



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 ForumTM Web site,
<http://www.wapforum.org/>, in the form of SIN documents, which are subject to revision or removal without notice.

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

© 2001, Wireless Application 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. DOCUMENT STATUS	5
2.1 COPYRIGHT NOTICE	5
2.2 ERRATA.....	5
2.3 COMMENTS.....	5
3. SCR FORMAT	6
3.1 CHANGE CLASSIFICATION	6
3.2 CHANGE SUMMARY.....	6
3.3 CHANGE.....	6

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

© Copyright Wireless Application Forum Ltd, 2001.

Terms and conditions of use are available from the Wireless Application Protocol Forum Ltd. web site at <http://www.wapforum.org/docs/copyright.htm>.

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	