Specification Information Note

WAP-199_103-WTLS-20010730-a

Version 30-Jul-2001

for

Wireless Application Protocol
WAP-199-WTLS-20000218-a
Wireless Transport Layer Security Specification
Version 18-Feb-2000

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.

© 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 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. SCR FORMAT **5**

3.1 CHANGE CLASSIFICATION 5
3.2 CHANGE SUMMARY 5
3.3 CHANGE DESCRIPTION 5
A.1 WTLS SERVER OPTIONS 5
A.2 WTLS CLIENT OPTIONS 9

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

1. Scope

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

- WAP-199-WTLS-20000218-a

It includes changes from the following:

- WAP-199_102-WTLS-20010214-a, i.e. addition of the "Requirement" column.

Additionally, it changes the SCR format

- removes the "Subfunction" chapter
- changes the item names from WTLS-Snnn to WTLS-S-nnn etc.

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. SCR Format

3.1 Change Classification

Class 3 – Clerical Corrections

3.2 Change Summary

- Inclusion of the requirement column as in the SIN WAP-199_102-WTLS-20010214-a, with more complete requirement description
- Deleting the "Subfunction column" (merging contents with "Function" column)
- Changing the item names from WTLS-Snnn to WTLS-S-nnn etc.

3.3 Change Description

Editor's note: On pages 93 – 97. Merging of tables and changing item names not shown as underlined.

A.1 WTLS Server Options

Item	Function	Reference	Status	Requirement
WTLS-S-001	Session management Full handshake (eg, needed for the anonymous handshake)	10.3	M	
WTLS-S-002	Session management Abbreviated handshake (ie, resume)	10.3	M	
WTLS-S-003	Session management Optimised public key handshake	10.3	O	
WTLS-S-004	Session management Session sharing (multiple connections)	11.1.4	O	
WTLS-S-005	Session management Record concatenation for handshake messages	10.4	M	
WTLS-S-006	Session management Handshake reliability over datagrams	10.4	M	
WTLS-S-007	Session management Sending of hello_request	10.5.1	O	
WTLS-S-010	Record protocol Explicit sequence numbering	9.2.3.1	M	
WTLS-S-011	Record protocol Implicit sequence numbering	9.2.3.1	O	
WTLS-S-012	Record protocol Duplicate removal	9.2.3.1	M	
WTLS-S-013	Record protocol Key refresh	Appendix B.3	M	
WTLS-S-020	Alerting Critical alerts (close connection)	10.2	M	

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

WTLS-S-021	Alerting Fatal alerts (close connection, invalidate session if not in cleartext)	10.2	M	
WTLS-S-022	Alerting Checking of checksums	10.2	M	
WTLS-S-025	Change Cipher Spec	10.1	M	
WTLS-S-026	Application Data	9.2	M	
WTLS-S-030	Anonymous handshaking options; at least one supported.	Appendix A	M	WTLS-S-031 OR WTLS-S-032 OR WTLS-S-033 OR WTLS-S-034 OR WTLS-S-035 OR WTLS-S-036 OR WTLS-S-037 OR WTLS-S-038 OR WTLS-S-049
WTLS-S-031	Anonymous handshaking options DH_ANON	Appendix A	O	
WTLS-S-032	Anonymous handshaking options DH_ANON_768	Appendix A	O	
WTLS-S-033	Anonymous handshaking options DH_ANON_512	Appendix A	O	
WTLS-S-034	Anonymous handshaking options RSA_ANON	Appendix A	O	
WTLS-S-035	Anonymous handshaking options RSA_ANON_768	Appendix A	O	
WTLS-S-036	Anonymous handshaking options RSA_ANON_512	Appendix A	O	
WTLS-S-037	Anonymous handshaking options ECDH_ANON	Appendix A	O	
WTLS-S-038	Anonymous handshaking options ECDH_ANON_131	Appendix A	O	
WTLS-S-049	Anonymous handshaking options ECDH_ANON_113	Appendix A	O	
WTLS-S-060	Non-anonymous (server authenticated) handshake options; at least one supported. If either of WTLS-S-062 and WTLS-S-063 is supported, then WTLS-S-061 MUST also be supported, with a minimum supported modulus of 1024 bits.	Appendix A	M	(WTLS-S-061 OR WTLS-S-064) AND WTLS-S-191
WTLS-S-061	Non-anonymous (server authenticated) handshake options RSA	Appendix A	O	
WTLS-S-062	Non-anonymous (server authenticated) handshake options RSA_768	Appendix A	O	WTLS-S-061
WTLS-S-063	Non-anonymous (server authenticated) handshake options RSA_512	Appendix A	O	WTLS-S-061
WTLS-S-064	Non-anonymous (server authenticated) handshake options ECDH_ECDSA	Appendix A	O	WTLS-S-165 OR WTLS-S-167
WTLS-S-070	Client authentication options; at least one supported.	Appendix A	O	WTLS-S-071 OR WTLS-S-072

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

WTLS-S-071	Client authentication options RSA	Appendix A	O	
WTLS-S-072	Client authentication options ECDH_ECDSA	Appendix A	O	
WTLS-S-080	Shared secret handshake	Appendix A	O	
WTLS-S-090	NULL key exchange	Appendix A	O	
WTLS-S-100	Data encryption options; at least one supported. Implementatations are RECOMMENDED to support RC5_CBC, RC5_CBC_64 and RC5_CBC_56 as minimum. Implementations are RECOMMENDED to support encryption options with the highest number of effective key bits (as preferred) and additionally, options with lower number of effective bits.	Appendix A	M	WTLS-S-101 OR WTLS-S-102 OR WTLS-S-103 OR WTLS-S-104 OR WTLS-S-105 OR WTLS-S-106 OR WTLS-S-107 OR WTLS-S-108
WTLS-S-101	Data encryption options RC5_CBC	Appendix A	O	
WTLS-S-102	Data encryption options RC5_CBC_56	Appendix A	O	
WTLS-S-103	Data encryption options DES_CBC	Appendix A	O	
WTLS-S-104	Data encryption options 3DES_CBC_EDE	Appendix A	O	
WTLS-S-105	Data encryption options IDEA_CBC	Appendix A	O	
WTLS-S-106	Data encryption options IDEA_CBC_56	Appendix A	O	
WTLS-S-107	Data encryption options RC5_CBC_64	Appendix A	O	
WTLS-S-108	Data encryption options IDEA_CBC_64	Appendix A	O	
WTLS-S-120	NULL encryption	Appendix A	O	
WTLS-S-130	MAC options; at least one supported. Implementations are RECOMMENDED to use SHA_80 in preference to SHA	Appendix A	M	
WTLS-S-131	MAC options SHA	Appendix A	M	
WTLS-S-132	MAC options SHA_80	Appendix A	O	
WTLS-S-133	MAC options SHA_40	Appendix A	O	
WTLS-S-134	MAC options (Algorithm removed)	N/A	N/A	
WTLS-S-135	MAC options MD5	Appendix A	O	
WTLS-S-136	MAC options MD5_80	Appendix A	O	

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

WTLS-S-137	MAC options MD5_40	Appendix A	O	
WTLS-S-140	NULL MAC (SHA_0)	Appendix A	O	
WTLS-S-141	NULL compression	Appendix A	M	
WTLS-S-151	Predefined Diffie-Hellman parameters Parameters 1	Appendix A	O	
WTLS-S-152	Predefined Diffie-Hellman parameters Parameters 2	Appendix A	O	
WTLS-S-165	ECC basic curves; if ECC is used, at least one MUST be supported and all SHOULD be supported. Curve 5 (163 bits)	Appendix A	O	
WTLS-S-167	ECC basic curves Curve 7 (160 bits)	Appendix A	O	
WTLS-S-161	ECC non-basic curves Curve 1 (113 bits)	Appendix A	O	
WTLS-S-163	ECC non-basic curves Curve 3 (163 bits)	Appendix A	O	
WTLS-S-164	ECC non-basic curves Curve 4 (113 bits)	Appendix A	O	
WTLS-S-166	ECC non-basic curves Curve 6 (112 bits)	Appendix A	O	
WTLS-S-168	ECC non-basic curves Curve 8 (112 bits)	Appendix A	O	
WTLS-S-169	ECC non-basic curves Curve 9 (160 bits)	Appendix A	O	
WTLS-S-170	ECC non-basic curves Curve 10 (233 bits)	Appendix A	O	
WTLS-S-171	ECC non-basic curves Curve 11 (233 bits)	Appendix A	O	
WTLS-S-172	ECC non-basic curves Curve 12 (224 bits)	Appendix A	O	
WTLS-S-180	ECC point compression	11.1.3	O	
WTLS-S-191	Verification of certificates; WTLS certificate verification MUST be supported if non-anonymous handshake is supported WTLS certificate	10.5.2	O	
WTLS-S-192	Verification of certificates X.509 certificate	10.5.2	O	
WTLS-S-193	Verification of certificates X9.68 certificate	10.5.2	O	
WTLS-S-200	GMT UNIX time support	10.5.1	M	

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

A.2 WTLS Client Options

Item	Function	Reference	Status	Requirement
WTLS-C-001	Session management Full handshake (eg, needed for the anonymous handshake)	10.3	M	
WTLS-C-002	Session management Abbreviated handshake (ie, resume)	10.3	M	
WTLS-C-003	Session management Optimised public key handshake	10.3	O	
WTLS-C-004	Session management Session sharing (multiple connections)	11.1.4	O	
WTLS-C-005	Session management Record concatenation for handshake messages	10.4	M	
WTLS-C-006	Session management Handshake reliability over datagrams	10.4	M	
WTLS-C-007	Session management Start negotiation after a cleartext Hello Request	10.5.1.1	O	
WTLS-C-010	Record protocol Explicit sequence numbering	9.2.3.1	M	
WTLS-C-011	Record protocol Implicit sequence numbering	9.2.3.1	O	
WTLS-C-012	Record protocol Duplicate removal	9.2.3.1	M	
WTLS-C-013	Record protocol Key refresh	Appendix B.3	M	
WTLS-C-020	Alerting Critical alerts (close connection)	10.2	M	
WTLS-C-021	Alerting Fatal alerts (close connection, invalidate session if not in cleartext)	10.2	M	
WTLS-C-022	Alerting Checking of checksums	10.2	M	
WTLS-C-025	Change Cipher Spec	10.1	M	
WTLS-C-026	Application Data	9.2	M	
WTLS-C-030	Anonymous handshaking options; at least one supported.	Appendix A	M	WTLS-C-031 OR WTLS-C-032 OR WTLS-C-033 OR WTLS-C-034 OR WTLS-C-035 OR WTLS-C-036 OR WTLS-C-037 OR WTLS-C-038 OR WTLS-C-049
WTLS-C-031	Anonymous handshaking options DH_ANON	Appendix A	O	
WTLS-C-032	Anonymous handshaking options DH_ANON_768	Appendix A	O	

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

WTLS-C-033	Anonymous handshaking options DH_ANON_512	Appendix A	O	
WTLS-C-034	Anonymous handshaking options RSA_ANON	Appendix A	O	
WTLS-C-035	Anonymous handshaking options RSA_ANON_768	Appendix A	O	
WTLS-C-036	Anonymous handshaking options RSA_ANON_512	Appendix A	O	
WTLS-C-037	Anonymous handshaking options ECDH_ANON	Appendix A	O	
WTLS-C-038	Anonymous handshaking options ECDH_ANON_131	Appendix A	O	
WTLS-C-049	Anonymous handshaking options ECDH_ANON_113	Appendix A	O	
WTLS-C-060	Non-anonymous (server authenticated) handshake options; at least one supported. If either of WTLS-C-062 and WTLS-C-063 is supported, then WTLS-C-061 MUST also be supported, with a minimum supported modulus of 1024 bits.	Appendix A	M	(WTLS-C-061 OR WTLS-C-064) AND WTLS-C-191
WTLS-C-061	Non-anonymous (server authenticated) handshake options RSA	Appendix A	O	
WTLS-C-062	Non-anonymous (server authenticated) handshake options RSA_768	Appendix A	O	WTLS-C-061
WTLS-C-063	Non-anonymous (server authenticated) handshake options RSA_512	Appendix A	O	WTLS-C-061
WTLS-C-064	Non-anonymous (server authenticated) handshake options ECDH_ECDSA	Appendix A	O	WTLS-C-165 OR WTLS-C-167
WTLS-C-070	Client authentication options; at least one supported.	Appendix A	O	WTLS-C-071 OR WTLS-C-072
WTLS-C-071	Client authentication options RSA	Appendix A	O	
WTLS-C-072	Client authentication options ECDH_ECDSA	Appendix A	O	
WTLS-C-080	Shared secret handshake	Appendix A	O	
WTLS-C-090	NULL key exchange	Appendix A	O	
WTLS-C-100	Data encryption options; at least one supported. Implementatations are RECOMMENDED to support RC5_CBC, RC5_CBC_64 and RC5_CBC_56 as minimum. Implementations are RECOMMENDED to support encryption options with the highest number of effective key bits (as preferred) and additionally, options with lower number of effective bits.	Appendix A	O	WTLS-C-101 OR WTLS-C-102 OR WTLS-C-103 OR WTLS-C-104 OR WTLS-C-105 OR WTLS-C-106 OR WTLS-C-107 OR WTLS-C-108
WTLS-C-101	Data encryption options RC5_CBC	Appendix A	O	
WTLS-C-102	Data encryption options RC5_CBC_56	Appendix A	O	

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

WTLS-C-103	Data encryption options DES_CBC	Appendix A	O	
WTLS-C-104	Data encryption options 3DES_CBC_EDE	Appendix A	O	
WTLS-C-105	Data encryption options IDEA_CBC	Appendix A	O	
WTLS-C-106	Data encryption options IDEA_CBC_56	Appendix A	O	
WTLS-C-107	Data encryption options RC5_CBC_64	Appendix A	O	
WTLS-C-108	Data encryption options IDEA_CBC_64	Appendix A	O	
WTLS-C-120	NULL encryption	Appendix A	O	
WTLS-C-130	MAC options; at least one supported. Implementations are RECOMMENDED to use SHA_80 in preference to SHA	Appendix A	M	
WTLS-C-131	MAC options SHA	Appendix A	M	
WTLS-C-132	MAC options SHA_80	Appendix A	O	
WTLS-C-133	MAC options SHA_40	Appendix A	O	
WTLS-C-134	MAC options (Algorithm removed)	N/A	N/A	
WTLS-C-135	MAC options MD5	Appendix A	O	
WTLS-C-136	MAC options MD5_80	Appendix A	O	
WTLS-C-137	MAC options MD5_40	Appendix A	O	
WTLS-C-140	NULL MAC (SHA_0)	Appendix A	O	
WTLS-C-141	NULL compression	Appendix A	M	
WTLS-C-151	Predefined Diffie-Hellman parameters Parameters 1	Appendix A	O	
WTLS-C-152	Predefined Diffie-Hellman parameters Parameters 2	Appendix A	O	
WTLS-C-165	ECC basic curves; if ECC is used, at least one MUST be supported. Verification SHOULD be supported with all basic curves that have field size not less than 160 bits Curve 5 (163 bits)	Appendix A	O	
WTLS-C-167	ECC basic curves Curve 7 (160 bits)	Appendix A	O	
WTLS-C-161	ECC non-basic curves Curve 1 (113 bits)	Appendix A	O	

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

WTLS-C-163	ECC non-basic curves Curve 3 (163 bits)	Appendix A	O	
WTLS-C-164	ECC non-basic curves Curve 4 (113 bits)	Appendix A	O	
WTLS-C-166	ECC non-basic curves Curve 6 (112 bits)	Appendix A	O	
WTLS-C-168	ECC non-basic curves Curve 8 (112 bits)	Appendix A	O	
WTLS-C-169	ECC non-basic curves Curve 9 (160 bits)	Appendix A	O	
WTLS-C-170	ECC non-basic curves Curve 10 (233 bits)	Appendix A	O	
WTLS-C-171	ECC non-basic curves Curve 11 (233 bits)	Appendix A	O	
WTLS-C-172	ECC non-basic curves Curve 12 (224 bits)	Appendix A	O	
WTLS-C-180	ECC point compression	11.1.3	O	
WTLS-C-191	Verification of certificates; WTLS certificate verification MUST be supported if non-anonymous handshake is supported WTLS certificate	10.5.2	O	
WTLS-C-192	Verification of certificates X.509 certificate	10.5.2	O	
WTLS-C-193	Verification of certificates X9.68 certificate	10.5.2	O	
WTLS-C-200	GMT UNIX time support	10.5.1	O	
WTLS-C-220	Use of WIM	[WAP WIM]	O	WTLS-C-070 AND WIM:MCF AND WIM-C-001

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