Enabler Release Definition for Wireless Public Key Infrastructure

Candidate Version 1.0 – 15 Jun 2004

Open Mobile Alliance

OMA-ERELD-WPKI-V1_0-20040615-C

Contents

1. Scope

The scope of this document is limited to the Enabler Release Definition of the Wireless Public Key Infrastructure enabler (abbreviated hereafter as WPKI) according to OMA Release process and the Enabler Release specification baseline listed in section 5.

2. References

2.1 Normative References

[IOPPROC]	"OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, URL: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
[WIM]	"Wireless Identity Module Version 1.1. Part: Security", OMA-WAP-WIM-v1_1, Open Mobile Alliance, URL: http://www.openmobilealliance.org
[WAPWPKI]	"Wireless Public Key Infrastructure Specification", WAP-217-WPKI, Open Mobile Alliance, URL: http://www.openmobilealliance.org
[WAPWTLS]	"Wireless Transport Layer Security", WAP-261-WTLS, Open Mobile Alliance, URL: http://www.openmobilealliance.org
[TLS Profile]	"TLS Profile and Tunneling Specification", WAP-219-TLS, Open Mobile Alliance, URL: http://www.openmobilealliance.org
[WMLScriptCrypto]	"WMLScript Crypto Library Specification", WAP-161-WMLScriptCrypto, Open Mobile Alliance, URL: http://www.openmobilealliance.org
[CertProf]	"Certificate and CRL Profiles", OMA-Security-CertProf-v1_1, Open Mobile Alliance, URL: http://www.openmobilealliance.org
[ESMPCrypto]	"ECMAScript Crypto library", OMA-WAP-ECMACR-V1_0, Open Mobile Alliance, URL: http://www.openmobilealliance.org

2.2 Informative References

None.

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

ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
OMA	Open Mobile Alliance
WPKI	Wireless Public Key Infrastructure

4. Introduction

This document outlines the Enabler Release Definition for Wireless Public Key Infrastructure (WPKI) and the respective conformance requirements for clients and servers claiming compliance to it as defined by the Open Mobile Alliance across the specification baseline.

WPKI provides the means to establish public key security features between clients and servers such as authentication, confidentiality and integrity of exchanged messages. Security features can be established either in the transport layer, in the application layer, or in both. It is also possible for clients to authenticate themselves to servers using strong public key authentication methods.

5. Enabler Release Specification Baseline

This section is normative.

The following list of specifications form the total WPKI Enabler Release, though a given device or server may support a valid subset of these specifications and the features contained within those specifications. The actual minimum profile for a device is defined in section 8. The minimum profile for the server is defined in section 9. A description of the minimum functionality is defined in section 6.

The following specifications comprise the WPKI enabler release:

Wireless PKI architecture	[WAPWPKI]
WTLS transport layer security	[WAPWTLS]
TLS transport layer security	[TLS Profile]
Certificate profile	[CertProf]
WML script crypto services	[WMLScriptCrypto]
Wireless Identity Module	[WIM]
ECMAScript Crypto	[ESMPCrypto]

6. Minimum Functionality Description for WPKI

This section is informative.

The WPKI version 1.0 provides security features that can be used in the transport layer and/or the application layer. There are then different possibilities for a minimum functionality. If transport layer security is to be provided, then the minimum functionality is the functionality specified either in [TLS Profile] or in [WAPWTLS]. If application layer security is to be provided, then the minimum functionality is the functionality specified in [WMLScriptCrypto] or [ESMPCrypto], and [WIM]. If client authentication is needed, then all the functions specified in [WIM] and [CertProf] are to be added.

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 WPKI - Client Requirements

This section is normative.

Table 1 ERDEF for WPKI Client-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-WPKI-C-000	Security features	M	OMA-ERDEF-WPKI-C-001 OR OMA-ERDEF-WPKI-C-002 OR OMA-ERDEF-WPKI-C-003
OMA-ERDEF-WPKI-C-001	Transport layer security Client	O	WAPWTLS:MCF OR TLSProfile:MCF
OMA-ERDEF-WPKI-C-002	Application layer security Client	O	WMLScriptCrypto:MCF OR ESMPCrypto:MCF
OMA-ERDEF-WPKI-C-003	Client authentication	O	WIM:MCF AND CertProf:MCF

9. ERDEF for WPKI - Server Requirements

This section is normative.

Table 2 ERDEF for WPKI Server-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-WPKI-S-000	Security features	M	OMA-ERDEF-WPKI-S-001 OR OMA-ERDEF-WPKI-S-002
OMA-ERDEF-WPKI-S-001	Transport layer security Server	O	WAPWTLS:MSF OR TLSProfile:MSF
OMA-ERDEF-WPKI-S-002	Application layer security Server	O	WMLScriptCrypto:MSF OR ESMPCrypto:MSF
OMA-ERDEF-WPKI-S-003	Client authentication	M	CertProf:MSF

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 V1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ERELD-WPKI-V1_0	14 Apr 2004	n/a	Corrections following consistency review
	20 Jan 2004	n/a	First draft
	26 Jan 2004	n/a	Update of the spec list (WIM and WPKI)
	30 Jan 2004	n/a	Update of the spec list
	02 Feb 2004	n/a	Various minor corrections
	04 Feb 2004	n/a	Various corrections, in pp in section 8 and 9, general cleanup of notes
	14 Apr 2004	n/a	Corrections following the consistency review
Candidate Version OMA-ERELD-WPKI-V1_0	15 Jun 2004	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2004-0193-WPKI-V1_0_for-candidate