Specification Information Note

WAP-211_104-WAPCert-20010928-a

Version 28-Sep-2001

for

Wireless Application Protocol
WAP-211-WAPCert-20010522-a
WAP Certificate and CRL Profiles Specification
Version 22-May-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.

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-211-WAPCert-20010522-a

2. Notation

In the subsections describing the changes the presented text is to replace the corresponding text in the specification. Text that is not presented is not affected at all. The change descriptions 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 clarify where and how the changes shall be applied.

3. Correction of SCR section

3.1 Change Classification

Class 3 – Clerical correction

3.2 Change Summary

SCR section was not in conformance with WAP-221-CREQ-20010425-a.

3.3 Change Description

Replace all of Annex C with the following text:

Annex C Static Conformance Requirements

C.1 ME Options

C.1.1. General Certificate Options

This table specifies generic certificate-processing requirements for MEs [1]. In the table, "M" stands for "Mandatory to implement" and "O" stands for "Optional."

Item	Function	Reference	Status	Requirements
Cert-Gen-C-001	General X.509 Certificate support - Parsing of fields as needed for functionality outlined below	6	M	
Cert-Gen-C-002	General X.509 Certificate support - Able to handle client certificates at least up to 700 bytes long	6	M	
Cert-Gen-C-003	Issuer Name - Recognize the following required RFC 2459 attributes: **countryName, organizationName, organizationalUnitName, commonName, stateOrProvinceName, domainComponent**	6.2, 6.3, 6.4	M	
Cert-Gen-C-004	Issuer Name - Recognize all recommended RFC 2459 attributes: **localityName, title, surname, givenName, initials, generationQualifier**	6.2, 6.3, 6.4	O	
Cert-Gen-C-005	Issuer Name - Capable of displaying **PrintableString**, **UTF8String** and **NumericString** values	6.2, 6.3, 6.4	M	
Cert-Gen-C-006	Issuer Name - Recognize the **serialNumber** attribute	6.2, 6.3, 6.4	M	

[1] This subsection does not apply to ME implementations that never handles (receives, stores, etc.) certificates profiled in accordance with this document

Item	Function	Reference	Status	Requirements
Cert-Gen-C-007	Subject Name - Recognize the following required RFC 2459 attributes: **countryName, organizationName, organizationalUnitName, commonName, stateOrProvinceName, domainComponent**	6.2, 6.3, 6.4	M	
Cert-Gen-C-008	Subject Name -Recognize all recommended RFC 2459 attributes: **localityName, title, surname, givenName, initials, generationQualifier**	6.2, 6.3, 6.4	O	
Cert-Gen-C-009	Subject Name - Capable of displaying **PrintableString, UTF8String** and **NumericString** values	6.2, 6.3, 6.4	M	
Cert-Gen-C-010	Subject Name - Recognize the **serialNumber** attribute	6.2, 6.3, 6.4	M	

C.1.2. X.509 Server Certificate options

This table specifies certificate-processing requirements for MEs that support X.509-based server authentication.

Item	Function	Reference	Status	Requirements
Cert-SrvA-C-001	General X.509 Certificate support - Parsing of all fields	6.1	M	
Cert-SrvA-C-002	General X.509 Certificate support - Able to process server certificates at least up to 1000 bytes long (CA certificates 2000 bytes)	6.4.1	M	
Cert-SrvA-C-003	General X.509 Certificate support - Capable of processing certificates with unknown distinguished name attributes (e.g. needed for chain building)	6.4.4 6.4.5	M	
Cert-SrvA-C-004	General X.509 Certificate support - Capable of processing certificates with unknown, non-critical certificate extensions	6.4.7	M	
Cert-SrvA-C-005	Verification - Certificate path processing as defined in [7] (and [8]), but subject to limitations in Section 6.4 and 6.1	6.4, 6.1	M	
Cert-SrvA-C-006	Serial Number - Handling of serial numbers up to 20 bytes long	6.4.2	M	
Cert-SrvA-C-007	Issuer Name - Recognize the following required RFC 2459 attributes: **countryName, organizationName, organizationalUnitName, commonName, stateOrProvinceName, domainComponent**	6.4.4	M	
Cert-SrvA-C-008	Issuer Name - Recognize all recommended RFC 2459 attributes: **localityName, title, surname, givenName, initials, generationQualifier**	6.4.4	O	
Cert-SrvA-C-009	Issuer Name - Recognize the **serialNumber** attribute	6.4.4	M	

Item	Function	Reference	Status	Requirements
Cert-SrvA-C-010	Subject Name - Recognize the following required RFC 2459 attributes: **countryName, organizationName, organizationalUnitName, commonName, stateOrProvinceName, domainComponent**	6.4.4, 6.4.5	M	
Cert-SrvA-C-011	Subject Name - Recognize all recommended RFC 2459 attributes: **localityName, title, surname, givenName, initials, generationQualifier**	6.4.4, 6.4.5	O	
Cert-SrvA-C-012	Subject Name - Recognize the **serialNumber** attribute	6.4.4, 6.4.5	M	
Cert-SrvA-C-013	Extensions - Recognize and process extensions as specified in this document: **keyUsage**, **subjectAltName**, **extKeyUsage**, **authorityKeyIdentifier**. For CA certificates, must also process the **basicConstraints** and **subjectKeyIdentifier** extension.	6.4.7 6.6.6	M	
Cert-SrvA-C-014	Extensions - Recognize and process extensions as specified in this document: **certificatePolicies, authorityAccessInfo**	6.4.7	O	
Cert-SrvA-C-015	Signature Algorithms - Capable of processing certificates signed with at least one of the algorithms specified in this document	6.4.3	M	Cert-SrvA-C-016 OR Cert-SrvA-C-017
Cert-SrvA-C-016	Signature Algorithms - Capable of verifying signatures made with RSA keys up to and including 2048 bits	6.4.3	O	
Cert-SrvA-C-017	Signature Algorithms - Capable of verifying signatures made with EC keys up to and including 233 bits	6.4.3	O	
NOTE – Only one of Cert-SrvA-C-016 and Cert-SrvA-C-017 need to be implemented, but see also Annex C.1.3.				

C.1.3. TLS Certificate options

This table specifies further certificate-processing requirements for those MEs that support server-authenticated TLS sessions.

Item	Function	Reference	Status	Requirements
Cert-TLS-C-001	Signature Algorithms - Capable of verifying signatures made with RSA keys up to and including 2048 bits	6.4.3	M	

C.2 Certificate-processing application Option

This section specifies requirements on certificate processing WAP applications not located in the ME, e.g. WTLS servers.

C.2.1 General Certificate Options

This table specifies generic certificate-processing requirements. In the table, “M” stands for “Mandatory to implement” and “O” stands for “Optional.

Item	Function	Reference	Status	Requirements
Cert-Gen-S-001	General X.509 Certificate support - Parsing of all fields	6	M	
Cert-Gen-S-002	General X.509 Certificate support - Able to handle certificates at least up to 2000 bytes long	6	M	
Cert-Gen-S-003	General X.509 Certificate support - Capable of processing certificates with unknown distinguished name attributes (e.g. needed for chain building)	6	M	
Cert-Gen-S-004	Verification - Certificate path processing as defined in [7] (and [8]).	6.1	M	
Cert-Gen-S-005	Issuer Name - Recognize the following required RFC 2459 attributes: **countryName, organizationName, organizationalUnitName, commonName, stateOrProvinceName, domainComponent**	6.2, 6.3	M	
Cert-Gen-S-006	Issuer Name - Recognize all recommended RFC 2459 attributes: **localityName, title, surname, givenName, initials, generationQualifier**	6.2, 6.3	O	
Cert-Gen-S-007	Issuer Name - Recognize the **serialNumber** attribute	6.2, 6.3	M	
Cert-Gen-S-008	Subject Name - Recognize the following required RFC 2459 attributes: **countryName, organizationName, organizationalUnitName, commonName, stateOrProvinceName, domainComponent**	6.2, 6.3	M	
Cert-Gen-S-009	Subject Name - Recognize all recommended RFC 2459 attributes: **localityName, title, surname, givenName, initials, generationQualifier**	6.2, 6.3	O	
Cert-Gen-S-010	Subject Name - Recognize the **serialNumber** attribute	6.2, 6.3	M	
Cert-Gen-S-011	Extensions - Recognize and process extensions as specified in this document	6	M	
Cert-Gen-S-012	Extensions - Recognize and process the **domainInformation** extension	10	O	
Cert-Gen-S-013	Signature Algorithms - Capable of processing certificates signed with at least one of the algorithms specified in this document	9	M	Cert-Gen-S-014 OR Cert-Gen-S-015
Cert-Gen-S-014	Signature Algorithms - Capable of verifying signatures made with RSA keys up to and including 2048 bits	6.6.5	O	

Item	Function	Reference	Status	Requirements
Cert-Gen-S-015	Signature Algorithms - Capable of verifying signatures made with EC keys up to and including 233 bits	6.6.5	O	
Cert-Gen-S-016	Chain Processing - Process certificate chains of at least 3	6.1	M	
NOTE – Only one of Cert-Gen-S-014 and Cert-Gen-S-015 need to be implemented.				