



Enabler Release Definition for Online Certificate Status Protocol Mobile Profile V1.0

Candidate Version 1.0 – 27 Jan 2004

Open Mobile Alliance
OMA-ERELED-OCSP-V1_0-20040127-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

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. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes 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. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR 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>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth 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 THE “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.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2004 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE	4
2. REFERENCES	5
2.1 NORMATIVE REFERENCES	5
3. TERMINOLOGY AND CONVENTIONS	6
3.1 CONVENTIONS	6
3.2 DEFINITIONS	6
3.3 ABBREVIATIONS	6
4. INTRODUCTION	7
5. ENABLER RELEASE SPECIFICATION BASELINE	8
6. MINIMUM FUNCTIONALITY DESCRIPTION FOR OCSP V1.0 ENABLER RELEASE	9
7. CONFORMANCE REQUIREMENTS NOTATION DETAILS	10
8. ERDEF FOR OCSP V1.0 - CLIENT REQUIREMENTS	11
9. ERDEF FOR OCSP V1.0 - SERVER REQUIREMENTS	12
APPENDIX A. CHANGE HISTORY (INFORMATIVE)	13
A.1 APPROVED VERSION HISTORY	13
A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY	13

1. Scope

The scope of this document is limited to the Enabler Release Definition of Online Certificate Status Protocol (OCSP) mobile profile V1.0 according to OMA Release process and the Enabler Release specification baseline listed in section 5. OCSP defines a protocol used to determine the current status of a digital certificate in lieu of using standard Certificate Revocation Lists (CRL's). The scope of this work item is to profile OCSP in such a way to ensure it can be used efficiently by limited wireless devices and to be interoperable with OCSP responders already at market. The profile will be defined as an OMA service enabler to ensure its use with any existing and future OMA applications and/or services.

2. References

2.1 Normative References

- [IOPPROC] "OMA Interoperability Policy and Process", Open Mobile Alliance. OMA-IOP-Process-V1_1, <http://www.openmobilealliance.org/>
- [RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. [URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)
- [OCSP] "Online certificate status protocol mobile profile". Open Mobile Alliance™ OMA-WAP-OCSP-V1_0. [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [RFC 2560] "X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP," M. Myers, et al., IETF RFC 2560, June 1999. URL: <http://www.ietf.org/rfc/rfc2560.txt>
- [RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. [URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

The formal notation convention used in sections 8 and 9 to formally express the structure and internal dependencies between specifications in the Enabler Release specification baseline is detailed in [IOPPROC].

3.2 Definitions

Enabler Release –a collection of specifications that combined together form an enabler for a service area, e.g. a download enabler, a browsing enabler, a messaging enabler, a location enabler, etc. The specifications that are forming an enabler should combined fulfil a number of related market requirements.

Minimum Functionality Description – Description of the guaranteed features and functionality that will be enabled by implementing the minimum mandatory part of the Enabler Release.

3.3 Abbreviations

CA	Certificate Authority
CRL	Certificate Revocation List
ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
OCSP	Online certificate status protocol
OMA	Open Mobile Alliance
OMA	Open Mobile Alliance

4. Introduction

This document outlines the Enabler Release Definition for the Online Certificate Status Protocol (OCSP) mobile profile V1_0 and the respective conformance requirements for clients and servers implementing claiming compliance to it as defined by Open Mobile Alliance across the specification baseline.

While digital certificates provide a secure mechanism to identify and authenticate an entity via the verification of a digital signature, there must also be mechanisms in place to validate that the certificate, and the associated private key, in use are in fact still considered trusted and valid. This issue is commonly known as certificate validation and is based on the concept of certificate revocation. Certificates may be revoked for various reasons, including, but not limited to, change of name, change of association between subject and CA and compromise or suspicion of compromise of the corresponding private key. Once revoked, there must be mechanisms in place to determine if a certificate has been revoked.

The Internet Engineering Task Force's (IETF) Public Key Infrastructure working group has defined a method of certificate validation that does not rely on CRL's. The Online Certificate Status Protocol (OCSP) as defined by [RFC 2560] replaces the CRL concept with a simple certificate status request and response protocol to a central server. This server is authorized to respond with certificate status information.

To perform an OCSP certificate status check, a client sends a request to an OCSP responder. The OCSP responder then determines the revocation status of the requested certificate and constructs the corresponding OCSP response. This response is typically signed by the OCSP responder to ensure data integrity and that the response originated from an authoritative source.

5. Enabler Release Specification Baseline

This section is normative.

The following specifications comprise the OCSP v.1.0 Enabler release:

OCSP Mobile Profile V1.0[OCSP]

6. Minimum Functionality Description for OCSP V1.0 Enabler Release

The minimum functionality for the OCSP mobile profile release includes:

- The ability for client to send an OCSPrequest for the status of a certificate.
- The ability for the client to process an OCSP response.

7. Conformance Requirements Notation Details

This section is informative

The tables in following chapters use the following notation:

Item:

Entry in this column **MUST** be a valid ScrItem according to [IOPPROC].

Feature/Application:

Entry in this column **SHOULD** be a short descriptive label to the **Item** in question.

Status:

Entry in this column **MUST** accurately reflect the architectural status of the **Item** in question.

- M means the **Item** is mandatory for the class
- O means the **Item** is optional for the class
- NA means the **Item** is not applicable for the class

Requirement:

Expression in the column **MUST** be a valid TerminalExpression according to [IOPPROC] and it **MUST** accurately reflect the architectural requirement of the **Item** in question.

8. ERDEF for OCSP V1.0 - Client Requirements

This section is normative.

Table 1 ERDEF for OCSP V1.0 Enabler Client-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-OCSP-C-001	OCSPV1_0 Client	M	OCSP MCF

9. ERDEF for OCSP V1.0 - Server Requirements

This section is normative.

The OCSP Enabler Release does not specify server requirements

Table 2 ERDEF for OCSP V1.0 Server-side Requirements

Item	Feature / Application	Status	Requirement
N/A	N/A	N/A	

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No previous version within OMA

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Version OMA-ERELED-OCSP-V1_0	07 Jan 2004	n/a	
Candidate Version OMA-ERELED-OCSP-V1_0	27 Jan 2004	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2004-0020-OSCP-V1_0-for-candidate-approval