ADSS Server - Known Issues

This document provides a high-level description of the known issues in this product release.

No.	Issue Description
ADSS Server Console Issues	
Key Manager	
1.	When using Aladdin USB tokens as the crypto source to generate key pairs, the corresponding public key certificate is not stored automatically on the token even though the option to store the certificate on the device is selected. However, the certificate is only stored within the ADSS Server database. This problem is not observed when using various other USB tokens or smart cards.
2.	When Georgian language characters are used in a key alias, it is not possible to delete such keys from the ADSS Server Key Manager module. Workaround – do not use Georgian language characters within the key and certificate aliases.
3.	Crypto Source can have multiple profiles only with same PKCS#11 Module for any Hardware CryptoSource i. e. different PKCS#11 Module cannot be used in this case.
CRL Monitor	
1.	Search functionality is not supported on the View CRLs page when using ADSS Server with a clustered database.
2.	ADSS Server will not import a non-expired CRL if it is older than a valid CRL already exist in the ADSS Server database. Note a CRL which is currently expired can still be imported even if a latest valid CRL is present in the database.
Manage CAs	
1.	An external CA address is reported as successfully tested even if only a part of the external CA address is provided (i.e. URL is provided only up to domain name e.g. http://test-ca). Ensure you provide the full path in the external CA address rather a portion of it.
ADSS Server Service Issues	
SAM Service	
1.	User can be registered with same user ID but different cases like jhon@ascertia.com & JHON@ASCERTIA.COM on PostgreSQL.
CSP Service	
1.	User can be registered with same user ID but different cases like jhon@ascertia.com & JHON@ASCERTIA.COM on PostgreSQL.
Certification Service	
1.	Renew/Rekey does not support Asynchronous request processing at Certification Service.
2.	In case of Rekey, we remove the old key-pair and generate a new one, and if certificate generation fails due to any reason, we lose the old key pair. However, the clients can resend the same request until the successful generation of the certificate.
Signing Service	
1.	XML local signing is not working when signing key algorithm is ECDSA
2.	Only one input and one output document is stored in the transaction logs even when multiple documents are signed in a single transaction and it is selected to store the documents in transactions logs.
3.	The PDF Editor is unable to show PDF documents which are password/certificate based encrypted and certified PDFs.

4.	PDF signing fails if the signature field name contains a "." (dot / full stop). Workaround – Do not include the "." (dot / full stop) character in the signature field name.
5.	In order to use eSeals functionality in the ADSS Server, the business application will be integrated with ADSS RAS Service directly. We cannot use ADSS Signing Service to perform eSeals signings using ADSS RAS/SAM.
Verification Service	
1.	Transaction detail is not saved because it contains detailed information about the certificate chain, revocation, signature verification and timestamp verification which is done on the ADSS Verification Server. Currently, there is no mechanism to share the Transaction details between the Gateway and Verification Server so on time Transaction detail view is not comprehensive information available on the Gateway.
2.	In case of Verification Gateway Mode, it is mandatory to use one to one communication interface like DSS to DSS and HTTP-to-HTTP protocol to avoid any mismatch request/response structure during information exchange.
3.	Request signing is not supported in gateway mode because on Verification Gateway need to add Profile ID and Client ID for ADSS Verification Server. If Gateway try to add this information in signed request then client generated signatures would be corrupted.
4.	Store input and output documents are not supported in the Gateway mode.
Go>Sign Service	
1.	"SHA384" and "SHA512" hash algorithms do not work for PDF/A compliant documents.
2.	When filling in PDF forms using Go>Sign Document Viewer, manually entering date/time values does not work. Workaround – Use the date/time picker control to enter date/time values.
3.	Key Generation is not supported in MAC Keychain
OCSP Service	
1.	Logs integrity check cannot be performed manually on OCSP transaction details.
2.	In OCSP Service >> Management Reporting >> Usage Report, the Show Top 20 target certificates/clients option will perform filtering based on the records present only on the first page. This issue is only observed when the ADSS Server is deployed with the Oracle 10g database.
CRL Monitor	
1.	When using High Availability configuration for the CRL Monitor, sometimes failover may not occur from primary to secondary, if the machine name for one instance is part of the machine name for other instance (e.g. ADSS and ADSS2). Workaround – The machine name for one instance should not be part of the machine name for the other instances e.g. the names ADSS1 and ADSS2 are ok as ADSS1 is not a part of the name ADSS2.
NPKD Service	
1.	ADSS NPKD Service cannot communicate with ICAO PKD over mutual TLS.
RAS Service	
1.	Signing operation will be failed, if in SAM Service, the user keys will be generated in a crypto source where key wrapping will be enabled using a Dynamic KEK.
Miscellaneous	

1.	If PSS padding scheme is configured in ADSS Server:
	• For signing with SHA512 hash algorithm, minimum key length must be 2048 else it will throw the encoding exception: Encoding error: emLen (128) shorter than hashLen + saltLen + 2!
	• Due to limitation in some of the third party libraries used by the ADSS Server, PSS signature padding is not supported yet:
	  ○ With some of the hardware tokens (Safenet, Utimaco)
	  ○ While doing client-side signing using Go>Sign Desktop as MS-CAPI doesn't support PSS padding scheme.
	• Although ADSS Server supports MS office word/excel signing and verification, but MS Office itself doesn't support PSS signature padding scheme yet. In case of MS office signing, ADSS Server will fall back to PKCS1.5 padding scheme for server-side signing even if PSS signature padding scheme is configured for signing service advanced settings under Global Settings > Advanced Settings.
	• For PKCS1 Signing profile, Compute hash at signing time option must be enabled in the advanced settings under Hash Signing Settings.

2.	If ADSS Server license does not allow exporting keys from Key Manager module then the exported configurations will not be imported on the target ADSS Server if any of the exported configurations refers a key in Key Manager module.
3.	If MSCAPI keystore is configured within the ADSS Server then the Microsoft Azure Key Vault keystore cannot be used. Workaround – Disable the MSCAPI keystore by changing the value of property ENABLE_MSCAPI_CRYPTO = FALSE on Global Settings > Advanced Settings page.
4.	PAdES LTV signatures cannot be created when documents are converted to PDF/A-1, PDF/A-2 and PDF/A-3 formats using ADSS Server.
5.	If your PKI has segmented CRLs which are being cached when discovered dynamically at the time of validation then Verification, XMKS and SCVP Services may behave inconsistently. PKITS test case "4.14.19 - Valid onlySomeReasons Test19" may get failed due to the above mentioned reason. Workaround – Disable the CRL/OCSP cache by setting the value of **ENABLE_CRL_OCSP_CACHING = FALSE** on ADSS Server console under **Global Settings > Advanced Settings > General Settings**. A restart of all services is required from Server Manager for this change to take effect.
6.	ADSS Server may behave abnormally if the database becomes unavailable while the ADSS Server service or daemon was running. In this situation, ADSS Server will automatically re-establish the connection to the database when it is available after a downtime.
7.	ADSS Server may behave abnormally if the configured HSM becomes disconnected while the ADSS Server service or daemon was running. In this situation, ADSS Server will automatically re-establish connection to the HSM when it is available again a downtime.
8.	Clicking the "Back" or "Forward" buttons of internet browser on any ADSS Server screen may result in an abnormal behaviour instead use the admin screen buttons to navigate.
9.	Occasionally exceptions are shown on different modules of the ADSS Server console when one of the database instances has failed in a clustered Oracle database environment. Workaround – re-launch the ADSS Server console. Services will continue to work correctly when such situation occurs.
10.	Occasionally an error message "Error while performing the request" is shown within ADSS Server modules. Workaround – accessing the same ADSS Server module again resolves the problem.

11.	If the database server being used by ADSS Server requires re-start for some maintenance operations then it is strongly recommended stopping ADSS Server Windows services or UNIX daemons first. This is because ADSS Server might be inserting some transactions into the database at the time it is being re-started. This may result in missing log IDs for the ADSS Server transaction logs. This issue shall be faced when using ADSS Server with Oracle or PostgreSQL databases. Note that ADSS Server will identify these missing log IDs when verifying HMAC integrity for the transaction logs.
12.	As archived logs are removed from the ADSS Server database therefore ADSS Server will not detect deletion of records which lie in the archived records range. Also, if first or last records are deleted either from the database or from the archived log files then this deletion is not detected while performing manual integrity check.
13.	Page navigation sometimes not work properly for offline help console.
14.	Remove the environmental variable JDK_HOME from host machine because tomcat on start-up first checks JDK_HOME from system and uses it instead of JDK present in ADSS Server installation directory which may result in inconsistent behaviour.
15.	When the operator takes backup of MySQL database where (lower_case_table_names=1) i.e. case insensitive and restores it to a another database where (lower_case_table_names=0) i.e. case sensitive then the restore operation will fail. Both database instances must have enabled case insensitive mode (i.e. lower_case_table_names=1).
16.	In ADSS Server v6.9, jQuery version has been updated from 1.9.1 to 3.5.1. Due to this change, only Go>Sign demos of v6.9 will work with ADSS Server v6.9. The Go>Sign demos of v6.8 and earlier versions will not work with ADSS Server v6.9.
17.	The ETSI Signatures Conformance Checker: • Does not validate EPES Signatures. • Does not support the EC/ECDSA Signatures. • Does not verify the XAdES-B-LTA signatures using XPath.
18.	The DSS Demonstration WebApp portal recognize the XAdES-E-X and XAdES-E-X-L as XAdE-C signature type as per its behaviour. However ADSS Verification Service and ETSI portal correctly identify the mentioned signatures.

*** End of document ***