

# **Enabler Test Report**

## **Online Certificate Status Protocol Mobile Profile v1.0**

OMA Test Fest (September 2006)  
Version 22-Sep-2006

---

Open Mobile Alliance  
OMA-Enabler\_Test\_Report-OCSP-20-2006-09-22

This document is a work in process and is not an approved Open Mobile Alliance™ specification. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the Open Mobile Alliance specifications.

© 2006 Open Mobile Alliance Ltd. All rights reserved.

Terms and conditions of use are available from the Open Mobile Alliance™ Web site at <http://www.openmobilealliance.org/copyright.html>.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance™. The Open Mobile Alliance authorises you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services offered by you.

The Open Mobile Alliance™ assumes no responsibility for errors or omissions in this document. In no event shall the Open Mobile Alliance be liable for any special, indirect or consequential damages or any damages whatsoever arising out of or in connection with the use of this information.

This document is not an Open Mobile Alliance™ specification, is not endorsed by the Open Mobile Alliance and is informative only. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the Open Mobile Alliance specifications.

Open Mobile Alliance™ members have agreed to use reasonable endeavors to disclose in a timely manner to the Open Mobile Alliance the existence of all intellectual property rights (IPR's) essential to the present document. However, the members do not have an obligation to conduct IPR searches. The information received by the members is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at <http://www.openmobilealliance.org/ipr.html>. Essential IPR is available for license on the basis set out in the schedule to the Open Mobile Alliance Application Form.

No representations or warranties (whether express or implied) are made by the Open Mobile Alliance™ or any Open Mobile Alliance member or its affiliates regarding any of the IPR's represented on this "OMA IPR Declarations" list, including, but not limited to the accuracy, completeness, validity or relevance of the information or whether or not such rights are essential or non-essential.

This document is available online in PDF format at <http://www.openmobilealliance.org/>.

Known problems associated with this document are published at <http://www.openmobilealliance.org/>.

Comments regarding this document can be submitted to the Open Mobile Alliance™ in the manner published at <http://www.openmobilealliance.org/documents.html>

# Contents

<b>1. SCOPE .....</b>	<b>4</b>
<b>2. REFERENCES.....</b>	<b>5</b>
<b>2.1 NORMATIVE REFERENCES .....</b>	<b>5</b>
<b>2.2 INFORMATIVE REFERENCES .....</b>	<b>5</b>
<b>3. TERMINOLOGY AND CONVENTIONS .....</b>	<b>6</b>
<b>3.1 CONVENTIONS .....</b>	<b>6</b>
<b>3.2 DEFINITIONS.....</b>	<b>6</b>
<b>3.3 ABBREVIATIONS .....</b>	<b>6</b>
<b>4. SUMMARY .....</b>	<b>7</b>
<b>5. TEST DETAILS .....</b>	<b>8</b>
<b>5.1 DOCUMENTATION.....</b>	<b>8</b>
<b>5.2 TEST CASE STATISTICS .....</b>	<b>9</b>
5.2.1 Test Case Summary.....	9
5.2.2 Test Case List .....	10
5.2.3 Problem Reports .....	12
<b>6. CONFIRMATION .....</b>	<b>13</b>
<b>APPENDIX A. CHANGE HISTORY (INFORMATIVE) .....</b>	<b>14</b>

# 1. Scope

This report describes the results from the testing carried out at OMA TestFest-16 September 2006 concerning the Online Certificate Status Protocol (OCSP) Mobile Profile version 1.0.

## 2. References

### 2.1 Normative References

[OMAIOPPROC]	OMA Interoperability Policy and Process, <a href="http://www.openmobilealliance.org/">http://www.openmobilealliance.org/</a>
[DRMEICS]	Enabler Implementation Conformance Statement, OMA OCSP 1.0 Enabler Release, 05-August-2005, <a href="http://www.openmobilealliance.org/">http://www.openmobilealliance.org/</a>
[ETR]	Enabler Test Report
[ETP]	Enabler Test Plan
[ETS]	OMA-ETS-OCSP-Mobile-Profile-V1_0-20050913-A Enabler Test Specification [ETS]

### 2.2 Informative References

[OMADICT]	Dictionary for OMA Specification, OMA-Dictionary <a href="http://www.openmobilealliance.org/">http://www.openmobilealliance.org/</a>
[DRM-v2.0]	“DRM Rights Management”. Open Mobile Alliance™. OMA-DRM-DRM-v2_0. URL: <a href="http://www.openmobilealliance.com/">http://www.openmobilealliance.com/</a> .

## 3. Terminology and Conventions

### 3.1 Conventions

This is an informative document, i.e. the document does not intend to contain normative statements.

### 3.2 Definitions

<b>Client</b>	A device (or application) that initiates a request for a connection with an OCSP server
<b>Server</b>	A device (or application) that passively waits for OCSP requests from one or more clients. A server may accept or reject a connection request from a client.

### 3.3 Abbreviations

ASN.1	Abstract Syntax Notation 1, as defined in [ISO/IEC 8824-1]
CA	Certification Authority
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules, as defined in [ISO/IEC 8825-1]
HTTP	Hypertext Transfer Protocol, as defined in [WAP HTTP]
OCSP	Online Certificate Status Protocol, as defined in [RFC2560]
OMA	Open Mobile Alliance
RSA	Rivest-Shamir-Adleman public key algorithm
SHA-1	Secure Hash Algorithm
TLS	Transport Layer Security Protocol, as defined in [TLS]
WAP	Wireless Application Protocol

## 4. Summary

This report gives details of the testing carried out during the OMA TestFest-16 (September 2006) for OCSP v1.0.

The report is compiled on behalf of OMA by the OMA Trusted Zone.

The work and reporting has followed the OMA IOP processes and policies [OMAIOPPROC].

## 5. Test Details

### 5.1 Documentation

This chapter lists the details of the enabler and any documentation, tools or test suites used to prove the enabler.

<b>Date:</b>	8th to 15th September 2006
<b>Location:</b>	Düsseldorf, Germany
<b>Enabler:</b>	OCSP v1.0
<b>Process:</b>	OMA Interoperability Policy and Process [OMAIOPPROC]
<b>Type of Testing</b>	Interoperability Testing
<b>Products tested:</b>	Client-to-server
<b>Test Plan:</b>	DRM Enabler Test Plan [ETP]
<b>Test Specification:</b>	DRM Enabler Test Specification [ETS]
<b>Test Tool:</b>	None
<b>Test Code:</b>	None
<b>Type of Test event:</b>	TestFest
<b>Participants:</b>	<i>CoreMedia and two other participant companies</i>
<b>Number of Client Products:</b>	2 (A Client for OCSP Testing represents a DRM Client and DRM Server pair)
<b>Participating Technology Providers for clients:</b>	<i>Two Anonymous DRM Clients</i>
<b>Number of Server Products:</b>	2 (A Client for OCSP Testing represents a DRM Client and DRM Server pair)
<b>Participating Technology Providers for servers:</b>	<i>Coremedia plus one other DRM Server</i>
<b>Number of OCSP Responder Products:</b>	1
<b>Participating Technology Providers for OCSP Responders:</b>	<i>One Anonymous OCSP Responder</i>
<b>Number of test sessions completed:</b>	3



## 5.2 Test Case Statistics

### 5.2.1 Test Case Summary

This chapter gives an overview of the result for all test cases included in [ETS].

The following status is used in the tables below:

- **Total number of TCs:** Used in the summary to indicate how many test cases there are in total.
- **Number of passed:** Used in the summary to indicate how many of the total test cases successfully passed.
- **Number of failed:** Used in the summary to indicate how many of the total test cases failed.
- **Number of N/A:** Used in the summary to indicate how many of the total test cases have not been run due to one of the implementations not supporting the functionality required to run this test case.
- **Number of OT:** Used in the summary to indicate how many of the total test cases have not been run due to no time to run the test case.
- **Number of INC:** Used in the summary to indicate how many of the total test cases have not been run due to functionality not being tested due to an error in the implementation or other functionality that is required to run this test case.

Test Section:	Number of test sessions:	Total number of TCs:	Number of Passed:	Number of Failed:	Number of N/A:	Number of OT:	Number of INC:	Total:
Client to Server TCs	3	8	14	0	7	3	0	24
<b>Total</b>	<b>3</b>	<b>8</b>	<b>14</b>	<b>0</b>	<b>7</b>	<b>3</b>	<b>0</b>	<b>24</b>

Table 1. Test Summary Table

## 5.2.2 Test Case List

This chapter lists the statistics for all test cases included in [ETS].

The following status is used in the tables below:

- **No. of runs(R):** Used to indicate how many times the test cases have been run in total.
- **No. of passed(P):** Used to indicate how many times the test case has been run with successful result.
- **No. of failed(F):** Used to indicate how many times the test case has been run with failed result
- **No. of OT(O):** Used to indicate how many times the test case has not been run due to no time available.
- **No. of INC(I):** Used to indicate how many times the test case has not been run due to errors being found in other functionality required for running this test case.
- **PR:** Used to indicate if any PRs (Problem Reports) have been issued during testing.
- **Note:** Used to indicate the cause of Inconclusive or Fail verdicts.

### Tests for DRM Enabler TestFest Taken From OMA-ETS-OCSP-Mobile-Profile-V1\_0-20050913-A

Test Case:	Test Case Description:	R	P	F	O	I	PR:	Note:
<b>OCSP-1.0-int-01</b>	Client generates request for a valid certificate. Client receives and processes a response with a "good" status	3	3	0	0	0		
<b>OCSP-1.0-int-02</b>	Client generates request for a revoked certificate. Client receives and processes a response with a "revoked" status	3	3	0	0	0		
<b>OCSP-1.0-int-03</b>	Client generates a request for a certificate unknown by the responder. Client receives and processes a response with an "unknown" status.	3	2	0	1	0		
<b>OCSP-1.0-int-04</b>	Client generates a request for a valid certificate that contains a nonce. Client receives and processes a response with a "good" status but that does not contain a nonce.	0	0	0	0	0		
<b>OCSP-1.0-int-05</b>	Client generates a signed request for a valid certificate. Client receives and processes a response with a "good" status	3	2	0	1	0		

Test Case:	Test Case Description:	R	P	F	O	I	PR:	Note:
<b>OCSP-1.0-int-06</b>	Client generates a request for a valid certificate that contains a nonce. Client receives and processes a response with a "good" status also containing a nonce	3	2	0	1	0		
<b>OCSP-1.0-int-07</b>	Client generates an OCSPRequest message that, when base64 and url-encoded, has a length of over 255 characters. Client receives and processes a response with a "good" status.	2	2	0	0	0		
<b>OCSP-1.0-int-08</b>	Client generates request for a valid certificate and sends it via TLS. Client receives and processes a response with a "good" status.	0	0	0	0	0		

Table 2. Test Case Counts

### 5.2.3 Problem Reports

During the activities for TestFest16, the following problem reports were generated relating to the test materials and test process:

No Problem Reports were entered during Test Fest

PR Number	Affecting	Description	Test Case reference / Specification reference

Full details of all Problem Reports can be found at:

<http://www.openmobilealliance.org/OMA-Problem-Reporting-System.html>

## 6. Confirmation

This signature states that the included information is true and valid.

A handwritten signature in black ink, appearing to read "Alan R. T. E.", with a long horizontal stroke extending to the right.

---

OMA Trusted Zone

## Appendix A. Change History (Informative)

Type of Change	Date	Section	Description
Initial Version	22 <sup>nd</sup> September 2006	All	First Version from TestFest-16