

# Certification Path Validation Test Tool — OCSP Test Results

# Document history

Version	Date	Editor	Description
1.0	31. 10. 2018	FS, EK	Created.
1.1		FS	Added KMail Test Report

## Authors

Dr. Evangelos Karatsiolis  
MTG AG  
Dolivostraße 11  
64293 Darmstadt

**MTG**

Dr. Falko Strenzke  
cryptosource GmbH  
Pallaswiesenstraße 182  
64293 Darmstadt



# Table of Contents

	Document history.....	2
1	Introduction.....	5
2	Test of Firefox Browser.....	6
2.1	OCSP-related Configuration Options in Firefox.....	6
2.2	Test Configurations.....	6
2.2.1	Tests with the First Configuration.....	6
2.2.2	Tests with the Second Configuration.....	7
2.2.3	Tests with the Third Configuration.....	7
2.2.4	Tests with the Fourth Configuration.....	7
2.3	Test Results.....	7
2.4	Discussion of the Test Results.....	13
2.4.1	Tests with the First Configuration: OCSP Stapling with the Default Configuration.....	14
2.4.2	Tests with the second Configuration: OCSP Requests with the Default Configuration.....	14
2.4.3	Tests with the third Configuration: OCSP Requests with Strict Configuration.....	15
2.4.4	Test with the fourth configuration: OCSP Responder is Unavailable.....	15
	Reference Documentation.....	16

## Figures

Figure 1: The GUI options for certificate validation in Firefox.....	6
Figure 2: OCSP-related options in Firefox' expert configuration.....	6

## Tables

Table 1: OCSP test results for the Firefox browser.....	13
---	----

# 1 Introduction

The Certification Path Validation Test Tool (CPT) [CPT-UD] version 1.1 and its associated TLS Test Tool [CPT-TE] have been enhanced with functionality for the Online Certificate Status Protocol (OCSP). Furthermore, the test suite shipped with the CPT has been extended by 20 tests targeting the processing of OCSP responses. The server certificates defined in those test cases feature an Authority Information Access (AIA) certificate extension which points to an OCSP responder URI, with the exception of those test cases where this property is deliberately violated.

These new OCSP tests have been applied to the following test subjects:

- Firefox 62.0.3 (64-bit)
- OpenSSL 1.1.0g
- KMail 5.8.3 (tested in Kubuntu 18.10)

The Firefox browser is tested using the TLS Test Tool together with the browser test web framework that are both part of the CPT extensions [CTP-TE]. The testing procedure and result regarding the Firefox Browser are presented in Section 2. For OpenSSL, the tests are performed on the OpenSSL command line application that supports OCSP queries. The concrete test setup and the test results for OpenSSL are described in Section Fehler: Referenz nicht gefunden. The tests of KMail using the S/MIME e-mail files generated by the CPT are documented in Section Fehler: Referenz nicht gefunden.

## 2 Test of Firefox Browser

In the following, the test setup and the test results for the Firefox Browser are presented.

### 2.1 OCSP-related Configuration Options in Firefox

Firefox offers the following configuration options with respect to OCSP-based determination of the revocation status of a certificate. In the GUI, when selecting “Preferences” from the main menu and afterwards “Privacy & Security”, at the very bottom of the displayed configuration page, a checkbox for querying of an OCSP responder can be set, as shown in Figure 1. By default, this checkbox is enabled.

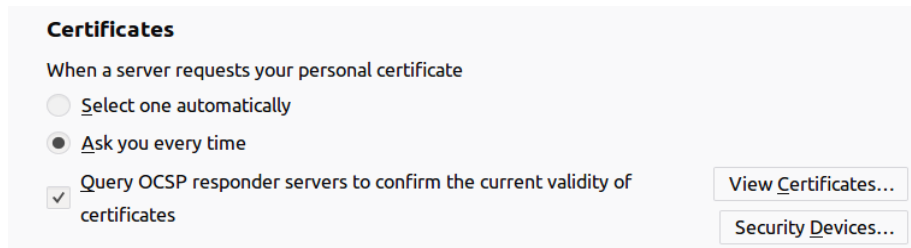


Figure 1: The GUI options for certificate validation in Firefox

The tests were executed with the checkbox enabled.

Furthermore, when accessing the advanced configuration options of Firefox by entering “about:config” in the address bar, and then restricting the displayed rows by entering the string “ocsp” in the “Search” field, the OCSP-related options as shown in Figure 2 are displayed.

Preference Name	Status	Type	Value
security.OCSF.enabled	default	integer	1
security.OCSF.require	default	boolean	false
security.OCSF.timeoutMilliseconds.hard	default	integer	10000
security.OCSF.timeoutMilliseconds.soft	default	integer	2000
security.ssl.enable_ocsp_must_staple	default	boolean	true
security.ssl.enable_ocsp_stapling	default	boolean	true
services.sync.prefs.sync.security.OCSF.enabled	default	boolean	true
services.sync.prefs.sync.security.OCSF.require	default	boolean	true

Figure 2: OCSP-related options in Firefox' expert configuration

From these variables, only the second from the top, namely “security.OCSF.require”, was varied in the tests. A Firefox configuration where this property is set to “true” is also referred to as “strict configuration” in the following.

### 2.2 Test Configurations

The Firefox browser supports determination of the certificate status based on OCSP requests [RFC 6960] as well as using the Certificate Status Request TLS extension [RFC 6066], colloquially referred to as “OCSP stapling”.

The OCSP tests of the default test suite of CPT were executed against the Firefox web browser in four different configurations of the TLS Test Tool and Firefox. All tests were executed using the test framework for web browsers that is part of the CPT extensions [CPT-TE].

#### 2.2.1 Tests with the First Configuration

The first test configuration is characterized as follows:

- Firefox is used in the default configuration,
- OCSP Stapling is activated in the TLS Test Tool (“do\_use\_ocsp\_stapling=True” in config.py).

## 2.2.2 Tests with the Second Configuration

The second test configuration is as follows:

- Firefox is again used in the default configuration,
- OCSP Stapling is disabled in the TLS Test Tool (“do\_use\_ocsp\_stapling=False” in config.py),
- and the HTTP OCSP server of the CPT is activated.

## 2.2.3 Tests with the Third Configuration

The third configuration that was tested is

- Firefox is used in a custom configuration, namely, in contrast to the default configuration, the property “security.OCSP.require” under “about:config” is set to “true” (“strict configuration”),
- OCSP Stapling is disabled in the TLS Test Tool (“do\_use\_ocsp\_stapling=False” in config.py),
- and the HTTP OCSP server of the CPT is activated.

## 2.2.4 Tests with the Fourth Configuration

For a fourth configuration, one specific test case was executed to determine the behaviour of Firefox when neither OCSP stapling nor an OCSP responder is available. This configuration is equal to the third configuration, with the only difference that the HTTP OCSP server of the CPT is not running.

Test case CERT\_PATH\_OCSP\_12 tests the behaviour of an application when a valid delegated OCSP-signer certificate is used to sign the OCSP response indicating that the certificate is “good”. Specifically, this positive test case was carried out in order to determine how Firefox behaves when the URL of OCSP server as indicated in the AIA extension of the server certificate is not available.

## 2.3 Test Results

Table 1 shows the OCSP test results for the Firefox browser with the first three configurations. Those columns the labels of which indicate “(1st Conf., Stapling)” refer to the first configuration.

The test results for the second configuration are given in the column “Test Result (2nd Conf., OCSP Request)”. For these test results, the column indicating the alerts sent is omitted. This is possible without any loss of information since the test results for the second configuration differ from that of the first configuration only in a number of tests where in the second configuration invalid certificates are accepted as valid. Accordingly, for non of those tests an alert is recorded. For the other tests, the results of which coincide with those for the first configuration, the alerts sent by the test subject are already documented for the first configuration.

The test results of the third configuration completely coincide with those of the first configuration and are thus not explicitly contained in the table.

The test results for the fourth configuration is as follows: The test result for CERT\_PATH\_OCSP\_12 is that Firefox denies the connection in this case and sends a bad\_certificate alert, and thus behaves correctly given that the OCSP URI specified in the server certificate is not available.

<b>Test</b>	<b>Test Result (1st Conf., Stapling)</b>	<b>Expected Result</b>	<b>Actual Result (1st Conf., Stapling)</b>	<b>TLS Alert (1st Conf., Stapling)</b>	<b>Test Result (2nd Conf., OCSP Request)</b>	<b>Test Description</b>
CERT_PATH_OCSP_01	PASS	VALID	VALID		PASS	Checks whether the application correctly processes an OCSP response indicating that the certificate status is “good”.
CERT_PATH_OCSP_02	PASS	INVALID	INVALID	unknown_ca	PASS	Checks the behaviour of the application when the OCSP response indicates the certificate status “unknown”. This path is invalid because revocation information for a certificate is not available.
CERT_PATH_OCSP_03	PASS	INVALID	INVALID	unknown_ca	PASS	Checks the behaviour of the application when the target certificate is indicated as revoked in an OCSP response. This path is invalid because the target certificate is revoked.
CERT_PATH_OCSP_04	ERROR	INVALID	VALID	unknown_ca	ERROR	Checks the behaviour of the application when an intermediate certificate is indicated as revoked in an OCSP response. This path is invalid because the target certificate is revoked.
CERT_PATH_OCSP_05	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when the signature of the OCSP response is wrong. The target certificate is not contained in the OCSP response. This path is invalid because the signature of the OCSP response is wrong.

<b>Test</b>	<b>Test Result (1st Conf., Stapling)</b>	<b>Expected Result</b>	<b>Actual Result (1st Conf., Stapling)</b>	<b>TLS Alert (1st Conf., Stapling)</b>	<b>Test Result (2nd Conf., OCSP Request)</b>	<b>Test Description</b>
CERT_PATH _OCSP_06	PASS	VALID	VALID		PASS	Checks the behaviour of the application when an OCSP response contains an unknown non-critical extension. The target certificate is contained in this OCSP response with status “good”. This path is valid because it is allowed for an application to ignore unknown non-critical extensions.
CERT_PATH _OCSP_07	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when an OCSP response contains an unknown critical extension. The target certificate is contained in this OCSP response with status “good”. This path is invalid because it is not allowed for an application to ignore unknown critical extensions.
CERT_PATH _OCSP_08	PASS	INVALID	INVALID		ERROR	Checks the behaviour of the application when an OCSP response is not yet valid (now < thisUpdate). The target certificate is contained in the OCSP response with status “good”. This path is invalid because the OCSP response is not valid yet.



<b>Test</b>	<b>Test Result (1st Conf., Stapling)</b>	<b>Expected Result</b>	<b>Actual Result (1st Conf., Stapling)</b>	<b>TLS Alert (1st Conf., Stapling)</b>	<b>Test Result (2nd Conf., OCSP Request)</b>	<b>Test Description</b>
CERT_PATH_OCSP_09	PASS	INVALID	INVALID	bad_certificate	PASS	Checks the behaviour of the application when an OCSP response has expired (now > nextUpdate). The target certificate is contained in the OCSP with status “good”. This path is invalid because the OCSP response has expired.
CERT_PATH_OCSP_10	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when the OCSP response's signature can be verified by a certificate whose certification path is invalid. Specifically, the OCSP signer certificate is a delegated certificate signed by the CA but does not feature the mandatory extended key usage value to be considered an authorized signer. This path is invalid because revocation information for the certificate is not available.
CERT_PATH_OCSP_11	ERROR	INVALID	VALID		ERROR	Checks the behaviour of the application when the OCSP response for an intermediate certificate indicates the revocation status as “unknown”. This path is invalid because revocation information for a CA certificate in the path is not available.

<b>Test</b>	<b>Test Result (1st Conf., Stapling)</b>	<b>Expected Result</b>	<b>Actual Result (1st Conf., Stapling)</b>	<b>TLS Alert (1st Conf., Stapling)</b>	<b>Test Result (2nd Conf., OCSP Request)</b>	<b>Test Description</b>
CERT_PATH_OCSP_12	PASS	VALID	VALID		PASS	Checks the behaviour of the application when a valid delegated OCSP-signer certificate is used to sign the OCSP response indicating that the certificate is “good”. This path is valid because the OCSP signer certificate is valid. In this test the responder ID is referenced “byKey” within the response. This is in contrast to the majority of the test cases, where the responder ID is referenced “byName”.
CERT_PATH_OCSP_13	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when it receives an exceptional response of the type “try-later”. This path is invalid because revocation information is not available to the application.
CERT_PATH_OCSP_14	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when it receives an OCSP response for the wrong certificate. This path is invalid because revocation information for the certificate is not available.

<b>Test</b>	<b>Test Result (1st Conf., Stapling)</b>	<b>Expected Result</b>	<b>Actual Result (1st Conf., Stapling)</b>	<b>TLS Alert (1st Conf., Stapling)</b>	<b>Test Result (2nd Conf., OCSP Request)</b>	<b>Test Description</b>
CERT_PATH_OCSP_15	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when an OCSP single response entry contains an unknown critical extension. The target certificate is contained in this OCSP response with status “good”. This path is invalid because it is not allowed for an application to ignore unknown critical extensions.
CERT_PATH_OCSP_16	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when a certificate does not contain the AIA extension. The target certificate is contained in this OCSP response with status “revoked”. This path is invalid because it is not allowed for an application to ignore the revocation status of a certificate in the case of an unknown responder URL.
CERT_PATH_OCSP_17	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when status response indicates an invalid responder-ID. The target certificate is contained in this OCSP response with status “good”. This path is invalid because it is not allowed for an application to accept a response from an invalid responder.

<b>Test</b>	<b>Test Result (1st Conf., Stapling)</b>	<b>Expected Result</b>	<b>Actual Result (1st Conf., Stapling)</b>	<b>TLS Alert (1st Conf., Stapling)</b>	<b>Test Result (2nd Conf., OCSP Request)</b>	<b>Test Description</b>
CERT_PATH_OCSP_18	PASS	INVALID	INVALID	unknown_ca	PASS	Checks the behaviour of the application when the target certificate is indicated as revoked in an OCSP response but has a negative serial number. This path is invalid because the target certificate is revoked, and applications are required to either reject negative serial numbers or to accept them gracefully.
CERT_PATH_OCSP_19	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks whether the application correctly processes an OCSP response with a wrong response version number. The response is indicating that the certificate status is “good”. The path is invalid since an application must reject such an invalid response.
CERT_PATH_OCSP_20	PASS	INVALID	INVALID	unknown_ca	ERROR	Checks the behaviour of the application when a delegated OCSP-signer certificate with an invalid issuer DN is used to sign the OCSP response indicating that the certificate is “good”. This path is invalid because the OCSP signer certificate is invalid.

Table 1: OCSP test results for the Firefox browser

## 2.4 Discussion of the Test Results

In this section the test results for Firefox in the four different configuration are discussed.

### 2.4.1 Tests with the First Configuration: OCSP Stapling with the Default Configuration

The first test configuration enables OCSP stapling in the TLS Test Tool and uses Firefox in the default configuration. In this case, Firefox sends the Certificate Status Request TLS Extension within its ClientHello message and the TLS Test Tool replies with a Certificate Status message containing the OCSP response for the server certificate defined for the respective test case. The test results given for this configuration in Table 1 only exhibit the following two failures:

- CERT\_PATH\_OCSP\_04
- CERT\_PATH\_OCSP\_11

Both of these tests check the behaviour of the test subject with respect to the revocation status of an intermediate CA certificate. From the test results, it can be concluded that Firefox deliberately omits the validation of the revocation status of such certificates. Note that based on the Certificate Status Request Extension [RFC 6066], it is generally only possible to indicate the revocation status of the server certificate itself, and not that of any intermediate CA certificates. Accordingly, the behaviour of Firefox can be seen as an acceptable choice for the validation of certificates in the scope of the TLS protocol.

### 2.4.2 Tests with the second Configuration: OCSP Requests with the Default Configuration

The tests with the second configuration have the purpose of checking the behaviour of Firefox in the default configuration when OCSP stapling is not supported by the TLS server it connects to. In this case, Firefox does not receive the OCSP response within the TLS handshake. Thus, it sends an OCSP request for the TLS server certificate to the HTTP OCSP server of the CPT. This server answers with the corresponding OCSP response for the current test case. As shown in Table 1, the test results for this configuration differ significantly from those for the first configuration. Namely, the following test cases, that result in “PASS” for the first configuration yield an error for the second. In all of these test cases, with the second configuration Firefox accepts erroneous OCSP responses which are correctly refused in the tests with the first configuration.

- CERT\_PATH\_OCSP\_05: invalid signature of the OCSP response
- CERT\_PATH\_OCSP\_07: unknown critical extension in the OCSP response
- CERT\_PATH\_OCSP\_08: OCSP response is not yet valid
- CERT\_PATH\_OCSP\_10: OCSP signer certificate is invalid (missing extended key usage)
- CERT\_PATH\_OCSP\_13: OCSP answers with “try-later”
- CERT\_PATH\_OCSP\_14: OCSP response for wrong certificate
- CERT\_PATH\_OCSP\_15: unknown critical extension in single OCSP response
- CERT\_PATH\_OCSP\_16: target certificate does not contain an OCSP URL
- CERT\_PATH\_OCSP\_17: OCSP response contains an invalid responder ID
- CERT\_PATH\_OCSP\_19: OCSP response carries wrong version number
- CERT\_PATH\_OCSP\_20: OCSP signer certificate is invalid (invalid issuer DN)

The test results show that the verification of the OCSP response by Firefox is basically not in place in this configuration. Only a minority of the negative test cases is processed correctly by the test subject. Furthermore, the selection of the checks that are actually applied in this configuration follows no consistent pattern. For instance, the test CERT\_PATH\_OCSP\_09, which checks for an expired response, is still “PASS”, while the test CERT\_PATH\_OCSP\_08, in which the OCSP response is not yet valid, fails.

Accordingly, the default configuration of Firefox must be considered as being vulnerable to accepting revoked certificates.

### 2.4.3 Tests with the third Configuration: OCSP Requests with Strict Configuration

The tests with the third configuration yield again the same test results as the first configuration, with the only exception of CERT\_PATH\_OCSP\_16. This test is “PASS” in the first configuration, but results in an error in the third configuration. In this test case the server certificate does not feature an AIA extensions and thus Firefox cannot fetch an OCSP response for the certificate. Whether the test result has to be considered an actual security vulnerability for this configuration cannot be unambiguously determined. Though the property “security.OCSP.require” is set to “true” in this configuration, it is not clear whether to interpret this in the sense that an OCSP response must be available whenever a certificate is checked or only when the certificate contains an AIA extension which points to a responder URI. The interpretation that lies behind the above described behaviour of Firefox is that only the latter requirement has to be met. Due to the absence of a documentation for the advanced configuration where the aforementioned property is set, a classification of the test result is not actually possible.

Obviously, as can be seen from the majority of the negative tests succeeding in this configuration in contrast to the second, the strict configuration of Firefox enables the enforcement of all checks of the OCSP response also in the case of OCSP responder queries. However, the test result for CERT\_PATH\_OCSP\_16 shows that an enforcement of an OCSP check for the server certificate is not possible if the certificate does not contain a pointer to an OCSP URI. If in such a case OCSP stapling is declined by the server, as is the case in this test configuration, the client would have to reject the server certificate in order to actually comply with a strict policy.

### 2.4.4 Test with the fourth configuration: OCSP Responder is Unavailable

The test with the fourth configuration shows that with the strict configuration, the unavailability of the OCSP responder is correctly handled by Firefox if an AIA featuring an OCSP responder URI is contained in the server certificate.

---

## Reference Documentation

- [RFC 5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF Request For Comments 5280, May 2008.
- [RFC 6066] D. Eastlake 3rd, Transport Layer Security (TLS) Extensions: Extension Definitions, January 2011
- [RFC 6960] S. Santesson, M. Meyers, R. Ankney, S. Galperin, C. Adams, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF Request For Comments 6960, June 2013.
- [CPT-UD] Federal Office for Information Security (BSI): Certification Path Validation Test Tool — User Documentation, November 2018.
- [CPT-TE] Federal Office for Information Security (BSI): CPT Tool Extensions — User Documentation, November 2018
- [RF-CPT] A. Cordel, H. Hagemeyer, E. Karatsiolis, F. Strenzke: Report on Findings for the Certification Path Validation Test Tool, Version 1.1, 16.05.2018