Specification Information Note

OMA-WAP-260_101-WIM-SIN-20020107-a

Version 07-Jan-2002

for

Open Mobile Alliance
OMA-WAP-260-WIM-20010712-a
Wireless Identity Module Specification
Version 12-July-2001

Continues the Technical Activities
Originated in the WAP Forum

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

Copyright 2002, Open Mobile Alliance Ltd., All Rights Reserved.

OMA Web Site Terms of Use, Trademark, Copyright Permission,
Membership and IPR Policy Rules Apply.

© 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

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

1. Scope

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

OMA-WAP-260-WIM-20010712-a

It includes changes from the following change requests:

- ADDITIONAL UPDATE-ACC FOR EF(PIN)
- CLARIFICATION ON CDF ENTRIES

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.

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

3. ADDITIONAL UPDATE-ACC FOR EF(PIN)

3.1 Change Classification

Class 2 – Bug Fixes

3.2 Change Summary

The current WIM-Specification - chapter 12.2 - describes the recommended Access-Conditions (ACC) for WIM-specific files.

The Update-ACC for “PIN files” is currently set to CHV, which basically enables the cardholder to manipulate sensitive authentication information.
Assuming that this is only the case for a minor amount of WIMs, this recommendation should additionally include the options SYS and NEV.

3.3 Change Description

Editor's note: On page 92 (only one row of the table is affected)

PIN files	Read: NEV Update: CHV | SYS | NEV	~~Updating~~ The PIN value can only be updated by the cardholder ~~is performed~~ using verification related operations.

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

4. Clarification on CDF entries

4.1 Change Classification

Class 3 – Clerical Corrections

4.2 Change Summary

The WIM spec states that "A CDF must be possible to modify by the cardholder if it points to certificate objects that are possible to modify by the cardholder. For modification, the PIN-G must be entered" (section 12.2).

The WIM spec also states that the WIM MUST enforce access conditions when accessing the PKCS#15 files (as for other objects). If a WIM contains certificates that are not modifiable by the user then the user should not be able to modify the CDF itself. If a WIM contains modifiable certificates and non-modifiable certificates there should be a different CDF list for user certificates that are modifiable and another list of CDFs which are not modifiable. All modifiable CDFs are put in a file with access conditions that allow update if PIN-G is verified. On the other hand all CDFs that are not modifiable are put in another file with access conditions that do not permit updating the CDFs content.

4.3 Change Description

Editor's note: On page 42

9.4.4 Certificate Directory Files (CDFs)

The Certificate Directory Files ([PKCS15], section 6.5.5) contain directories of certificates known to the PKCS#15 application. At least one CDF MUST be present on a WIM which contains certificates (or references to certificates).

Each logical record of a CDF, describing a single certificate, MUST contain the following fields

- human readable label to describe the certificate (commonObjectAttributes.label)
- common flags (commonObjectAttributes.flags)
- 20-byte public key SHA-1 hash, as defined in [PKCS15], to correlate the certificate with a certain private key (PKCS15CommonCertificateAttributes.iD)
- file path, index (binary offset), and length, to be used in selecting the file and binary read operations, or a certificate url
- the 20-byte public key SHA-1 hash of the issuer key (PKCS15CommonCertificateAttributes.requestId) (this field need not used for root CA certificates, unless it is necessary for maintaining a fixed record length)

A logical record of a CDF, describing a CA certificate MUST also contain the field PKCS15CommonCertificateAttributes.authority.

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

A CDF pointed by a certificates field in the ODF, contains references to certificates issued to the WIM user.
(If some user certificates are modifiable and some are not then there may be two distinct CDFs pointed by a certificates field in the ODF. One is grouping all references to modifiable certificates and another is grouping all references to non-modifiable certificates).

A CDF pointed by a trustedCertificates field in the ODF, contains references to trusted CA certificates. Both the CDF and the EF(s) containing the certificate data pointed to MUST NOT be modifiable by the user. These CA certificates are considered trusted by the WIM issuer and should thus be trusted by the user, too. They can be used by the ME to verify a server in a WTLS handshake, or to verify signatures in downloaded content, eg, downloaded applications.

A CDF pointed by a usefulCertificates field in the ODF, contains references to CA certificates that are updateable by the user.

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