



## **Specification Information Note**

**WAP-219\_100-TLS-20011029-a**

Version 29-October-2001

---

for

Wireless Application Protocol

WAP-219-TLS-20010411-a

TLS

Version 11-April-2001

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 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. REPLACE SCR TABLES .....	5
3.1 CHANGE CLASSIFICATION .....	5
3.2 CHANGE SUMMARY.....	5
3.3 CHANGE DESCRIPTION.....	5

# 1. Scope

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

- WAP-219-TLS-20010411-a

It includes changes to support latest format specified by:

- WAP-221-CREQ-20010425-a

# 2. Notation

In the subsections describing the changes new text is underlined. Removed text has ~~striketrough~~ 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.

## 3. Replace SCR Tables

### 3.1 Change Classification

Class 3 – Clerical Corrections

### 3.2 Change Summary

Replace SCR tables with new format and naming convention as specified in WAP-221-CREQ-20010425-a.

### 3.3 Change Description

**Editor's note:** Replace the whole of Appendix A with the following:

## Appendix A Static Conformance Requirements

This static conformance clause defines a minimum set of features that should be implemented to ensure interoperability. A feature can be optional (O), or mandatory (M) [WCREQ].

### A.1 General Requirements

~~This section applies to all the clients and servers that conform to this specification.~~

Item	Functionality	Reference	Status	Requirement
<del>TLS-001</del>	<del>Conform to TLS 1.0 [RFC2246]</del>	<del>6</del>	<del>M</del>	

### A.2A.1 Client Options

#### A.2.1A.1.1 Basic

This section applies to all clients that conform to this specification.

Item	Functionality	Reference	Status	Requirement
TLS- <del>C</del> -001	Conform to TLS 1.0 [RFC2246]	6	M	<del>[RFC2246]</del>
TLS-C-010	RSA based Cipher Suites (TLS-C-011 and TLS-C-012); at least one supported.	6.1	M	TLS-C-011 OR TLS-C-012
TLS-C-011	TLS_RSA_WITH_RC4_128_SHA	6.1	O	
TLS-C-012	TLS_RSA_WITH_3DES_EDE_CBC_SHA	6.1	O	
TLS-C-020	Session Resume	6.2.1	M	
TLS-C-030	Server Authentication	6.3	M	TLS-C-031

Item	Functionality	Reference	Status	Requirement
TLS-C-031	Support X.509 certificate processing in accordance with the WAP Certificate and CRL Profile Specification [WAPCert]	6.3	M	Cert-SrvA-C-001 AND Cert-SrvA-C-002 AND Cert-SrvA-C-003 AND Cert-SrvA-C-004 AND Cert-SrvA-C-005 AND Cert-SrvA-C-006 AND Cert-SrvA-C-007 AND Cert-SrvA-C-009 AND Cert-SrvA-C-010 AND Cert-SrvA-C-012 AND Cert-SrvA-C-013 AND Cert-TLS-C-001 [WAPCert]
TLS-C-040	Client Authentication	6.4	O	TLS-C-100 AND TLS-C-102
<u>TLS-C-041</u>	<u>TLS Tunnelling support</u>	<u>7</u>	<u>O</u>	<u>TLS-C-200 AND</u> <u>TLS-C-201 AND</u> <u>TLS-C-202 AND</u> <u>TLS-C-203</u>

## A.2.2A.1.2 Client Authentication

This section only applies to the client that supports client authentication.

Item	Functionality	Reference	Status	Requirement
TLS-C-100	Support use of WAP profiled X.509 client certificate [WAPCert]	6.4	O	WAPCert:MCF [WAPCert]
TLS-C-101	Support use of X.509 client certificate [RFC2459]	6.4	O	[RFC2459]
TLS-C-102	Support RSA client certificate and signature	6.4	O	

## A.2.3A.1.3 TLS Tunneling

This section only applies to clients that support proxy.

Item	Functionality	Reference	Status	Requirement
TLS-C-200	Support TLS tunneling	7	<del>MO</del>	
TLS-C-201	Establish the tunnel over the raw TCP connection	7	<del>OM</del>	
TLS-C-202	Use HTTP CONNECT to establish a TLS tunnel <a href="#">[RFC2817]</a>	7	<del>OM</del>	<del>[RFC2817]</del>
TLS-C-203	Abort the attempt to establish a TLS tunnel if a non-successful response for an HTTP CONNECT request is received	7	<del>OM</del>	

## A.3A.2 Server Options

### A.3.1A.2.1 Basic

This section applies to all servers (ie, origin server or proxy server) that conform to this specification.

Item	Functionality	Reference	Status	Requirement
TLS-S-001	Conform to TLS 1.0 <a href="#">[RFC2246]</a>	6	M	<del>[RFC2246]</del>
TLS-S-011	TLS_RSA_WITH_RC4_128_SHA	6.1	M	
TLS-S-013	TLS_RSA_WITH_3DES_EDE_CBC_SHA	6.1	M	
TLS-S-020	Session Resume	6.2	M	
TLS-S-030	Server Authentication	6.3	M	TLS-S-031 OR TLS-S-032
TLS-S-031	Use of WAP profiled X.509 server certificate <a href="#">[WAPCert]</a>	6.3	O	<del>[WAPCert]</del>
TLS-S-032	Use of X.509 server certificate <a href="#">[RFC2459]</a>	6.3	O	<del>[RFC2459]</del>



Item	Functionality	Reference	Status	Requirement
TLS-S-040	Client Authentication	6.4	O	TLS-S-100 AND TLS-S-101 AND TLS-S-102 AND TLS-S-103

### A.3.2A.2.2 Client Authentication

This section only applies to servers that support client authentication.

Item	Functionality	Reference	Status	Requirement
TLS-S-100	Support WAP profiled X.509 client certificate <a href="#">[WAPCert]</a>	6.4	O	WAPCert:MSF <a href="#">[WAPCert]</a>
TLS-S-101	Support X.509 client certificate <a href="#">[RFC2459]</a>	6.4	O	<a href="#">[RFC2459]</a>
TLS-S-102	Support verification of RSA client certificate and signature	6.4	O	
TLS-S-103	Request RSA certificate type for client certificate	6.4	O	