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.

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

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 ~~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.

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.1General Requirements

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

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

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-C-001	Conform to TLS 1.0 [RFC2246]	6	M	[RFC2246]
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
TLS-C-041	TLS Tunnelling support	7	O	TLS-C-200 AND TLS-C-201 AND TLS-C-202 AND TLS-C-203

~~A.2.2~~A.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.2.3~~A.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	~~M~~O	
TLS-C-201	Establish the tunnel over the raw TCP connection	7	O~~M~~	
TLS-C-202	Use HTTP CONNECT to establish a TLS tunnel [RFC2817]	7	O~~M~~	~~[RFC2817]~~
TLS-C-203	Abort the attempt to establish a TLS tunnel if a non-successful response for an HTTP CONNECT request is received	7	O~~M~~	

~~A.3~~A.2 Server Options

~~A.3.1~~A.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 [RFC2246]	6	M	~~[RFC2246]~~
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 [WAPCert]	6.3	O	~~[WAPCert]~~
TLS-S-032	Use of X.509 server certificate [RFC2459]	6.3	O	~~[RFC2459]~~

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.3.2~~A.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 [WAPCert]	6.4	O	WAPCert:MSF ~~[WAPCert]~~
TLS-S-101	Support X.509 client certificate [RFC2459]	6.4	O	~~[RFC2459]~~
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	