



## A Quick Guide for using OCSP Crusher

This document aims to provide a quick *'do this and it works'* guide to using OCSP Crusher.

### OCSP Crusher Overview:

The performance of an OCSP server is a key factor since it offers a real-time online service. It is important to assess how well your OCSP service is meeting the demands of your users.

Ascertia OCSP Crusher is a sophisticated tool for PKI administrators, allowing them to test the performance and efficiency of their OCSP servers. Each OCSP server can be stress tested with a selectable number of OCSP requests running in a single or concurrent sessions. This allows PKI operation managers to prove how their systems are capable of responding to varying load conditions.

### Key Features:

Since this is an RFC 2560 OCSP Client, the target OCSP responder creates a signed reply for each request that OCSP Crusher sends it. OCSP Crusher receives these OCSP responses, analyses the time taken to respond and then produces a report of the total time taken and the average time per OCSP request. OCSP requests can optionally be signed to prove requester's identification. Following sections guide how to configure and use OCSP Crusher.

### System Requirements:

Windows 2003 Server + SP1 or Windows XP

### Quick Installation and Configuration Steps:

OCSP Crusher can be quickly configured for use following these steps:

1. Extract/unzip the setup of Ocs Crusher-v2.0-Full-10Apr2009.zip
2. Open OCSP Crusher <installation directory>\conf\ocsp\_crusher\_profile1.conf
3. Write an address of a specific OCSP Responder
4. Define the HTTP Method (POST/GET) to use in Communication
5. Identify the number of batches and concurrent requests
6. Specify the Target and Issuer certificate
7. Verify the OCSP response signature, when selected the signature on the OCSP response message itself is verified.
8. Verify the OCSP responder chain, when selected a valid certificate chain is constructed using the certificates provided in the OCSP response message. The expiry status of each certificate is checked as well as its signature value using the public key from the next certificate in the chain. Note – if responder chain verification results in failure responder trust building with the trust anchor certificate would also fail if configured below in step-9.
9. Specify the Trust Anchor certificate to act as the final trust point for the OCSP Responder certificate. This can be either the responder certificate itself or any certificate in the OCSP responder chain (e.g. Root CA or an intermediate CA). The OCSP responder certificate path is built up to the specified trusted anchor. Note in case a Root CA is configured as the trust anchor, ensure any intermediate CA certificate(s) are provided in the OCSP response in order for path building to succeed.
10. Configure whether to ensure correct Cert ID is present in response
11. Set a specific value for clock tolerance and also configure which time checks to perform, e.g. whether OCSP Crusher should check that the Produced At and This Update are before the current time and the value for Next Update is after the current time.
12. Specify whether to add nonce in the request and whether to add Service Locator extension in the request

13. Set a Timeout value and configure any proxy settings (if applicable)
14. Set an expected result in the profile which will be matched with the received one
15. Mention the path for the log files
16. Configure whether to run each batch automatically upon completion of previous batch or after some input from the user

### The OCSP Crusher is now installed and ready to use

#### Running OCSP Crusher:

Run OCSP Crusher from following location: <installation\_directory>\Ocs Crusher-v2.0-Full-10Apr2009\bin\ocsp\_crusher\_profile1.bat in order to stress test the OCSP Server.

#### Configuring multiple profile(s):

Multiple OCSP Crusher profiles can be configured, each testing a different OCSP responder or with different set of configurations.

Following are steps to configure more than one profile in OCSP Crusher:

1. Create a copy of “ocsp\_crusher\_profile1.conf” file from the location:
2. <installation\_directory>\Ocs Crusher-v2.0-Full-10Apr2009\profiles\
3. Rename the file and configure it as required
4. Create a copy of “ocsp\_crusher\_profile1.bat” file from the location:
5. <installation\_directory>\Ocs Crusher-v2.0-Full-10Apr2009\bin\
6. Rename the BAT file as of the newly created profile
7. Open the BAT file in Notepad or WordPad and edit the profile name with the newly created one

#### Trusting SSL/TLS Server Authentication Certificate(s):

If the OCSP responder communicates over an SSL/TLS channel, follow these instructions to trust the responder’s SSL/TLS certificate in the OCSP Crusher’s JVM key store:

1. Go to the location: “<OCSP Crusher directory>/ssl” and execute the “ssl\_trust\_manager.bat” file
2. SSL Trust Manager utility will be launched, click on Add Certificate button
3. Select the relevant SSL Server Authentication certificate for your OCSP responder and click on Trust Certificate button
4. The newly added SSL Server Authentication certificate will be shown among the trusted certificates, click on the exit button to close the SSL Trust Manager utility.

#### Product Notes

1. This is an evaluation version of OCSP Crusher
2. It allows up to 100 Transactions and/or validity period up to 30 Days followed by 10 grace days which ever reaches first. The Batch Count is limited to 3. The Concurrent Request is limited to 20.
3. Ascertia can provide free email based support, Skype and MSN chat, web-based training and even phone based assistance and other additional services for OCSP Crusher as required.

#### Contact Details

**For Commercial Sales:** Rod Crook on +44 (0) 1256 895416, [rod.crook@ascertia.com](mailto:rod.crook@ascertia.com)

**For Support:** email [support@ascertia.com](mailto:support@ascertia.com)