Specification Information Note

WAP-198_102-WIM-20001227-a

Version 27-Dec-2000

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 **5**

2. NOTATION **5**

3. WIM PIN-G USEAGE .....

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

4. SERVER KEY EXPONENT LENGTH RESTRICTION FOR SMART CARD WIM **7**

4.1 CHANGE CLASSIFICATION 7
4.2 CHANGE SUMMARY 7
4.3 CHANGE DESCRIPTION 7

5. WIM STATUS WORDS DESCRIPTION CLARIFICATION **9**

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

6. TYPOS **10**

6.1 CHANGE CLASSIFICATION 10
6.2 CHANGE SUMMARY 10
6.3 CHANGE DESCRIPTION 10

7. CLARIFICATION ON KEY GENERATION **13**

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

8. CLARIFICATION RE LOGICAL RECORD LENGTHS **14**

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

9. RECOMMENDED PIN TYPE **15**

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

10. LE VALUE FOR SELECT FILE COMMAND **16**

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

11. CLARIFICATION ON TRUSTED CDF UPDATES **17**

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

12. INCORRECT PRKDF FIELD **18**

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

13. MISSING FUNCTIONS IN TABLE **19**

13.1 CHANGE CLASSIFICATION 19
13.2 CHANGE SUMMARY 19
13.3 CHANGE DESCRIPTION 19

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

14. MULTIPLE EF(AODF) FILES 20
14.1 CHANGE CLASSIFICATION 20
14.2 CHANGE SUMMARY 20
14.3 CHANGE DESCRIPTION 20
15. CHANGE REFERENCE DATA LENGTHS 21
15.1 CHANGE CLASSIFICATION 21
15.2 CHANGE SUMMARY 21
15.3 CHANGE DESCRIPTION 21
16. STATUS WORD TABLE 22
16.1 CHANGE CLASSIFICATION 22
16.2 CHANGE SUMMARY 22
16.3 CHANGE DESCRIPTION 22
17. SESSIONS AND PEERS DATA OBJECTS 23
17.1 CHANGE CLASSIFICATION 23
17.2 CHANGE SUMMARY 23
17.3 CHANGE DESCRIPTION 23
18. FIXED LENGTH DATA ITEMS 24
18.1 CHANGE CLASSIFICATION 24
18.2 CHANGE SUMMARY 24
18.3 CHANGE DESCRIPTION 24
19. MASTER SECRET KEY REFERENCES 25
19.1 CHANGE CLASSIFICATION 25
19.2 CHANGE SUMMARY 25
19.3 CHANGE DESCRIPTION 25
20. STATUS WORD IN VERIFY WITH AN EMPTY BODY 27
20.1 CHANGE CLASSIFICATION 27
20.2 CHANGE SUMMARY 27
20.3 CHANGE DESCRIPTION 27
21. CURRENT CONSUMPTION 28
21.1 CHANGE CLASSIFICATION 28
21.2 CHANGE SUMMARY 28
21.3 CHANGE DESCRIPTION 28
22. SIGNATURE VERIFICATION IN GENERIC SECURITY ENVIRONMENT 29
22.1 CHANGE CLASSIFICATION 29
22.2 CHANGE SUMMARY 29
22.3 CHANGE DESCRIPTION 29

© 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-Slb-HK-01	WIM PIN-G usage
WIM-OCS-Munich-02	Server key exponent length restriction for smart card WIM
WIM-OCS-Munich-01	WIM status words description clarification
WIM-Motorola-Munich-01	Typos
WIM-Motorola-Munich-18	Clarification on key generation
WIM-Motorola-Munich-04	Clarification re logical record lengths
WIM-Motorola-Munich-05	Recommeded PIN type
WIM-Motorola-Munich-06	Le value for Select File command
WIM-Motorola-Munich-07	Clarification on trusted CDF updates
WIM-Motorola-Munich-08	Incorrect PrKDF field
WIM-Motorola-Munich-21	Missing functions in table
WIM-Motorola-Munich-10	Multiple EF(AODF) files
WIM-Motorola-Munich-11	Change reference data lengths
WIM-Motorola-Munich-12	Status word table
WIM-Motorola-Munich-19	Sessions and Peers data objects
WIM-Motorola-Munich-14	Fixed length data items
WIM-Motorola-Munich-16	Master secret key references
WIM-Nokia-Munich-01	Status word in VERIFY with an empty body
WIM-T-Mobil-Munich-01	Current consumption
WIM-Nokia-Munich-02	Signature verification in GENERIC security environment

2. Notation

In the subsections describing the changes new text is <u>underlined</u>. 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. WIM PIN-G useage

3.1 Change Classification

Class 3 – Clerical Corrections

3.2 Change Summary

Clarification regarding WIM PIN-G usage.

3.3 Change Description

Section 13.5 "Usage of PINs" add the following text:

All private key operations are protected either with PIN-G or PIN-NR, as MUST be indicated in the PKCS #15 structure. PIN-G protects all operations with Master Secrets, as MUST be indicated in the PKCS #15 structure.

PIN-G also protects all operations with public keys and pre-master secrets (e.g. Encipher, Verify Signature, MSE-Derive key). On the other hand all MSE operations for setting attributes in Security Environments do not demand a prior verification of PIN-G.

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

4. Server key exponent length restriction for smart card WIM

4.1 Change Classification

Class 3 – Clerical Corrections

4.2 Change Summary

Clarification regarding server key exponent length restriction for smart card implementation of WIM.

4.3 Change Description

Section 13, add a new chapter:

13.7 Server RSA Public Key Constraints When Using T=0

The following chapter applies for smart card implementing the transmission protocol T=0 and to servers wishing to transfer Server RSA Public keys to the WIM for WTLS Key Transport operation or Signature verification.

Because of T=0 transport protocol constraints, the data field of APDUs sent to the WIM cannot exceed 255 bytes. In addition, data are sent to the WIM wrapped into TLV data element, reducing the remaining length for actual data as explained below.

In short, it is recommended that the length of the Server RSA Public exponent is at maximum 3 bytes.

In case larger exponents are needed, this chapter indicates how to calculate the maximum size for the exponent.

The maximum size supported by the MSE SET commands preceding both PSO_VerifyDigitalSignature and PSO_Encipher Key Transport: In the MSE command preceding a PSO VerifyDigitalSignature a digest TLV and a public key TLV are sent to the WIM in the following format:

Digest Tag	Digest Len	Digest	Publickey Tag	Publickey Len	Exp Len	Exp	Mod Len	Modulus

For example

- 22 bytes are used for the digest, its tag and length,
- 3 bytes are used for PublicKey tag and length,
- 4 bytes are used for Exponent length and Modulus Length (WTLS coding)

In this case the maximum public key exponent length can not exceed 98 bytes, if 128-byte modulus is used.

In the MSE command preceding the PSO Encipher Key Transport operation, a client version TLV, a random TL and a Public key TLV are sent to the WIM in the following format:

Tag	Len	Client Version	Tag	Len	Tag	Len	ExpLen	Exp	ModLen	Modulus

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

For example

- 3 bytes are used for the client version, its tag and length
- 2 bytes are used for the random tag and length (00, no Value field here)
- 3 bytes are used for PublicKey tag and length,
- 4 bytes are used for Exponent length and Modulus Length (WTLS coding)

In this case the maximum public key exponent length can not exceed 115 bytes, if 128-byte modulus is used.

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

5. WIM status words description clarification

5.1 Change Classification

Class 3 – Clerical Corrections

5.2 Change Summary

WIM status words description clarification.

5.3 Change Description

Section 11.3.8: WIM Status words:

6982	MSE PSO	Execution rights not fulfilled ~~PIN not verified.~~	Security status not satisfied
	READ BINARY UPDATE BINARY	Access rights not fulfilled	

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	Internal data not ready or condition of use not satisfied	
	GET RESPONSE	Internal data not ready	

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

6. Typos

6.1 Change Classification

Class 3 – Clerical Corrections

6.2 Change Summary

Typo Corrections

6.3 Change Description

1 Scope, page 6, 7th paragraph, 3rd sentence: are known to

3.1 Normative References, page 8. With reference to CR wap-cr-mse-p1, need to amend ISO 7816-8 reference to refer to version indicated in CR.

3.1 Normative References, page 8. Amend [WAPWTLS] reference to WAP-199-WTLS Version 18-Feb-2000.

4.2 Abbreviations, page 11. Need to add OMT (used in section 10.1) and PPS (section 11.2.1.2).

6.1 WTLS Operations, page 15, 4th paragraph, 2nd and 3rd sentences: Storage of trusted (root) CA certificates has significance also from a security point of view: they must not be altered – but they can be exposed without danger. CA ~~keys~~certificates may be stored by WIM issuers…….

6.1 WTLS Operations, page 15, 5th paragraph, 3rd sentence: the server may retrieve a client's certificate

6.2.1 Unwrapping a Key, page16: a public key that corresponds to a private key

7.2.4.2 WIM-VerifySignature, page 23, 1st paragraph: CA public key or peer public key

7.2.4.2 WIM-VerifySignature, page 23, 2nd paragraph: takes the signature and the corresponding ~~the~~ digest

7.2.4.4 WIM-KeyTransport, page 24, 2nd paragraph, 3rd sentence: appended with the server public key

8 WIM Operations in WTLS, page 27, 1st sentence: messages sent during

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

8 WIM Operations in WTLS, page 27, 2nd sentence: message flow between the WTLS client

8.1 RSA Handshake, page 27, 1st paragraph: In an RSA handshake…retrieving the client public key or…proving the client's identity…..pre-master secret with the server public key…

8.1 RSA Handshake, page 29, Establish pre-master secret, 3rd sentence: value appended with the server public key.

8.1 RSA Handshake, page 30, Calculate client finished check: "client finished" + H(handshake_messages)~~)~~

8.1 RSA Handshake, page 30, Calculate server finished check: "server finished" + H(handshake_messages)~~)~~

8.1 RSA Handshake, page 30, Calculate client write key block, 2nd sentence: the bytes to be used by the ME as the client write key block.

8.1 RSA Handshake, page 30, last paragraph: The client finished check must be calculated before the server finished check.

8.2 ECDH_ECDSA Handshake, page 31, 1st sentence: used to provide the client's identity

8.4 Optimised ECDH_ECDSA Handshake, page 34, 1st sentence: retrieves the client certificate

9 Information Format, page 36, 3rd paragraph, 2nd sentence: store user related information ~~to~~on the WIM.

9.4.2 Private Key Directory Files (PrKDFs), page 38, 6th bullet point: the private key in ~~a~~ the path

10.1 Security Environment Definition, page 44, 3rd paragraph: which means a maximum of five templates.

10.2.1.1 DST, page 46, structure definition: verificationD~~d~~igest[];

11.3.1 Mapping Service Primitives to Card Commands, page 57, last entry in table: exceptions may occur with all commands

11.3.4 Verification Related Operations, page 62, 3rd paragraph, 2nd sentence: reference data should ~~h~~be handled

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

11.3.6.3 MSE – SET, page 70, 1st sentence: one or several components of the current SE

11.3.7.1 GET RESPONSE, page 80, Le entry in Command APDU table: ~~l~~equal to the XX value

11.4.4 Perform WTLS RSA handshake, top of page 86: master secret reference and cryptographic~~s~~ checksum

11.4.6 Perform Application Level Signature, page 86, 3rd paragraph, 3rd sentence: may need to construct~~s~~ the digestInfo structure

13.4 Saving Certificates, page 93, 3rd paragraph, 2nd sentence: all data is not consiste~~a~~nt .

13.6 Using the WIM for Non-WAP Applications, page 94, 2nd paragraph, 1st sentence: so that the WTLS pre-master secret and master secret ~~is~~ never leave the tamper resistant module.

13.6.1 Signing, page 94, 2nd paragraph, 3rd sentence: any byte string, the length of which is limited to

13.6.1 Signing, page 94, 1st paragraph: 11.3~~5~~.6

13.6.2 Private Key Decryption, page 94, 1st paragraph: 11.3.6~~5.7~~.

13.6.3 Certificate Storage, page 94, end of 2nd paragraph: in ~~a~~ Java applications

14.1.1 General WIM Options and 14.2.1 General ME Options, pages 96 and 98. PKCS#15 CDF useful certificates needs to be inserted.

14.1.1 General WIM Options, page 96, entry in Function column for WIM-023..26: Gener~~er~~ic

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

7. Clarification on key generation

7.1 Change Classification

Class 3 – Clerical Corrections

7.2 Change Summary

Clarification on key generation

7.3 Change Description

Section 6.1:

Permanent key pairs may be generated in the WIM or stored there as part of the manufacturing or personalisation process. However, key generation is not specified in the current version of this specification. It is anticipated that key pairs are generated as a part of the personalisation process.

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

8. Clarification re: logical record lengths

8.1 Change Classification

Class 3 – Clerical Corrections

8.2 Change Summary

Clarification regarding logical record lengths

8.3 Change Description

All Elementary Files (EF) are binary (transparent) files. ~~Some of these files logically consist of fixed length records but are still accessed as binary. The ME should calculate the proper offset based on the known logical record length.~~ This makes it possible to access one or several logical records at a time, or part of a logical record. The Peers EF and Sessions EF data consists of fixed length records. Therefore, the ME should calculate the proper offset based on the known logical record lengths for these two files.

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

9. Recommended PIN type

9.1 Change Classification

Class 3 – Clerical Corrections

9.2 Change Summary

Recommended PIN type

9.3 Change Description

Section 12.1.4.1:

Change the Value of the first entry in the table in section 12.1.4.1 from 'ASCII' *to* 'ascii-numeric'. *Remove last sentence in section 12.1.4.1 (top of page 90).*

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

10. Le Value for Select File command

10.1 Change Classification

Class 2 – Bug Fixes

10.2 Change Summary

Le value for Select File command

10.3 Change Description

Section 11.3.5.1, change the last row of the Command APDU table as follows:

Le	Empty, or ~~FCI length~~00

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

11. Clarification on trusted CDF updates

11.1 Change Classification

Class 3 – Clerical Corrections

11.2 Change Summary

Clarification on trusted CDF updates

11.3 Change Description

Section 9.4.4:

A CDF pointed to by a *trustedCertificates* field in the ODF , contains references to CA certificates. Both the CDF and the EF(s) containing the certificate data pointed to ~~that~~ MUST NOT be modifiable by the user.

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

12. Incorrect PrKDF field

12.1 Change Classification

Class 3 – Clerical Corrections

12.2 Change Summary

Incorrect PrKDF field.

12.3 Change Description

Section 9.4.2:

the ~~**keyHash**~~ keyIdentifiers field MUST be omitted

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

13. Missing functions in table

13.1 Change Classification

Class 3 – Clerical Corrections

13.2 Change Summary

Missing functions in table.

13.3 Change Description

Modify the first row of the table in section 11.3.8 on page 81 to:

61XX	SELECT PSO – Decipher PSO – ComputeCryptographicChecksum PSO- ComputeDigitalSignature ~~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

Modify the 15th row to:

6CXX	GET RESPONSE	Length error, the length that MUST be used is XX. Note that this status is related to the TPDU level.	Wrong length Le

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

14. Multiple EF(AODF) files

14.1 Change Classification

Class 3 – Clerical Corrections

14.2 Change Summary

Clarification regarding multiple EF(AODF) files

14.3 Change Description

Section 9.4.6, page 40, line 7:

The first object in the first AODF listed in EF(ODF) is considered as a General PIN (PIN-G).

Section 13.5, page 93, line 23:

The first object in the first AODF listed in EF(ODF) is considered as a General PIN (PIN-G).

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

15. **Change reference data lenths**

15.1 Change Classification

Class 3 – Clerical Corrections

15.2 Change Summary

Clarification regarding CHANGE REFERENCE DATA lengths

15.3 Change Description

Section 11.3.4.4, page 65, line 5:

This command is used to initiate the comparison of the verification data with the reference data, and then to conditionally replace the existing reference data with new reference data sent in the command. The verification data length and the new reference data length are both fixed by the PKCS15PinAttributes.storedLength field of the corresponding AODF record.

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

16. Status word table

16.1 Change Classification

Class 1 – New Feature, Major Change or Market Effecting Change

16.2 Change Summary

Status word table

16.3 Change Description

Section 11.3.8, page 81: add the following text before the table.

The WIM shall return the status words shown in the following table if, and only if, the corresponding conditions indicated apply.

Section 11.3.8, page 81: add the following row to the table.

63CX	VERIFY	X further retries allowed (command issued with empty body). This status word is recommended over SW1-SW2 = '6300' since it is implemented in the USIM specification.	X further retries allowed (command issued with empty body)

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

17. Sessions and Peers data objects

17.1 Change Classification

Class 3 – Clerical Corrections

17.2 Change Summary

Sessions and Peers data objects

17.3 Change Description

Section 9.4.5, page 39, second paragraph:

WTLS session related data is referenced using opaque Data Objects ‘Peers’ and ‘Sessions’ described in a single DODF.

Section 9.4.5, page 39, third paragraph:

The logical records of the DODF referencing WTLS `Peers' and `Sessions' MUST contain the following fields

Section 12.1.3, page 89:

There MUST be ~~a~~ exactly one Peers Data Object and ~~a~~ exactly one Sessions Data Object.

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

18. Fixed length data items

18.1 Change Classification

Class 2 – Bug Fixes

18.2 Change Summary

Fixed length data items.

18.3 Change Description

Section 12.3, page 91, first paragraph:

All data items that are updateable, ~~MUST~~ SHOULD have fixed length within ~~a~~ the same file (eg, CDF). The following values SHOULD be used.

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

19. Master secret key references

19.1 Change Classification

Class 3 – Clerical Corrections

19.2 Change Summary

Clarification regarding master secret key references

19.3 Change Description

Section 9.4.11,page 42, last line.

~~Note that the master secret is handled internally by the WIM, so that the key reference is equal to the record number in the file (1,2,…).~~ The ME SHOULD maintain a correspondence between the record number in the Sessions EF (1,2,…) and the master secret key reference used in MSE - Derive Key. This will help ensure reliable resumption of secure sessions.

Section 11.3.6.1,page 78, Command APDU table:

Command APDU

CLA	8X
INS	22
P1	41 (MSE SET)
P2	B4 (Cryptographic Checksum Template)
Lc	Length of the Data field.
Data	Concatenation of CRDOs: 84 01 SecretKeyRef + 94 SeedLength Seed SecretKeyRef identifies the resulting master secret. Note that both parameters are mandatory, but the order is not significant. Key derivation process is initiated when both these parameters are set. Master secret key references outside of the EF(Sessions) record range MUST be rejected by the WIM.
Le	Empty

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

Section 11.3.8, page 81, Status Words table:

Add the following row to the list of commands that support the SW1-SW2 = ‘6A88’.

6A88	**PSO** MSE Derive Key	Private key reference not found or incorrect Master Secret key reference.	**Referenced data not found.**

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

20. Status word in VERIFY with an empty body

20.1 Change Classification

Class 3 – Clerical Corrections

20.2 Change Summary

Status word in VERIFY with an empty body

20.3 Change Description

With an empty body ~~the~~, this command may be used to check whether

- verification is not required (SW1-SW2 = ‘9000’), eg, if the verification requirement has been disabled
- verification is required (SW1-SW2 = ‘6300’)
- verification is required, with indication of remaining tries (SW1-SW2 = ‘63CX’)

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

21. Current consumption

21.1 Change Classification

Class 1 – New Feature, Major Change or Market Effecting Change

21.2 Change Summary

Current consumption

21.3 Change Description

Section 3.1, include reference:

[TS 102.221] Smart Cards; UICC-Terminal interface; Physical and logical characteristics (ETSI TS 102 221, version 4.0.0)

Section 11.2, change:

11.2 Electronic Signals And Transmission Protocols

The electronic signals and transmission protocols of cards used for WIM MUST be in accordance with [ISO7816-3] and additional requirements of [GSM11.11], [GSM11.12] and [GSM11.18], if it is integrated with a GSM SIM, if applicable.

The electronic signals and transmission protocols of cards used for WIM MUST be in accordance with [ISO7816-3] and additional requirements of [TS 102.221] if it is implemented on a UICC, if applicable.

The power consumption of the cards used for WIM MUST comply to [TS 102.221].

Section 3.1, include reference:

[TS 102.221] Smart Cards; UICC-Terminal interface; Physical and logical characteristics (ETSI TS 102 221, version 4.0.0)

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

22. Signature verification in GENERIC security environment

22.1 Change Classification

Class 3 – Clerical Corrections

22.2 Change Summary

Signature verification in GENERIC security environment

22.3 Change Description

Section 6.2, add following subchapter:

6.2.3 Signature Verification

Signature verification by WIM may be used in cases where an application needs verification capability (e.g. certificate or end entity signature verification) but the verification algorithm is not present in the ME, or the verification algorithm implementation is more efficient in the WIM. It is not anticipated that this would be practical in all cases, e.g., due to the fact that WIM cryptographic capabilities are likely to be targeted for handling keys suitable for end entities and may not be sufficient for handling keys used by CAs.

In verification, the ME sends the public key, the signature and the hash of the data to the WIM. The WIM returns the status of verification.

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