Specification Information Note

WAP-217_103-WPKI-20011102-a

Version 2-Nov-2001

for

Wireless Application Protocol
WAP-217-WPKI-20010424-a

WPKI
Version 24 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 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-217-WPKI-20010424-a

It includes changes from the following change requests:

- CR-WPKI-BALTIMORE-22-10-2001

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

1. Incorporation of comments on SCRs (see below for comments) and clerical corrections.
    a. SCR Items should include "-C-XXX" or "-S-XXX" definition
    b. WPKI-Client-008 … 009 has WTLS reference but no requirement
    c. WPKI-Client-010 incorrect reference to WTLS-C070
    d. WPKI-Client-011 incorrect reference to WMLSCrypt-C001
    e. WPKI-Client-012 incorrect reference to WTLS-C070
    f. WPKI-Client-013 incorrect reference to WMLSCrypt-C001
    g. WPKI-Client-017 … 018 has WTLS reference but no requirement
    h. WPKI-Client-019 … 020 syntax error in reference to WIM
    i. WPKI-Portal-012 incorrect reference to WTLS-S70
    j. WPKI-Portal-013 invalid reference to content requirement (out of scope)

3.3 Change Description

Editor's note: Replace all of Section 8 with the following:

8 WPKI Static Conformance Requirement

This static conformance requirement lists a minimum set of functions that can be implemented to help ensure that WAP implementations using WPKI will be able to inter-operate. The "Status" column indicates if the function is mandatory (M) or optional (O). Where a reference to an entire section of the specification is given without further qualification then implementations MUST support all "MUST" statements in the section, and MAY support all "SHOULD" and "MAY" statements.

Where no sub-function is given a later subsection of this section contains details or the "Status" column applies to relevant parts of the entire section (where the relevant parts are clear from the context).

This section in its entirety only applies to WAP implementation that claim conformance to "the WAP PKI". Parts of this section do apply to all WAP implementations that implement either signText() or WTLS classes 2 or 3.

8.1 Client Options

Item	Function	Reference	Status	Requirement
WPKI-C-001	Public key capabilities	0	M	
WPKI-C-002	Private key capabilities	0	O	

8.1.1 Client Public Key Capability Options

This chapter presents client options related to public key operations used for verification purposes (that is, WTLS server authentication). This chapter is related to all WPKI-capable clients.

Item	Function	Reference	Status	Requirement
WPKI-C-003	Local trusted CA information handling.	7.1.1	M	
WPKI-C-004	OTA Trusted CA information download. Hashed CA information.	7.1.3	M	WSP:MCF
WPKI-C-005	OTA Trusted CA information download. OTA Signed CA information.	7.1.4	M	WSP:MCF
WPKI-C-006	Trusted CA key roll-over rollover-certificate[1]	7.1.5	O	WSP:MCF
WPKI-C-007	Public key algorithms for certificate signature validation: Either RSA or ECC		M	WPKI-C-008 OR WPKI-C-009
WPKI-C-008	RSA Private key algorithms for signature verification.	[WAPWTLS]	O	WTLS-C-060
WPKI-C-009	ECC Private key algorithms for signature verification. (Curves as defined in [WAPWTLS])	[WAPWTLS]	O	WTLS-C-060

8.1.2 Client Private Key Capability Options

This chapter is only related to clients that support private keys. The client may implement private key support using WIM or otherwise (including software only).

Item	Function	Reference	Status	Requirement
WPKI-C-010	Private key capability (note: this doesn't mean all clients have key pairs, just that they be capable of storing and using private keys) Support for the authentication key (WTLS Class 3)	6.2	M	WTLS-C-070
WPKI-C-011	Private key capability (note: this doesn't mean all clients have key pairs, just that they be capable of storing and using private keys) Support for the signText() key.	6.2	M	WMLSCrypt-C-001
WPKI-C-012	OTA WTLS client authentication (here used for registration)	7.3.1	M	WTLS-C-070
WPKI-C-013	WMLScript signText (here used for registration)	7.3.2	M	WMLSCrypt-C-001

[1] The justification for this is that the useful lifetime of a WAP device or server is expected to be significantly shorter than the typical validity of root CA information.

WPKI-C-014	Certificate delivery: Handling of cert-response messages.	7.3.5	M	WSP:MCF AND WIM-ICC-016 AND WIM-C-016
WPKI-C-015	Certificate delivery: x509-user-cert	7.3.5	O	WSP:MCF; AND WIM-ICC-016 AND WIM-C-016
WPKI-C-016	Private key algorithms for signing (either RSA or ECC)		M	WPKI-C-017 OR WPKI-C-018
WPKI-C-017	RSA Private key algorithms for signing	[WAPWTLS]	O	WTLS-C-070
WPKI-C-018	ECC Private key algorithms for signing. (Curves as defined in [WAPWTLS])	[WAPWTLS]	O	WTLS-C-070

8.1.3 Client root certificate storage options

This sections specifies the options for client access to root certificates.

Item	Function	Reference	Status	Requirement
WPKI-C-019	Accessing root certificates: The client shall be able to access certificates stored in a WIM on the same ICC as the SIM. This option applies to clients that support a SIM and a WIM only.	6	M	WIM-ICC-015 AND WIM-ICC-016 AND WIM-C-017 AND WIM-C-018
WPKI-C-020	Accessing root certificates: The client shall be able to access certificates stored in a WIM not on the same ICC as the SIM. This applies to clients that support a WIM only	6	M	WIM-ICC-015 AND WIM-ICC-016 AND WIM-C-017 AND WIM-C-018
WPKI-C-022	Accessing root certificates: The client shall be able to access certificates stored on the client itself.	6	O	

8.2 PKI Portal Options

This section specifies the options for PKI portal implementers.

Item	Function	Reference	Status	Requirement
WPKI-Portal-S-001	Public key capabilities	0	M	
WPKI-Portal-S-002	Support Client private keys	8.2.3	O	

8.2.1 PKI Portal Public Key Capability Options

Item	Function	Reference	Status	Requirement
WPKI-Portal-S-003	OTA Trusted CA certificate download support: Hashed-certificate.	7.1.3	M	
WPKI-Portal-S-004	OTA Trusted CA certificate download support: Signed root.	7.1.4	M	
WPKI-Portal-S-005	Trusted CA key roll-over: Rollover-certificate.	7.1.5	O	

8.2.2 PKI Portal Options to Support WTLS Server Certification

Item	Function	Reference	Status	Requirement
WPKI-Portal-S-006	Handling of PKCS#10 long term server certification requests.	7.2.1	M	
WPKI-Portal-S-007	Responses to PKCS#10 requests:	7.2.1	M	WPKI-Portal-S-008
WPKI-Portal-S-008	Responses to PKCS#10 requests: Direct return of WTLSCertificate.	7.2.1	M	
WPKI-Portal-S-009	Responses to PKCS#10 requests: Direct return of X.509 Certificate.	7.2.1	O	
WPKI-Portal-S-010	Responses to PKCS#10 requests: Return of URL.	7.2.1	O	
WPKI-Portal-S-011	Short-lived certificate retrieval protocol	7.2.3	O	

8.2.3 PKI Portal Options to Support Client Registration

Item	Function	Reference	Status	Requirement
WPKI-Portal-S-012	WTLS client authentication (here used for registration)	7.3.1	M	WTLS-S-070
WPKI-Portal-S-013	WMLScript signText support (here used for registration)	7.3.2	M	
WPKI-Portal-S-014	Certificate delivery: cert-response	7.3.5	M	
WPKI-Portal-S-015	Certificate delivery: x509-user-cert	7.3.5	O	
WPKI-Portal-S-016	Support for certificate URL retrieval:	7.4	M	WPKI-Portal-S-017
WPKI-Portal-S-017	Support for certificate URL retrieval: HTTP scheme	7.4.1	M	

WPKI-Portal-S-018	Support for certificate URL retrieval: LDAP scheme	7.4.2	O	

8.2.4 PKI Portal Options to interact with X.509 PKI

Item	Function	Reference	Status	Requirement
WPKI-Portal-S-019	Support CMP between PKI portal and RA/CA	7.3	O	
WPKI-Portal-S-020	Support CMC between PKI portal and RA/CA	7.3	O	

8.3 WTLS Server Options

This section describes PKI options related to WTLS servers.

Item	Function	Reference	Status	Requirement
WPKI-S-001	Local trusted CA information handling	7.1.2	M	
WPKI-S-002	Production of PKCS#10 requests	7.2.1	O	
WPKI-S-003	Handling responses to PKCS#10 requests: Direct return of WTLSCertificate	7.2.1	O	
WPKI-S-004	Handling responses to PKCS#10 requests: Direct return of X.509 Certificate	7.2.1	O	
WPKI-S-005	Handling responses to PKCS#10 requests: Return of URL	7.2.1	O	
WPKI-S-006	Short-lived cert retrieval protocol	7.2.3	O	
WPKI-S-007	Support for certificate URL retrieval.	7.4	M	WPKI-S-008
WPKI-S-008	Support for certificate URL retrieval: HTTP scheme.	7.4.1	M	
WPKI-S-009	Support for certificate URL retrieval: LDAP scheme.	7.4.2	O	

8.4 signText() Verifier Options

Item	Function	Reference	Status	Requirement
WPKI-Verif-S-001	Local trusted CA information handling.	7.1.2	M	
WPKI-Verif-S-002	Support for certificate URL retrieval.	7.4	M	WPKI-Verif-S-003
WPKI-Verif-S-003	Support for certificate URL retrieval: HTTP scheme.	7.4.1	M	
WPKI-Verif-S-004	Support for certificate URL retrieval: LDAP scheme.	7.4.2	O	