OCSP Client Tool 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.

OCSP Client Tool v3.1 — April 2016

- Hash algorithm to be used while composing CertIDs is now configurable in OCSP Client Tool. Support for SHA2 algorithms is also added.

OCSP Client Tool v3.0 — October 2013

- This major release of OCSP Client Tool requires a new license file – contact your sales representative if you need a new license. The downloaded product includes a restricted evaluation-use-only license good for 10 days and/or 20 transactions.
- The detail for X.509v1 certificates can now be shown within the certificate viewer in addition to the more usual X.509v3 certificates.
- A request which does not contain a nonce can now be imported and viewed even if the policy in Advanced Settings mandates a nonce be used.
- When importing an OCSP request file, if a file name is not entered and the "Import" button was selected and error is now shown.
- Two CA certificates with the same Subject Name can now be used – this is useful for handling certificates from an old SHA1 based CA and a new SHA2 based CA.
- Ascertia Root CA 2 has been added to the default trust anchors list.
- The OCSP GET request has been updated to remove unnecessary characters.
- Trust Status issues have been fixed when using multiple CertIDs.
- When upgrading from an earlier version the logs moved to the new v3 logs directory.
- An error message is now shown if there is no OCSP address configured in the Import OCSP Request tab.

OCSP Client Tool v2.3 — December 2012

- These enhancements have been made:
  (a) An pre-defined OCSP request can now be loaded, stored and sent to the OCSP Server
  (b) The HTTP GET method is now supported as an alternative to HTTP POST

OCSP Client Tool v2.2 — December 2009

- The Trust Anchor menu is moved to the main menu bar from the Options menu.

OCSP Client Tool v2.1 — April 2009

- Minor functionality improvements, e.g. loading of last active profile rather than the default profile on starting the product and any changes to the Options menu are not automatically saved but only when selected by the operator.
- Enhanced logging.
- Minor improvements to GUI.

OCSP Client Tool v2.0 — October 2008

- OCSP Client Tool configurations can now be stored in the form of profiles which can later be reloaded thus allowing easy switching of configurations.
- The OCSP Client Tool trust anchor list is now linked with the Java keystore, this means any certificates registered, suspended or removed from the OCSP Client Tool trust anchor list will also be similarly changed in the Java keystore. There is no need to manage the Java keystore separately anymore (e.g. for managing the SSL/TLS Server authentication certificates).
- Supports more extensive certificate path building for the OCSP responder certificate (i.e. intermediate CA certificates can be retrieved either from the OCSP response itself or from the OCSP Client Tool trust anchor list)
- There are some minor changes in the GUI of the OCSP Client Tool.

OCSP Client Tool Release Notes

OCSP Client Tool v2.0	October 2008

For Sales & Solutions information:
Email: sales@ascertia.com

For Technical Product Support:
Email: support@ascertia.com