Specification Information Note

WAP-198_103-WIM-20010214-a

Version 14-Feb-2001

for

Wireless Application Protocol
WAP-198-WIM-20000218-a

Wireless Identity Module Specification
Version 18-Feb-2000

This document is considered confidential and may not be disclosed in any manner to any non-member of the WAP Forum™, unless there has been prior explicit Board approval.

This document is a work in process and is not an approved WAP Forum™ specification. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the WAP Forum specifications.

© 2001, Wireless Application Protocol Forum, Ltd. All Rights Reserved. Terms and conditions of use are available from the WAP Forum™ Web site (http://www.wapforum.org/what/copyright.htm).

© 2001, Wireless Application Protocol Forum, Ltd. All rights reserved.

Terms and conditions of use are available from the WAP Forum™ 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 WAP Forum™. The WAP Forum 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 WAP Forum™ assumes no responsibility for errors or omissions in this document. In no event shall the WAP Forum 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.wapforum.org/.

Known problems associated with this document are published at http://www.wapforum.org/.

Comments regarding this document can be submitted to the WAP Forum™ in the manner published at http://www.wapforum.org/.

Contents

1. SCOPE **4**

2. NOTATION **4**

3. INCLUSION OF INTER-SPECIFICATION DEPENDENCIES & EDITORIAL CORRECTIONS **5**

3.1 CHANGE CLASSIFICATION 5
3.2 CHANGE SUMMARY 5
3.3 CHANGE DESCRIPTION 5

4. ADD REFERENCE DESCRIBING THE SCR SYNTAX **11**

4.1 CHANGE CLASSIFICATION 11
4.2 CHANGE SUMMARY 11
4.3 CHANGE DESCRIPTION 11

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

1. Scope

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

- WAP-198-WIM-20000218-a

It includes changes from the following change requests:

- WIM-Nokia-Interspec SCR Format

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.

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

3. Inclusion of Inter-specification dependencies and editorial corrections.

3.1 Change Classification

Class 3 – Clerical Corrections

3.2 Change Summary

Inclusion of inter-specification dependencies. Editoria corrections.

3.3 Change Description

Editor's note: Replace 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	Subfunction	Reference	Status	Requirement
WIM-001	WTLS supported		6.1	M	
WIM-002	Generic (application level) functionality	Signing of hash	6.2.2	M	WIM-023 OR WIM-025
WIM-003		Unwrap (decipher) a key	6.2.1	O	WIM-024 OR WIM-026
WIM-004	Data storage	PKCS#15 ODF	9.4.1	M	
WIM-005		PKCS#15 TokenInfo	9.4.7	M	
WIM-006		PKCS#15 PrKDF	9.4.2	M	
WIM-007		PKCS#15 PuKDF	9.4.3	O	
WIM-008		PKCS#15 CDF	9.4.4	M	
WIM-009		PKCS#15 CDF trusted certificates	9.4.4	O	
WIM-090		PKCS#15 CDF useful certificates	9.4.4	O	
WIM-010		PKCS#15 AODF	9.4.6	M	
WIM-011		PKCS#15 DODF	9.4.5	M	
WIM-012		PKCS#15 UnusedSpace	9.4.8	M	
WIM-013		Private key, use by ME	9.4.2	M	
WIM-014		Public key, read by ME	9.4.3	O	
WIM-015		Certificate, read by ME	9.4.4	M	
WIM-016		Certificate, store by ME	9.4.4	M	
WIM-017		WTLS Peers	9.4.10	M	
WIM-018		WTLS Sessions	9.4.11	M	

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

WIM-019	Random number generation		6.1	M	
WIM-020	WTLS key exchange algoritms; at least one supported		8	M	WIM-021 OR WIM-022
WIM-021		RSA	8.1	O	WIM-028
WIM-022		ECDH	8.2	O	WIM-030 OR WIM-032
WIM-023	Genereric (application level) algorithms. Either RSA or ECC MUST be supported. In case of ECC, ECDSA MUST be supported; ECES SHOULD be supported.	RSA signing	6.2.2	O	WIM-028
WIM-024		RSA decryption	6.2.1	O	WIM-028
WIM-025		ECDSA signing	6.2.2	O	WIM-030 OR WIM-032
WIM-026		ECES decryption	6.2.1	O	WIM-030 OR WIM-032
WIM-027	WTLS pseudo-random function based on SHA-1		7.2.4.6, 7.2.4.7	M	
WIM-028	RSA modulus length (bits), when RSA supported	Minimum 1024	12.1.1	O	
WIM-030	ECC basic curves; if ECC is used, at least one MUST be supported	Curve 5 (163 bits)	WTLS App. A	O	
WIM-032		Curve 7 (160 bits)	WTLS App. A	O	
WIM-033	ECC non-basic curves	Curve 1 (113 bits)	WTLS App. A	O	
WIM-034		Curve 3 (163 bits)	WTLS App. A	O	
WIM-029		Curve 4 (113 bits)	WTLS App. A	O	
WIM-031		Curve 6 (112 bits)	WTLS App. A	O	
WIM-035		Curve 8 (112 bits)	WTLS App. A	O	
WIM-036		Curve 9 (160 bits)	WTLS App. A	O	
WIM-037	Private keys Note: keys in colums mean separate keys	Authentication key (MAY be used for decryption, too)	12.1.1	M	
WIM-038		Decryption key (application level)	12.1.1	O	
WIM-039		Non-repudiation key (application level)	12.1.1	M	
WIM-040	PIN handling	Recommended PIN format	12.1.4.1	M	
WIM-041	Digital signature verification	RSA	7.2.4.2	O	
WIM-042		ECDSA	7.2.4.2	O	

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

14.1.2 WIM ICC Options

Item	Function	Subfunction	Reference	Status	Requirement
WIM-101	Application selection; at least one method supported		11.3.3	M	
WIM-102		Direct application selection	11.3.3.1	M	
WIM-103		(Subfunction removed)			
WIM-104	Logical channels. WIM ICC that supports also some other applications (eg, GSM SIM) MUST support logical channels.		11.3.2	O	WIM-105
WIM-105	ICC commands MANAGE CHANNEL MUST be supported by ICC that supports multiple applications.	MANAGE CHANNEL	11.3.2	O	
WIM-106		VERIFY	11.3.4.1	M	
WIM-107		DISABLE VERIFICATION	11.3.4.2	O	
WIM-108		ENABLE VERIFICATION	11.3.4.3	O	
WIM-109		CHANGE REFERENCE DATA	11.3.4.4	M	
WIM-110		RESET RETRY COUNTER	11.3.4.5	M	
WIM-111		SELECT	11.3.5.1	M	
WIM-112		READ BINARY	11.3.5.2	M	
WIM-113		UPDATE BINARY	11.3.5.3	M	
WIM-114		MANAGE SECURITY ENVIRONMENT	11.3.6.1	M	
WIM-115		PERFORM SECURITY OPERATION	11.3.6.4	M	
WIM-116		ASK RANDOM	11.3.6.12	M	
WIM-117		GET RESPONSE	11.3.7.1	M	
WIM-118	ICC size; at least one supported		11.1	M	WIM-119 OR WIM-120
WIM-119		ID-1	11.1	O	
WIM-120		ID-000 (Plug-in)	11.1	O	
WIM-121	Transmission protocols	T=0	11.2	M	
WIM-122		T=1	11.2	O	
WIM-123	Supply voltage	3 V	11.2	M	
WIM-124		5 V	11.2	O	

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

14.2 ME Options

14.2.1 General ME Options

Item	Function	Subfunction	Reference	Status	Requirement
WIMME-001	WTLS		[WAP WTLS]	O	WIMME-019 AND WIMME-020 AND WIMME-022 AND WIMME-039
WIMME-002	Generic (application level) functionality	Signing of hash	6.2.2	O	WIMME-025 OR WIMME-027
WIMME-003		Unwrap (decipher) a key	6,2,1	O	WIMME-026 OR WIMME-028
WIMME-004	Data storage	PKCS#15 ODF	9.4.1	M	
WIMME-005		PKCS#15 TokenInfo	9.4.7	M	
WIMME-006		PKCS#15 PrKDF	9.4.2	M	
WIMME-007		PKCS#15 PuKDF	9.4.3	O	
WIMME-008		PKCS#15 CDF	9.4.4	M	
WIMME-009		PKCS#15 CDF trusted certificates	9.4.4	M	
WIMME-090		PKCS#15 CDF useful certificates	9.4.4	M	
WIMME-010		PKCS#15 AODF	9.4.6	M	
WIMME-011		PKCS#15 DODF	9.4.5	M	
WIMME-012		PKCS#15 UnusedSpace	9.4.8	M	
WIMME-013		Use private key	9.4.2	M	
WIMME-014		Read public key	9.4.3	O	
WIMME-015		Read user certificate	9.4.4	M	
WIMME-016		Store user certificate	9.4.4	M	
WIMME-017		Read CA certificate	9.4.4	M	
WIMME-018		Store CA certificate	9.4.4	M	
WIMME-019		WTLS Peers	9.4.10	O	
WIMME-020		WTLS Sessions	9.4.11	O	
WIMME-021	Use of random numbers generated by the WIM		6.1	O	
WIMME-022	WTLS key exchange algoritms; at least one supported		8	O	WIMME-023 OR WIMME-024
WIMME-023		RSA based	8.1	O	WIMME-029 AND WIMME-030
WIMME-024		ECDH based	8.2	O	WIMME-029 AND (WIMME-032 OR WIMME-034)

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

WIMME-025	Generic (application level) algorithms	RSA signing	6.2.2	O	WIMME-030
WIMME-026		RSA decryption	6.2.1	O	WIMME-030
WIMME-027		ECDSA signing	6.2.2	O	WIMME-032 OR WIMME-034
WIMME-028		ECES decryption	6.2.1	O	WIMME-032 OR WIMME-034
WIMME-029	Use WTLS pseudo-random function based on SHA-1		7.2.4.6, 7.2.4.7	O	
WIMME-030	Expected RSA modulus length (bits) for signing performed in WIM, when RSA supported	Minimum 1024	12.11	O	
WIMME-032	ECC basic curves; if ECC is used, at least one MUST be supported	Curve 5 (163 bits)	WTLS App. A	O	
WIMME-034		Curve 7 (160 bits)	WTLS App. A	O	
WIMME-035	ECC non-basic curves	Curve 1 (113 bits)	WTLS App. A	O	
WIMME-036		Curve 3 (163 bits)	WTLS App. A	O	
WIMME-031		Curve 4 (113 bits)	WTLS App. A	O	
WIMME-033		Curve 6 (112 bits)	WTLS App. A	O	
WIMME-037		Curve 8 (112 bits)	WTLS App. A	O	
WIMME-038		Curve 9 (160 bits)	WTLS App. A	O	
WIMME-039	Use private keys for a particular purpose	Use authentication key for WTLS client authentication	12.1.1	O	
WIMME-040		Use authentication key for decryption	12.1.1	O	
WIMME-041		Use decryption key (application level)	12.1.1	O	
WIMME-042		Use non-repudiation key (application level)	12.1.1	O	
WIMME-043	PIN handling	Recommended PIN format	12.1.4.1	M	
WIMME-044	Use WIM for digital signature verification	RSA	7.2.4.2	O	
WIMME-045		ECDSA	7.2.4.2	O	

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

14.2.2 ME Use of WIM ICC

Item	Function	Subfunction	Reference	Status	Requirement
WIMME-101	Application seletion	Direct application selection	11.3.3.1	M	
WIMME-102		(Subfunction removed)			
WIMME-103	Logical channels. ME that uses some other application (eg, GSM SIM) of ICC WIM, MUST support logical channels.		11.3.2	O	WIMME-104
WIMME-104	ICC commands	MANAGE CHANNEL	11.3.2	O	
WIMME-105		VERIFY	11.3.4.1	M	
WIMME-106		DISABLE VERIFICATION	11.3.4.2	M	
WIMME-107		ENABLE VERIFICATION	11.3.4.3	M	
WIMME-108		CHANGE REFERENCE DATA	11.3.4.4	M	
WIMME-109		RESET RETRY COUNTER	11.3.4.5	M	
WIMME-110		SELECT	11.3.5.1	M	
WIMME-111		READ BINARY	11.3.5.2	M	
WIMME-112		UPDATE BINARY	11.3.5.3	M	
WIMME-113		MANAGE SECURITY ENVIRONMENT	11.3.6.1	M	
WIMME-114		PERFORM SECURITY OPERATION	11.3.6.4	M	
WIMME-115		ASK RANDOM	11.3.6.12	O	
WIMME-116		GET RESPONSE	11.3.7.1	M	
WIMME-117	ICC size; at least one supported		11.1	M	WIMME-118 OR WIMME-119
WIMME-118		ID-1	11.1	O	
WIMME-119		ID-000 (Plug-in)	11.1	O	
WIMME-120	Transmission protocols	T=0	11.2	M	
WIMME-121		T=1	11.2	O	
WIMME-122	Supply voltage, SIM card	3 V	11.2	M	
WIMME-123		5 V	11.2	O	
WIMME-124	Supply voltage, external card	3 V	11.2	M	
WIMME-125		5 V	11.2	O	

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

4. Add reference describing the SCR syntax.

4.1 Change Classification

Class 3 – Clerical Corrections

4.2 Change Summary

Add reference describing the SCR syntax.

4.3 Change Description

Editor's note: In 3.1, add reference

[WAPCREQ] "Specification of WAP Conformance Requirements", WAP-221-CREQ, WAP Forum Ltd, URL:http//www.wapforum.org/"

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved