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.

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 ~~strikethrough~~ 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 tha 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”.)