



## OCSP Crusher Tool



The OCSP Crusher Tool is a useful test tool for PKI administrators and support staff that need to test the performance and efficiency of one or more OCSP Validation Authority servers. It can be used to ensure that important Validation Authority systems are operating effectively as measured from an OCSP client perspective. OCSP Crusher Tool can be used both during the installation and configuration of an OCSP Responder as well as during upgrade processes. It is also a useful tool for capacity planning purposes.

The OCSP Crusher Tool enables stress testing of OCSP servers with a selectable batch of OCSP requests. This facility allows PKI operations managers to prove how their systems respond to varying loads. The product has been built as a batch tool that uses all the available resources of the client workstation to create multiple OCSP requests. Consequently there is no graphical administrative user interface so instead a control file is used (various files can be used for different tests) that:

- Identifies the OCSP responder system port to which the requests should be sent
- Identifies the certificate to be included in an OCSP request
- Defines the number of batches of tests to be run
- Defines the number of concurrent sessions to use (to increase the load)
- Defines the total number of requests to be sent within a single test
- Defines if an SSL session is to be used
- Defines if the requests are to be signed and if so the local certificate to use

Since this is a full RFC 2560 OCSP Client, the target OCSP responder should create a signed reply for each request that OCSP Crusher sends it. OCSP Crusher receives these OCSP responses, analyses the time taken to respond and can then produce a report of the total time taken and the average time per OCSP request.

OCSP Crusher also offer comprehensive checks on the responses, verifying verifies the OCSP signature, Nonce, CertID / SingleResponse, ThisUpdate and NextUpdate validity, Responder certificate chain validity, Responder certificate Extended Key Usage and Responder certificate trust building.

The Ascertia OCSP Crusher Tool is fully compliant with the OCSP specifications as defined in IETF RFC2560, and interoperates with any OCSP servers meeting this standard.

The OCSP Crusher Tool is written in Java and is supported on Windows 32 and 64 bit desktops and Server systems.

It can be downloaded and evaluated on request.

|                           |  |
|---------------------------|--|
| System Requirements:      | Windows XP<br>Windows 7<br>Windows 2003 Server<br>Windows 2008 Server                        |
| Interfaces and Protocols: | RFC 2560 (OCSP), SSL/TLS, PFX/PKCS#12 for OCSP request signing, X.509v1 and v3 certificates. |

Ascertia Limited  
Web: [www.ascertia.com](http://www.ascertia.com)  
Email: [info@ascertia.com](mailto:info@ascertia.com)  
Tel: +44 1256 895416 US: +1 508 283 1890  
40 Occam Road, Guildford, Surrey, GU2 7YG, UK  
© Copyright Ascertia Limited 2013. All Rights Reserved, E&OE