Specification Information Note

WAP-261_102-WTLS-20011027-a

Version 27-Oct-2001

for

Wireless Application Protocol
WAP-261-WTLS-20010406-a
Wireless Transport Layer Security
Version 06-April-2001

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

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

- WAP-261-WTLS-20010406-a

It includes changes from the following change requests:

- Change Request Ericsson-Bangkok-2001-CR-No2 2001-09-27

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. Correction of usage of key_identifier in the certificate request

3.1 Change Classification

Class 2 – Bug Fix

3.2 Change Summary

The server can optionally request a certificate from the client, and in this message the server can tell the client which certificate that shall be sent back to the server. This is done by using the different identifier types (0=no identity supplied, 1=textual name, 2=binary identity, 254=SHA-1 hash of public key, 255=X.509 distinguished name). The proposal is to reduce the set to the following identifier types:

- 0, no identity supplied
- 254, SHA-1 hash of public key. Mandatory for WTLS.
- 255, X.509 distinguished name. Mandatory for TLS (already the only option).

Indexing on the WIM is the main reason for the change, i.e. the identifier sent in server hello should be the identifier used as an index on the WIM.

If this approach is not taken the client will have to parse the certificates stored on the WIM in order to make the match, this will of course add complexity and make the operation more time consuming. For WTLS certificates parsing is not an issue since this is mandatory functionality for clients anyway. Without the suggested change a serious problem could arise when the client must look for a client certificate not using the identifier on the WIM. This will require the client to parse X.509 certificates. It seems to be overkill to include a X.509 parser just to search for certificates.

3.3 Change Description

Editor's note: On pages 69-70

10.5.4 Certificate Request

Item	Description
trusted_authorities	A list of the ~~names and types~~ identifiers of acceptable certificate authorities. These ~~names~~ identifiers may specify a desired ~~id for a~~ root CA or ~~for a~~ subordinate CA; thus, this message can be used both to describe known roots and a desired authorisation space. The identifier type shall be limited to the following values: • 0, no identity supplied • 254, SHA-1 hash of public key. If no authorities are sent, client may send any certificate, or if the client supplied a key identifier in ClientHello.client_key_ids, the client should use the corresponding key for authentication but send no certificates. This corresponds to the case when the client certificate is known to the server by the key identifier. Fetching client certificate by the key identifier (public key hash) may be possible e.g., when client certificates are contained in a local cache, or if certificates contain the key identifier (as subject key identifier) and search on this field is enabled. The server may request the client to send any certificate for a particular key exchange suite by sending this message with a KeyExchangeId that has Identifier.identifier_type null.