine certificate status information in the past.
- Verification Service has been updated to support XML DigSig verification and also S/MIME email signatures (interoperability tested with Microsoft email solutions only).