Specification Information Note
WAP-161_101-WMLScriptCrypto-20010730-a

Version 30-Jul-2001

for

Wireless Application Protocol
WAP-161-WMLScriptCrypto-19991105-a

WMLScript Crypto Library
Version 05-Nov-1999

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.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

Specification Information Note (SIN) fixes technical and clerical errors in the originally published approved specification. This SIN addresses the following issues in WAP WMLScript Crypto Library Specification, WAP-161-WMLScriptCrypto, Version 05-Nov-1999:

- correction in the format of the Static Conformance Requirement

1.1 Included Change Requests

None.

1.2 Affected Sections

This Specification Information Note modifies the following specification sections:

- Appendix D Static Conformance Requirement

2. Document Status

This document is available online in the following formats:

PDF format at http://www.wapforum.org/.

2.1 Copyright Notice

2.2 Errata

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

2.3 Comments

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

3. SCR Format

3.1 Change Classification

1 – New Feature, Major Change or Market Effecting Change	**[ ]**
2 – Bug Fixes	**[ ]**
3 – Clerical Corrections	**[X]**

3.2 Change Summary

- Deletion of the "Subfunction" column (merging the content to the "Function" column).
- Changing item names from WMLSCrypt-Cnnn to WMLSCrypt-C-nnn etc.

3.3 Change

Change to be as follows:

D Static Conformance Requirement

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

D.1 Client Options

Item	Function	Reference	Status	Requirement
WMLSCrypt-C-001	SignText Function supported with at least one signature algorithm	5.1	M	WMLSCrypt-C-002 OR WMLSCrypt-C-003
WMLSCrypt-C-002	SignText RSA	6	O	
WMLSCrypt-C-003	SignText ECDSA	6	O	
WMLSCrypt-C-004	SignText Use of WIM	5.1.4	O	WIM:MCF AND WIM-C-002 AND WIM-C-042

D.2 Script Encoder Options

Item	Function	Reference	Status	Requirement
WMLSCrypt-S-001	SignText	5.1	M	

D.3 Application Options

Item	Function	Reference	Status	Requirement
WMLSCrypt-A-001	SignText output (SignedContent) verification with at least one signature algorithm	5.1	M	WMLSCrypt-A-002 OR WMLSCrypt-A-003
WMLSCrypt-A-002	SignText output (SignedContent) verification RSA	6	O	
WMLSCrypt-A-003	SignText output (SignedContent) verification ECDSA	6	O	