

Specification Information Note OMA- WAP-260_100-WIM-SIN-20010725-a

Version 25-Jul-2001

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 WAP ForumTM Web site, http://www.wapforum.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.openmobile.anniance.org/documents/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 OMATM. 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 OMATM 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.

Open Mobile AllianceTM members have agreed to use reasonable endeavors to disclose in a timely manner to the Open Mobile Alliance 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 Open Mobile Alliance 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 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 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 OMATM in the manner published at http://www.openmobilealliance.org/technical.htm

Contents

1.	SC	COPE	4
2.	NO	OTATION	4
3.	IN	CLUSION OF INTER-SPECIFICATION DEPENDENCIES AND EDITORIAL CORRECTIONS	5
3		CHANGE CLASSIFICATION	
3	3.2	CHANGE SUMMARY	
3	3.3	CHANGE DESCRIPTION	
14	WIM	A STATIC CONFORMANCE REQUIREMENT	5
1	4.1	WIM OPTIONS	4
		ME OPTIONS	

1. Scope

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

OMA-WAP-260-WIM-20010712-a

It includes changes to:

- Remove sub-function from SCR table.

2. Notation

In the subsections describing the changes new text is <u>underlined</u>. Removed text has <u>strikethrough</u> 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. Inclusion of Inter-specification dependencies and editorial corrections.

3.1 Change Classification

Class 3 - Clerical Corrections

3.2 Change Summary

Remove sub-function from SCR tables to conform to WAP-221-CREQ [WAPCREQ].

3.3 Change Description

Editor's note: The Function and Sub-function columns have been merged. To perform the merge, the original Function cell was split to obtain one cell per SCR Item and the text duplicated in each cell. This new cell was then merged with the corresponding Sub-function cell. These changes are **not** highlighted.

The combined text has been editted where necessary. These changes are highlighted.

Replace the whole of Section 14 with the following:

14 WIM Static Conformance Requirement

This static conformance requirement [WAPCREQ] lists a minimum set of functions that can be implemented to help ensure that WIM implementations and ME implementations will be able to inter-operate. The "Status" column indicates if the function is mandatory (M) or optional (O).

14.1 WIM Options

14.1.1 General WIM Options

Item	Function	Reference	Status	Requirement
WIM-ICC-001	WTLS supported	6.1	M	
WIM-ICC-002	Generic (application level) functionality	6.2.2	M	WIM-ICC-023
	Signing of hash			OR
	Either RSA or ECC MUST be supported.			WIM-ICC-025
	In case of ECC, ECDSA MUST be supported.			
WIM-ICC-003	Generic (application level) functionality	6.2.1	О	WIM-ICC-024
	Unwrap (decipher) a key			OR
	Either RSA or ECC MAY be supported.			WIM-ICC-026
	In case of ECC, ECES SHOULD be supported.			
WIM-ICC-004	Data storage	9.4.1	M	
	PKCS#15 ODF			
WIM-ICC-005	Data storage	9.4.7	M	
	PKCS#15 TokenInfo			
WIM-ICC-006	Data storage	9.4.2	M	
	PKCS#15 PrKDF			
WIM-ICC-007	Data storage	9.4.3	О	
	PKCS#15 PuKDF			

Item	Function	Reference	Status	Requirement
WIM-ICC-008	Data storage	9.4.4	M	
	PKCS#15 CDF			
WIM-ICC-009	Data storage	9.4.4	О	
	PKCS#15 CDF trusted certificates			
WIM-ICC-090	Data storage	9.4.4	О	
	PKCS#15 CDF useful certificates			
WIM-ICC-010	Data storage	9.4.6	M	
	PKCS#15 AODF			
WIM-ICC-011	Data storage	9.4.5	M	
	PKCS#15 DODF-wtls			
WIM-ICC-012	Data storage	9.4.8	M	
	PKCS#15 UnusedSpace			
WIM-ICC-013	Data storage	9.4.2, 12.1.1	M	
	Private key, use by ME			
WIM-ICC-014	Data storage	9.4.3	О	
	Public key, read by ME			
WIM-ICC-015	Data storage	9.4.4, 12.1.1	M	
	Certificate, read by ME	,		
WIM-ICC-016	Data storage	9.4.4, 13.4	M	
	Certificate, store by ME	,		
WIM-ICC-017	Data storage	9.4.10	M	
	WTLS Peers			
WIM-ICC-018	Data storage	9.4.11	M	
	WTLS Sessions			
WIM-ICC-019	Random number generation	6.1	M	
WIM-ICC-020	WTLS key exchange algorithms; at least one supported	8	M	WIM-ICC-021
				OR
				WIM-ICC-022
WIM-ICC-021	RSA	8.1	O	WIM-ICC-023
				AND
				WIM-ICC-028 AND
				WIM-ICC-130
WIM-ICC-022	ECDH	8.2	0	WIM-ICC-025
WIWI ICC 022	Bebli	0.2		AND
				WIM-ICC-051
				AND
				WIM-ICC-131
WIM-ICC-023	Generic (application level) algorithms.	6.2.2	О	WIM-ICC-028
	RSA signing			
WIM-ICC-024	Generic (application level) algorithms.	6.2.1	О	WIM-ICC-028
	RSA decryption			
WIM-ICC-025	Generic (application level) algorithms.	6.2.2	О	WIM-ICC-050
	ECDSA signing			
WIM-ICC-026	Generic (application level) algorithms.	6.2.1	О	WIM-ICC-050
	ECIES decryption			
WIM-ICC-027	WTLS pseudo-random function based on SHA-1	8	M	

Item	Function	Reference	Status	Requirement
WIM-ICC-028	Minimum RSA modulus length is 1024 bits, when RSA supported	12.1.1	О	
WIM-ICC-051	ECC key length (bits), when ECC supported Minimum 160	12.1.1	О	
WIM-ICC-050	If ECC is used, at least one basic curve MUST be supported.	WTLS App.	0	WIM-ICC-030 OR WIM-ICC-032
WIM-ICC-030	ECC basic curves Curve 5 (163 bits)	WTLS App.	О	
WIM-ICC-032	ECC basic curves Curve 7 (160 bits)	WTLS App. A	О	
WIM-ICC-033	ECC non-basic curves Curve 1 (113 bits)	WTLS App.	О	
WIM-ICC-034	ECC non-basic curves Curve 3 (163 bits)	WTLS App.	О	
WIM-ICC-029	ECC non-basic curves Curve 4 (113 bits)	WTLS App. A	О	
WIM-ICC-031	ECC non-basic curves Curve 6 (112 bits)	WTLS App.	О	
WIM-ICC-035	ECC non-basic curves Curve 8 (112 bits)	WTLS App.	О	
WIM-ICC-036	ECC non-basic curves Curve 9 (160 bits)	WTLS App.	О	
WIM-ICC-080	ECC non-basic curves Curve 10 (233 bits)	WTLS App.	О	
WIM-ICC-081	ECC non-basic curves Curve 11 (233 bits)	WTLS App.	О	
WIM-ICC-082	ECC non-basic curves Curve 12 (224 bits)	WTLS App.	О	
WIM-ICC-037	Private keys Authentication key Note: This key MUST be a separate key to each of the non-repudiation keys, but may be used for decryption.	12.1.1	M	
WIM-ICC-038	Private keys Decryption key (application level) Note: This key MUST be a separate key to each of the non-repudiation keys, but may be combined with the Authentication key.	12.1.1	0	
WIM-ICC-039	Private keys Non-repudiation key (application level) Note: Each non-repudiation key MUST be a separate key and separate to the Authentication and Decryption key(s).	12.1.1	M	
WIM-ICC-040	PIN handling Recommended PIN format	12.1.4.1	M	
WIM-ICC-041	Digital signature verification RSA	7.2.4.2	О	

Item	Function	Reference	Status	Requirement
WIM-ICC-042	Digital signature verification	7.2.4.2	О	
	ECDSA			
WIM-ICC-043	Use of PKCS#15 file path fields	9.4.1	M	WIM-ICC-044 OR WIM-ICC-045
WIM-ICC-044	PKCS#15 file path fields as 2-byte file identifiers	9.4.1	О	
WIM-ICC-045	PKCS#15 file path fields as absolute or relative paths	9.4.1	О	

14.1.2 WIM ICC Options

Item	Function	Reference	Status	Requirement
WIM-ICC-101	Removed.			
WIM-ICC-102	Direct application selection	11.3.3.1	M	
WIM-ICC-103	Removed.			
WIM-ICC-104	Logical channels. A WIM ICC that supports also some	11.3.2	О	WIM-ICC-105
	other applications (eg, GSM SIM) MUST support logical			
	channels.			
WIM-ICC-105	ICC commands	11.3.2	О	
	MANAGE CHANNEL			
	MANAGE CHANNEL MUST be supported by an ICC			
	that supports multiple applications.			
WIM-ICC-106	ICC commands	11.3.4.1	M	
	VERIFY			
WIM-ICC-107	ICC commands	11.3.4.2	О	
	DISABLE VERIFICATION			
WIM-ICC-108	ICC commands	11.3.4.3	О	
	ENABLE VERIFICATION			
WIM-ICC-109	ICC commands	11.3.4.4	M	
	CHANGE REFERENCE DATA			
WIM-ICC-110	ICC commands	11.3.4.5	M	
	RESET RETRY COUNTER			
WIM-ICC-111	ICC commands	11.3.5.1	M	
	SELECT			
WIM-ICC-112	ICC commands	11.3.5.2	M	
	READ BINARY			
WIM-ICC-113	ICC commands	11.3.5.3	M	
	UPDATE BINARY			
WIM-ICC-114	ICC commands	11.3.6.1	M	
	MANAGE SECURITY ENVIRONMENT			
WIM-ICC-115	ICC commands	11.3.6.4,	M	WIM-ICC-130
	PERFORM SECURITY OPERATION (all but Key	11.3.6.7, 11.3.6.8,		OR WIM-ICC-131
	Transport and Key Agreement)	11.3.6.8,		W IIVI-ICC-131
		11.3.6.10		
WIM-ICC-130	ICC commands	11.3.6.4,	О	
	PERFORM SECURITY OPERATION Key Transport	11.3.6.5		
WIM-ICC-131	ICC commands	11.3.6.4,	0	
	PERFORM SECURITY OPERATION Key Agreement	11.3.6.6		
WIM-ICC-116	ICC commands	11.3.6.12	M	
	ASK RANDOM			
WIM-ICC-117	ICC commands	11.3.7.1	M	
	GET RESPONSE			
WIM-ICC-118	ICC size; at least one supported	11.1	M	WIM-ICC-119
				OR
				WIM-ICC-120
WIM-ICC-119	ID-1	11.1	0	
WIM-ICC-120	ID-000 (Plug-in)	11.1	0	

Function Status Item Reference Requirement WIM-ICC-121 Transmission protocols 11.2 M WIM-ICC-122 Transmission protocols 11.2 O WIM-ICC-123 Supply voltage; indicated in ATR 11.2 M WIM-ICC-124 Supply voltage; indicated in ATR 11.2 O WIM-ICC-125 Enforce access control rules 12.2 M

14.2 ME Options

14.2.1 General ME Options

Item	Function	Reference	Status	Requirement
WIM-C-001	WTLS	[WAPWTLS], 8	О	WIM-C-019 AND WIM-C-020 AND WIM-C-022 AND WIM-C-039
WIM-C-002	Generic (application level) functionality Signing of hash	6.2.2	0	WIM-C-025 OR WIM-C-027
WIM-C-003	Generic (application level) functionality Unwrap (decipher) a key	6,2,1	0	WIM-C-026 OR WIM-C-028
WIM-C-004	Data storage PKCS#15 ODF	9.4.1	М	
WIM-C-005	Data storage PKCS#15 TokenInfo	9.4.7	M	
WIM-C-006	Data storage PKCS#15 PrKDF	9.4.2	М	
WIM-C-007	Data storage PKCS#15 PuKDF	9.4.3	О	
WIM-C-008	Data storage PKCS#15 CDF	9.4.4	M	
WIM-C-009	Data storage PKCS#15 CDF trusted certificates	9.4.4	M	
WIM-C-090	Data storage PKCS#15 CDF useful certificates	9.4.4	M	
WIM-C-010	Data storage PKCS#15 AODF	9.4.6	M	
WIM-C-011	Data storage PKCS#15 DODF	9.4.5	M	
WIM-C-012	Data storage PKCS#15 UnusedSpace	9.4.8	M	
WIM-C-013	Data storage Use private key	9.4.2	M	
WIM-C-014	Data storage Read public key	9.4.3	О	
WIM-C-015	Data storage Read user certificate	9.4.4	M	
WIM-C-016	Data storage Store user certificate	9.4.4	M	
WIM-C-017	Data storage Read CA certificate	9.4.4	М	

Item **Function** Reference Status Requirement WIM-C-018 9.4.4 М Data storage Store CA certificate WIM-C-019 Data storage 9.4.10 O WTLS Peers O WIM-C-020 Data storage 9.4.11 WTLS Sessions Use of random numbers generated by the WIM WIM-C-021 6.1 O WIM-C-022 O 8 WIM-C-023 WTLS key exchange algorithms; at least one supported OR WIM-C-024 RSA 8.1 O WIM-C-029 WIM-C-023 AND WIM-C-030 AND WIM-C-130 O WIM-C-024 **ECDH** 8.2 WIM-C-029 AND WIM-C-050 AND WIM-C-131 WIM-C-025 6.2.2 Generic (application level) algorithms \mathbf{O} WIM-C-030 RSA signing WIM-C-026 6.2.1 O WIM-C-030 Generic (application level) algorithms RSA decryption WIM-C-027 Generic (application level) algorithms 6.2.2 O WIM-C-050 **ECDSA** signing 6.2.1 O WIM-C-028 Generic (application level) algorithms WIM-C-050 ECIES decryption O WIM-C-029 Use WTLS pseudo-random function based on SHA-1 8 WIM-C-030 If RSA is supported, the minimum expected RSA 12.11 \mathbf{O} modulus length is 1024 bits, for signing performed in WIM. If ECC is used, at least one basic curve MUST be WIM-C-050 WTLS App. A WIM-C-032 supported. OR WIM-C-034 WIM-C-032 ECC basic curves O WTLS App. A Curve 5 (163 bits) WIM-C-034 ECC basic curves O WTLS App. A Curve 7 (160 bits) WIM-C-035 ECC non-basic curves WTLS App. A Curve 1 (113 bits) WIM-C-036 ECC non-basic curves WTLS App. A O Curve 3 (163 bits) WIM-C-031 ECC non-basic curves O WTLS App. A Curve 4 (113 bits) WIM-C-033 ECC non-basic curves WTLS App. A O Curve 6 (112 bits)

Item	Function	Reference	Status	Requirement
WIM-C-037	ECC non-basic curves	WTLS App. A	О	
	Curve 8 (112 bits)			
WIM-C-038	ECC non-basic curves	WTLS App. A	О	
	Curve 9 (160 bits)			
WIM-C-080	ECC non-basic curves	WTLS App. A	О	
	Curve 10 (233 bits)			
WIM-C-081	ECC non-basic curves	WTLS App. A	О	
	Curve 11 (233 bits)			
WIM-C-082	ECC non-basic curves	WTLS App. A	О	
	Curve 12 (224 bits)			
WIM-C-039	Use private Authentication key for WTLS client authentication	12.1.1	О	
WIM-C-040	Use private Authentication key for decryption	12.1.1	О	
WIM-C-041	Use private Decryption key (application level) for decryption.	12.1.1	О	
WIM-C-042	Use private Non-repudiation key (application level)	12.1.1	О	
WIM-C-043	PIN handling	12.1.4.1	M	
	Recommended PIN format			
WIM-C-044	Use WIM for digital signature verification	7.2.4.2	О	
	RSA			
WIM-C-045	Use WIM for digital signature verification	7.2.4.2	О	
	ECDSA			
WIM-C-046	PKCS#15 file path fields	9.4.1	M	
	Support of 2-byte file identifiers			
WIM-C-047	PKCS#15 file path fields	9.4.1	M	
	Support of absolute or relative paths			

14.2.2 ME Use of WIM ICC

Item	Function	Reference	Status	Requirement
WIM-C-101	Direct application selection	11.3.3.1	M	
WIM-C-102	Removed.			
WIM-C-103	Logical channels. A ME that uses some other application on ICC WIM (eg, GSM SIM), MUST support logical channels.	11.3.2	О	WIM-C-104
WIM-C-104	ICC commands MANAGE CHANNEL	11.3.2	О	
WIM-C-105	ICC commands VERIFY	11.3.4.1	M	
WIM-C-106	ICC commands DISABLE VERIFICATION	11.3.4.2	M	
WIM-C-107	ICC commands ENABLE VERIFICATION	11.3.4.3	M	
WIM-C-108	ICC commands CHANGE REFERENCE DATA	11.3.4.4	M	

Item	Function	Reference	Status	Requirement
WIM-C-109	ICC commands	11.3.4.5	M	
	RESET RETRY COUNTER			
WIM-C-110	ICC commands	11.3.5.1	M	
	SELECT			
WIM-C-111	ICC commands	11.3.5.2	M	
	READ BINARY			
WIM-C-112	ICC commands	11.3.5.3	M	
	UPDATE BINARY			
WIM-C-113	ICC commands	11.3.6.1	M	
	MANAGE SECURITY ENVIRONMENT			
WIM-C-114	ICC commands	11.3.6.4	M	
	PERFORM SECURITY OPERATION			
WIM-C-114	ICC commands	11.3.6.4,	M	WIM-C-130
	PERFORM SECURITY OPERATION (all but Key	11.3.6.7,		OR
	Transport and Key Agreement)	11.3.6.8,		WIM-C-131
		11.3.6.9, 11.3.6.10		
WIM-C-130	100			
WIM-C-130	ICC commands	11.3.6.4, 11.3.6.5	О	
WIM-C-131	PERFORM SECURITY OPERATION Key Transport		0	
W IM-C-131	ICC commands	11.3.6.4, 11.3.6.6	0	
WD4 C 115	PERFORM SECURITY OPERATION Key Agreement			
WIM-C-115	ICC commands	11.3.6.12	О	
WW 1 C 11 C	ASK RANDOM	11.07.1	3.6	
WIM-C-116	ICC commands	11.3.7.1	M	
WD 4 C 117	GET RESPONSE	11.1	2.6	WD4 C 110
WIM-C-117	ICC size; at least one supported	11.1	M	WIM-C-118 OR
				WIM-C-119
WIM-C-118	ID-1	11.1	0	
WIM-C-119	ID-000 (Plug-in)	11.1	0	
WIM-C-120	Transmission protocols	11.2	M	
WHAT & 120	T=0	11.2	1,1	
WIM-C-121	Transmission protocols	11.2	О	
WHVI C 121	T=1	11.2		
WIM-C-122	Supply voltage, SIM card	11.2	M	
WHVI C 122	3 V	11.2	171	
WIM-C-123	Supply voltage, SIM card	11.2	0	
WHVI C 123	5 V	11.2		
WIM-C-124	Supply voltage, external card	11.2	M	
,, IIII-C-124	3 V	11,2	141	
WIM-C-125	Supply voltage, external card	11.2	0	
WIN C-123	5 V	11.2		
WIM-C-126	Support access control rules	12.2	M	
VV 11V1-C-12U	Support access control rules	12.2	171	