Specification Information Note

WAP-198_100-WIM-20000630-a

Approved Version 30-June-2000

for

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

Wireless Identity Module Specification
Version 18-Feb-2000

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.

This document is not a WAP Forum™ specification, is not endorsed by the WAP Forum and is informative only. 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.

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 **5**

3. PSO-DECIPHER PADDING INDICATOR BYTE **6**

3.1 CHANGE CLASSIFICATION 6
3.2 CHANGE SUMMARY 6
3.3 CHANGE DESCRIPTION 6

4. MSE - SET P1 BYTE **8**

4.1 CHANGE CLASSIFICATION 8
4.2 CHANGE SUMMARY 8
4.3 CHANGE DESCRIPTION 8

5. STATUS WORDS **9**

5.1 CHANGE CLASSIFICATION 9
5.2 CHANGE SUMMARY 9
5.3 CHANGE DESCRIPTION 9

6. EC ENCRYPTION SCHEME **12**

6.1 CHANGE CLASSIFICATION 12
6.2 CHANGE SUMMARY 12
6.3 CHANGE DESCRIPTION 12

7. ECDSA SIGNATURE FORMAT **13**

7.1 CHANGE CLASSIFICATION 13
7.2 CHANGE SUMMARY 13
7.3 CHANGE DESCRIPTION 13

8. PIN USAGE **14**

8.1 CHANGE CLASSIFICATION 14
8.2 CHANGE SUMMARY 14
8.3 CHANGE DESCRIPTION 14

9. TAGS FOR DATA OBJECTS **15**

9.1 CHANGE CLASSIFICATION 15
9.2 CHANGE SUMMARY 15
9.3 CHANGE DESCRIPTION 15

10. RSA PUBLIC KEY FORMAT **16**

10.1 CHANGE CLASSIFICATION 16
10.2 CHANGE SUMMARY 16
10.3 CHANGE DESCRIPTION 16

11. TAG FOR A FILE PATH **17**

11.1 CHANGE CLASSIFICATION 17
11.2 CHANGE SUMMARY 17
11.3 CHANGE DESCRIPTION 17

12. TYPOS **18**

12.1 CHANGE CLASSIFICATION 18
12.2 CHANGE SUMMARY 18
12.3 CHANGE DESCRIPTION 18

13. NOTE ABOUT READING DIR FILE **20**

13.1 CHANGE CLASSIFICATION 20
13.2 CHANGE SUMMARY 20
13.3 CHANGE DESCRIPTION 20

© 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
  - Corrections regarding ISO7816 compliance and status words
  - Clarifications regarding ECC object format
  - Clarifications regarding PIN management
  - Clerical editorial corrections

It includes changes from the following change requests:

- WIM-Telstra-LA-1 - PSO-DECIPHER Padding Indicator Byte
- WIM-Telstra-LA-2 - MSE – SET P1 byte
- WIM-Telstra-LA-3 - ECDSA signature format
- WIM-Telstra-LA-4 - EC encryption scheme
- WIM-Telstra-LA-5 - Typos
- WIM-Bull-LA-1 - Public Key format
- WIM-Bull-LA-3 - Tags for data Object
- WIM-Schlumberger-LA-1 - Typos, corrections
- WIM-Nokia-LA-1 - PIN usage
- WIM-Nokia-Miami-1 - Note about reading DIR file

Affected Sections

This Specification Information Note modifies the following specification sections:

- 3.1 Normative References
- 4.2 Abbreviations
- 5 Architectural Overview
- 9.3 ISO Object Identifiers
- 9.4.1 EE(ODF)
- 10.3.2 WIM_GENERIC_ECC Security Environment
- 11.3 Description of Card Commands
- 11.3.5 Operations Related to Data Storage
- 11.3.6 Cryptographic Operations
- 11.3.8 Status Words

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

- 11.4.4 Perform WTLS RSA Handshake
- 11.4.5 Perform WTLS ECDH_ECDSA Handshake
- 11.4.6 Perform Application Level Signature
- 11.4.7 Perform Application Related Deciphering
- 12.3 Attribute Formats
- 13.5 Usage of Pins
- 14.1.1 General WIM Options

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. PSO-DECIPHER Padding Indicator Byte

3.1 Change Classification

Class 2 – Bug Fixes

3.2 Change Summary

A padding indicator byte of ‘00’ is prepended to cryptograms, to be compatible with ISO7816.

3.3 Change Description

In 11.3.6 “Cryptographic Operations”, append the following sentence to the Value in Table 3 for Tag 86:

The padding indicator byte is ‘00’ for asymmetric key operations.

In 11.3.6.5 “PSO – ENCIPHER, Key Transport”, change the P1 field in the Command APDU to:

86 (padding indicator byte followed by cryptogram)

In 11.3.6.5 “PSO – ENCIPHER, Key Transport”, change the Data field in the Response APDU to:

Padding indicator byte ‘00’ + RSA encrypted data. PKCS #1 block type 2 is used.

In 11.3.6.7 “PSO – DECIPHER, Application Level”, change the P2 field in the Command APDU to:

86 (padding indicator byte followed by cryptogram)

In 11.3.6.7 “PSO – DECIPHER, Application Level”, change the Data field in the Command APDU to:

Padding indicator byte ‘00’ + data to be deciphered (encrypted message key)

In 11.4.4 “Perform WTLS RSA handshake”, change the last paragraph in the “Establish pre-master secret” section as follows:

The card keeps the original value (client version and 19 random bytes) and returns the padding indicator byte ‘00’ followed by the encrypted value. The encrypted value is ~~to be~~ transmitted to the server. The pre-master secret is the original value concatenated with KPubServer.

In 11.4.7 “Perform Application Related Deciphering”, change the Data field of the PSO command to:

Command	**CLA**	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**
PSO	8X	2A	80	86	XX	00 + WrappedKey	YY

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

In 11.4.7 "Perform Application Related Deciphering", Add a sentence after the PSO command table:

The padding indicator byte is '00'.

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

4. MSE – SET P1 Byte

4.1 Change Classification

Class 2 – Bug Fixes

4.2 Change Summary

According to ISO7816-8, the P1 byte of the MSE - SET command APDU should be 41 for deciphering and signing, and 81 for enciphering and verification.

4.3 Change Description

In 11.3.6.3 "MSE – SET", change the P1 table entry to:

P1	41 for computation (signing) and deciphering, 81 for enciphering and verification

In 11.4.4 "Perform WTLS RSA handshake", in the "Establish pre-master secret" section change the P1 table entry in the MSE-SET command from 41 *to* 81.

In 11.4.5 "Perform WTLS ECDH_ECDSA Handshake", change the P1 table entry in the MSE-SET command from 41 *to* 81.

In 11.4.7 "Perform Application Related Deciphering", change the P1 table entry in the MSE-SET command from 81 *to* 41.

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

5. Status Words

5.1 Change Classification

Class 2 – Bug Fixes

5.2 Change Summary

Status words defined to cover errors regarding

- closing a logical channel
- unblocking PIN (RESET RETRY COUNTER) when it is no more allowed
- verification or enabling/disabling verification requirement when in contradiction with PIN status
- performing security operation with invalid master secret reference

5.3 Change Description

In 11.3.8 "Status Words", change the table as follows:

SW1 **SW2**	**Applicable for Commands**	Description	**ISO7816 Description**
61XX	All	Normal ending of the command (data of length XX to be recovered by GET RESPONSE). Note that this status is related to the TPDU level.	Normal processing, SW2 indicates the number of response bytes still available
6200	MANAGE CHANNEL Open/Close	Cannot open or close a ~~new~~ logical channel	No information given
6300	VERIFY DISABLE VERIFICATION ENABLE VERIFICATION CHANGE REFERENCE DATA RESET RETRY COUNTER	PIN verification failed	Verification failed
6581	All	Memory failure (eg, data corrupted)	Memory failure
6600	MSE Restore	Security environment cannot be set	The environment cannot be set or modified [ISO7816-8]
	MSE Set PSO	No security environment set or template cannot be set	
6700	All	Lack of Lc, Data, or Le; Unexpected Lc, Data, or Le;	Wrong length

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

		Length rejected by the command	
6982	MSE PSO	PIN not verified	Security status not satisfied
	READ BINARY UPDATE BINARY	Access rights not fulfilled	
6983	VERIFY DISABLE VERIFICATION ENABLE VERIFICATION CHANGE REFERENCE DATA RESET RETRY COUNTER	PIN blocked	Authentication method blocked
6985	VERIFY DISABLE VERIFICATION ENABLE VERIFICATION	In contradiction with PIN status	Condition of use not satisfied
	MSE Derive Key	Pre-master secret not ready	
	PSO GET RESPONSE	Internal data not ready	
6986	READ BINARY UPDATE BINARY	No current EF	No current EF
6A80	MSE Set MSE Derive key	Incorrect tag	Incorrect parameters in data field
	PSO	Incorrect data	
6A82	SELECT Application	Application not found	File not found
	SELECT File	File not found	
	PSO	Key file not found	
	VERIFY	PIN file not selected or found	
6A88	PSO	Private key or master secret reference not found	Referenced data not found
	VERIFY	PIN reference not found	
6B00	All	Incorrect parameters P1-P2	Wrong parameters P1-P2
6CXX	GET RESPONSE	Length error, the length that MUST be used is XX	Wrong length Le
6D00	All	Unknown INS byte	Instruction code not supported or

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

			invalid
6E00	All	Unknown CLA byte	Class not supported
	Commands with CLA = 8X	Using any CLA = 8X command before selecting the application	
6F00	All	Technical problem with no diagnostic given	No precise diagnosis
9000	All	Normal ending of the command	Normal processing

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

6. EC Encryption Scheme

6.1 Change Classification

Class 3 – Clerical Corrections

6.2 Change Summary

Replace ECES with ECIES (Elliptic Curve Integrated Encryption Scheme), according to the new version of P1363.

6.3 Change Description

In 3.1 "Normative References", replace the [P1363] reference with the following:

[P1363] "Standard Specifications for Public Key Cryptography", IEEE P1363 / D13 (Draft Version 13), 12 November 1999. URL: http://grouper.ieee.org/groups/1363/

In 3.1 "Normative References", add a reference to P1363a as follows:

[P1363a] "Standard Specifications for Public Key Cryptography: Additional Techniques", IEEE P1363a / D4 (Draft Version 4), 22 May 2000. URL: http://grouper.ieee.org/groups/1363/

In 4.2"Abbreviations", replace the ECES abbreviation with one for ECIES:
ECIES Elliptic Curve Integrated Encryption Scheme

In 10.3.2 "WIM_GENERIC_ECC Security Environment", replace "ECSA for PSO-Decipher" with "ECIES for PSO-Decipher".

In 10.3.2 "WIM_GENERIC_ECC Security Environment", append the following sentence:
ECIES is specified in [P1363a].

*In 11.4.7 "Perform Application Related Deciphering", change "*ECES*" to "*ECIES*" in the first sentence.*

*In 14.1.1 "General WIM Options", change both occurrences of "*ECES*" to "*ECIES*" in row WIM-026.*

*In 14.1.1 "General ME Options", change "*ECES*" to "*ECIES*" in row WIMME-028.*

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

7. ECDSA Signature Format

7.1 Change Classification

Class 3 – Clerical Corrections

7.2 Change Summary

Explicit description of ECDSA signature format. Also, updated reference to X9.62.

7.3 Change Description

In 3.1 "Normative References", replace the X.92 reference with the following:

[X9.62] "The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62 – 1998 (Approved: January 7, 1999).

In 11.3.6.8 "PSO – COMPUTE DIGITAL SIGNATURE", modify the last paragraph in the "Description" section as follows:

For ECDSA, signing is performed according to [X9.62]. The signature is returned as ~~an octet string~~ the concatenation or *r* and *s*, each represented most significant byte first using the same number of octets as are required to represent *n* (the order of the base point).

In 11.4.6 "Perform Application Level Signature", modify the last sentence of the last paragraph as follows:
For a 163 bit ECC key, it is 42 bytes (concatenation of *r* and *s*, each 21 bytes~~ the signature if formatted according to [X9.62], octet string format~~).

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

8. PIN Usage

8.1 Change Classification

Class 3 – Clerical Corrections

8.2 Change Summary

Clarify usage of PIN-G regarding digital signatures.

8.3 Change Description

In 13.5 "Usage of PINs", change as follows:

The first object in the AODF is considered as a General PIN (PIN-G). If not otherwise indicated, all files (eg, CDF, PrKDF) are write-protected with this PIN. Obviously, EF(ODF) and EF(AODF) SHOULD be readable without a PIN verification. (Note: according to 12.2, files like CDF, PrKDF, DODF and certificate files should be readable without entering a PIN.)

In a typical case, the PIN-G is used to protect all files (which need to be protected) and keys except non-repudiation keys. If the PIN-G is not disabled, the ME must send the PIN-G after the WIM application is selected, in order to be able to use keys and perform other operations that require the PIN-G. More precisely, the ME SHOULD do the following when the secure functions are required the first time

1. Open a logical channel, if logical channels are used
2. Select the WIM application
3. Read EF(TokenInfo)
4. Read EF(ODF)
5. Read EF(AODF)
6. Read the information about PIN-G
7. Find out if PIN-G is enabled
8. Enter the PIN-G (if operations requiring PIN-G are used)

The ME does not need to send the PIN-G, unless or before protected operations are performed. E.g. the ME may read files that are readable without a PIN. Also, PIN-G need not be sent before using non-repudiation keys, since they are protected with a separate PIN.

After the PIN-G is entered, it remains valid until the logical channel is closed. The ME SHOULD close the logical channel when the secure functions are no more required. When the logical channel is opened again, the PIN will be required. If logical channels are not supported, the ME SHOULD reset the card in order to validate the PIN.

Note that a non-repudiation key is protected with a non-repudiation PIN (PIN-NR). If there are several non-repudiation keys, then each key MUST be protected with a separate PIN-NR. However, it is anticipated that there is only a single non-repudiation key and the corresponding PIN-NR.

When the user is asked to enter PIN-G or PIN-NR, it should be made clear to the user that the PIN entry procedure is safe and the entered PIN is not going to be sent across the network. Under any circumstances the entered PIN (PIN-G, PIN-NR) MUST NOT be sent to the WAE.

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

9. Tags for Data Objects

9.1 Change Classification

Class 3 – Clerical Corrections

9.2 Change Summary

Add a missing ISO7816 tag definition.

9.3 Change Description

In 11.3.6 "Cryptographic Operations", Table 3 "Tags for Data Objects", add the following row:

A8	Input template for DS verification

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

10. RSA Public Key Format

10.1 Change Classification

Class 3 – Clerical Corrections

10.2 Change Summary

Add an explicit definition of the RSA public key format.

10.3 Change Description

In 11.4.4 "Perform WTLS RSA Handshake", "Verify server certificate", add:

Note that KPubCA is the public key of the CA, formatted according to [WAPWTLS]:

KPubCA = ExpLength(2 bytes) + Exponent + ModLength (2 bytes) + Modulus.

In 11.4.4 "Perform WTLS RSA Handshake", "Establish pre-master secret", add:

Note that KPubServer is the public key of the server, formatted according to [WAPWTLS]:

KPubServer = ExpLength(2 bytes) + Exponent + ModLength (2 bytes) + Modulus

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

11. Tag for a File Path

11.1 Change Classification

Class 3 – Clerical Corrections

11.2 Change Summary

Add the ISO7816 tag 81 to the CRDO table in section 11.3.6.

11.3 Change Description

In 11.3.6 "Cryptographic Operations", Table 4 "Control Reference Data Objects", add the following row:

81	File path (used for indicating the private key file path)	B6 (DST) B8 (CT Asym)

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

12. Typos

12.1 Change Classification

Class 3 – Clerical Corrections

12.2 Change Summary

Typo Corrections.

12.3 Change Description

In 5 "Architectural Overview", 3rd paragraph, 1st sentence:

format on a cryptographic token

In 9.3 "ISO Object Identifiers":

joint-iso-itu-t(2)

In 9.4.1 "EF(ODF)":

{ wap-wsg-3 } to { wap-wsg 3 }

In 9.4.1 "EF(ODF)":

OCTET STRING : '3F00 5015'H

In 11.3.5.1 "SELECT FILE":

but other data objects could be provided.

In 11.3.6.2 "MSE – RESTORE":

mentio~~n~~ned

In 11.4.4 "Perform WTLS RSA Handshake", "Restore the Security Environment", change to:

The EF TokenInfo indicates the SE number to be used for the WTLS_RSA SE. If not already done in a previous handshake, the SE must be restored using ~~PSO-RESTORE~~ MSE-RESTORE.

In 11.4.7 "Perform Application Related Deciphering", change to:

The ME sets the key reference for the private key in the ~~DST~~ CT of the current SE. Also the file path of the key, if not the current one, needs to be indicated.

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

In 12.3 Attribute Format:

within ~~a~~ the same file

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

13. Note about Reading DIR File

13.1 Change Classification

Class 3 – Clerical Corrections

13.2 Change Summary

Remove note about reading DIR file. This note is irrelevant for WIM, since the only used application selection is the direct method.

READ BINARY is only used after selecting the WIM application, so the option for using CLA=0X is not used.

13.3 Change Description

In 11.3 "Description of Card Commands", Table 1 "Card commands", change table row "READ BINARY" as follows:

READ BINARY	~~0X /~~ 8X	B0	[ISO7816-4]

In 11.3 "Description of Card Commands", change as follows:

In the CLA byte, the X denotes the logical channel number. For SELECT, CLA=0X is used of for selecting an application (direct application selection with AID), and CLA=8X for selecting a file. ~~For selecting and reading the EF(DIR), the value 0X SHOULD be used. After the WIM application is selected, the value 8X SHOULD be used.~~

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