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 Forum™ Web site, http://www.wapforum.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.openmobilealliance.org/technical.htm

Contents

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

Item	Function	Reference	Status	Requirement
WIM-ICC-008	Data storage PKCS#15 CDF	9.4.4	M	
WIM-ICC-009	Data storage PKCS#15 CDF trusted certificates	9.4.4	O	
WIM-ICC-090	Data storage PKCS#15 CDF useful certificates	9.4.4	O	
WIM-ICC-010	Data storage PKCS#15 AODF	9.4.6	M	
WIM-ICC-011	Data storage PKCS#15 DODF-wtls	9.4.5	M	
WIM-ICC-012	Data storage PKCS#15 UnusedSpace	9.4.8	M	
WIM-ICC-013	Data storage Private key, use by ME	9.4.2, 12.1.1	M	
WIM-ICC-014	Data storage Public key, read by ME	9.4.3	O	
WIM-ICC-015	Data storage Certificate, read by ME	9.4.4, 12.1.1	M	
WIM-ICC-016	Data storage Certificate, store by ME	9.4.4, 13.4	M	
WIM-ICC-017	Data storage WTLS Peers	9.4.10	M	
WIM-ICC-018	Data storage WTLS Sessions	9.4.11	M	
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	O	WIM-ICC-025 AND WIM-ICC-051 AND WIM-ICC-131
WIM-ICC-023	Generic (application level) algorithms. RSA signing	6.2.2	O	WIM-ICC-028
WIM-ICC-024	Generic (application level) algorithms. RSA decryption	6.2.1	O	WIM-ICC-028
WIM-ICC-025	Generic (application level) algorithms. ECDSA signing	6.2.2	O	WIM-ICC-050
WIM-ICC-026	Generic (application level) algorithms. ECIES decryption	6.2.1	O	WIM-ICC-050
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	O	
WIM-ICC-051	ECC key length (bits), when ECC supported Minimum 160	12.1.1	O	
WIM-ICC-050	If ECC is used, at least one basic curve MUST be supported.	WTLS App. A	O	WIM-ICC-030 OR WIM-ICC-032
WIM-ICC-030	ECC basic curves Curve 5 (163 bits)	WTLS App. A	O	
WIM-ICC-032	ECC basic curves Curve 7 (160 bits)	WTLS App. A	O	
WIM-ICC-033	ECC non-basic curves Curve 1 (113 bits)	WTLS App. A	O	
WIM-ICC-034	ECC non-basic curves Curve 3 (163 bits)	WTLS App. A	O	
WIM-ICC-029	ECC non-basic curves Curve 4 (113 bits)	WTLS App. A	O	
WIM-ICC-031	ECC non-basic curves Curve 6 (112 bits)	WTLS App. A	O	
WIM-ICC-035	ECC non-basic curves Curve 8 (112 bits)	WTLS App. A	O	
WIM-ICC-036	ECC non-basic curves Curve 9 (160 bits)	WTLS App. A	O	
WIM-ICC-080	ECC non-basic curves Curve 10 (233 bits)	WTLS App. A	O	
WIM-ICC-081	ECC non-basic curves Curve 11 (233 bits)	WTLS App. A	O	
WIM-ICC-082	ECC non-basic curves Curve 12 (224 bits)	WTLS App. A	O	
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	O	
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	O	

Item	Function	Reference	Status	Requirement
WIM-ICC-042	Digital signature verification ECDSA	7.2.4.2	O	
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	O	
WIM-ICC-045	PKCS#15 file path fields as absolute or relative paths	9.4.1	O	

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 other applications (eg, GSM SIM) MUST support logical channels.	11.3.2	O	WIM-ICC-105
WIM-ICC-105	ICC commands MANAGE CHANNEL MANAGE CHANNEL MUST be supported by an ICC that supports multiple applications.	11.3.2	O	
WIM-ICC-106	ICC commands VERIFY	11.3.4.1	M	
WIM-ICC-107	ICC commands DISABLE VERIFICATION	11.3.4.2	O	
WIM-ICC-108	ICC commands ENABLE VERIFICATION	11.3.4.3	O	
WIM-ICC-109	ICC commands CHANGE REFERENCE DATA	11.3.4.4	M	
WIM-ICC-110	ICC commands RESET RETRY COUNTER	11.3.4.5	M	
WIM-ICC-111	ICC commands SELECT	11.3.5.1	M	
WIM-ICC-112	ICC commands READ BINARY	11.3.5.2	M	
WIM-ICC-113	ICC commands UPDATE BINARY	11.3.5.3	M	
WIM-ICC-114	ICC commands MANAGE SECURITY ENVIRONMENT	11.3.6.1	M	
WIM-ICC-115	ICC commands PERFORM SECURITY OPERATION (all but Key Transport and Key Agreement)	11.3.6.4, 11.3.6.7, 11.3.6.8, 11.3.6.9, 11.3.6.10	M	WIM-ICC-130 OR WIM-ICC-131
WIM-ICC-130	ICC commands PERFORM SECURITY OPERATION Key Transport	11.3.6.4, 11.3.6.5	O	
WIM-ICC-131	ICC commands PERFORM SECURITY OPERATION Key Agreement	11.3.6.4, 11.3.6.6	O	
WIM-ICC-116	ICC commands ASK RANDOM	11.3.6.12	M	
WIM-ICC-117	ICC commands GET RESPONSE	11.3.7.1	M	
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	O	
WIM-ICC-120	ID-000 (Plug-in)	11.1	O	

Item	Function	Reference	Status	Requirement
WIM-ICC-121	Transmission protocols T=0	11.2	M	
WIM-ICC-122	Transmission protocols T=1	11.2	O	
WIM-ICC-123	Supply voltage; indicated in ATR 3 V	11.2	M	
WIM-ICC-124	Supply voltage; indicated in ATR 5 V	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	O	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	O	WIM-C-025 OR WIM-C-027
WIM-C-003	Generic (application level) functionality Unwrap (decipher) a key	6,2,1	O	WIM-C-026 OR WIM-C-028
WIM-C-004	Data storage PKCS#15 ODF	9.4.1	M	
WIM-C-005	Data storage PKCS#15 TokenInfo	9.4.7	M	
WIM-C-006	Data storage PKCS#15 PrKDF	9.4.2	M	
WIM-C-007	Data storage PKCS#15 PuKDF	9.4.3	O	
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	O	
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	M	

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

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

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	O	WIM-C-104
WIM-C-104	ICC commands MANAGE CHANNEL	11.3.2	O	
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 RESET RETRY COUNTER	11.3.4.5	M	
WIM-C-110	ICC commands SELECT	11.3.5.1	M	
WIM-C-111	ICC commands READ BINARY	11.3.5.2	M	
WIM-C-112	ICC commands UPDATE BINARY	11.3.5.3	M	
WIM-C-113	ICC commands MANAGE SECURITY ENVIRONMENT	11.3.6.1	M	
WIM-C-114	ICC commands PERFORM SECURITY OPERATION	11.3.6.4	M	
WIM-C-114	ICC commands PERFORM SECURITY OPERATION (all but Key Transport and Key Agreement)	11.3.6.4, 11.3.6.7, 11.3.6.8, 11.3.6.9, 11.3.6.10	M	WIM-C-130 OR WIM-C-131
WIM-C-130	ICC commands PERFORM SECURITY OPERATION Key Transport	11.3.6.4, 11.3.6.5	O	
WIM-C-131	ICC commands PERFORM SECURITY OPERATION Key Agreement	11.3.6.4, 11.3.6.6	O	
WIM-C-115	ICC commands ASK RANDOM	11.3.6.12	O	
WIM-C-116	ICC commands GET RESPONSE	11.3.7.1	M	
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	O	
WIM-C-119	ID-000 (Plug-in)	11.1	O	
WIM-C-120	Transmission protocols T=0	11.2	M	
WIM-C-121	Transmission protocols T=1	11.2	O	
WIM-C-122	Supply voltage, SIM card 3 V	11.2	M	
WIM-C-123	Supply voltage, SIM card 5 V	11.2	O	
WIM-C-124	Supply voltage, external card 3 V	11.2	M	
WIM-C-125	Supply voltage, external card 5 V	11.2	O	
WIM-C-126	Support access control rules	12.2	M	