

Specification Information Note
OMA-WAP-217_105-WPKI-SIN-20020816-a
Version 16-Aug-2002

for

Open Mobile Alliance
OMA-WAP-217-WPKI-20010424-a
Wireless Application Protocol
Public Key Infrastructure Definition
Version 24-April-2001

Continues the Technical Activities
Originated in the WAP Forum



A list of errata and updates to this document is available from Open Mobile Alliance™ Web site,
<http://www.openmobilealliance.org/>, in the form of SIN documents, which are subject to revision or removal without notice.

© 2002, Open Mobile Alliance, Ltd. All rights reserved.

Terms and conditions of use are available from the OMA™ Web site at <http://www.wapforum.org/what/copyright.htm>.

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 OMA™. 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 OMA™ 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.

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

No representations or warranties (whether express or implied) are made by the WAP Forum™ or any WAP Forum member or its affiliates regarding any of the IPR's represented on this 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 OMA™ in the manner published at <http://www.wapforum.org/>.

Contents

1. SCOPE.....	4
2. NOTATION	4
3. REPLACE SCR TABLES	5
3.1 CHANGE CLASSIFICATION	5
3.2 CHANGE SUMMARY.....	5
3.3 CHANGE DESCRIPTION	5

1. Scope

This document provides changes and corrections to the following document files:

- OMA-WAP-217-WPKI-20010424-a

It includes changes to clarify the usage of the “CA_DOMAIN” field in the CERTRESPONSE from the change request CR-RSA-Singapore-WPKI-1.

2. Notation

In the subsections describing the changes new text is underlined. Removed text has ~~striketrough~~ marks. The presented text is copied from the specification. Text that is not presented is not affected at all. The change descriptions may also include editor’s notes similar to the one below. The notes are not part of the actual changes and must not be included in the changed text.

Editor's note: Framed notes like these only clarify where and how the changes shall be applied.

3. Replace SCR Tables

3.1 Change Classification

Class 1 – Corrections

3.2 Change Summary and Motivation

1. The previous text mandates a MUST that only applies if you break another MUST: “ca_domain: MUST contain the hash of the CA’s public key. If omitted IdentifierType.null MUST be used to indicate the absence of the ca_domain”.
2. There are no arguments to require the MUST in “MUST contain the hash of the CA’s public key”, a SHOULD is more appropriate.
3. The usage of the “ca_domain” field is not discussed.
4. Typo of “uint8” in CertResponse.

3.3 Change Description

Editor's note:-Affected Section 7.3.5:

7.2.5 Delivery of Certificates

[Add the following text to beginning paragraphs of section 7.3.5:](#)

[The “ca_domain” value may be used e.g. by clients to compare it with values given by origin servers in WMLScript Crypto Library’s signText\(\) TRUSTED_KEY_HASH fields. Thus issuing a CertResponse cert_info with a ca_domain of IdentifierType “null” would make that impossible.](#)

[Change in the table in 7.3.5:](#)

cert_info These fields contain the details of a certificate which has been issued for the client.

display_name: (max 32 chars, so it can fit in a PKCS#15 label) SHOULD be a human readable name which indicates the services for which the certificate is useful. This field MUST NOT be empty. The character set used here SHOULD be UTF8 (in order to be stored in WIM, it MUST be UTF8)

ca_domain: ~~MUST contain the hash of the CA's public key—this MAY be omitted if the cert field is present and the certificate contain an authority KeyId extension and the client is able to extract this field from the certificate. If omitted IdentifierType.null MUST be used to indicate the absence of the ca_domain.~~ SHOULD contain the hash of the CA’s public key in an Identifier.key_hash_sha field. ~~Otherwise the IdentifierType “null” alternative MUST be used to indicate the absence of an explicit CA domain.~~ Note that the ca_domain field might, in some cases, not match the AKID from the client certificate, if e.g. the issuing CA is subordinate CA within a hierarchy and the WTLS servers use the root of the hierarchy as the ca_domain.

[Correction of the typo:](#)

Replace the “version” line inside the CertResponse structure with:

uint8 version ;

(It currently says “unit8”.)