Specification Information Note

WAP-261_100-WTLS-20010926-a

Version 26-Sept-2001

for

Wireless Application Protocol
WAP-261-WTLS-20010406-a

Wireless Transport Layer Security
Version 06-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-261-WTLS-20010406-a

It includes changes from the following change requests:

- Change Request Ericsson-2 2001-07-23

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. Clarification on when a WAP server shall send a server certificate to the client

3.1 Change Classification

Class 3 – Clerical Corrections

3.2 Change Summary

In the Chapter Server Certificate,

"The key exchange list contains the cryptographic key exchange algorithms supported by the client in decreasing order of preference. In addition, each entry defines the certificate or public key the client wishs to use. The server will select one or, if no acceptable choices are presented, return a handshake_failure alert and close the secure connection. The trusted authorities list with a similar format identifies the trusted certificates known by the client."

The interpretation of this sentence is that if the client sends a list of certificates that the client knows about, the server shall choose one of the certificates in the list. If the server doesn't support any of the certificates in the list the server shall choose to do an anonymous handshake. The server shall not send a server certificate to the client to which the client doesn't have the corresponding CA certificate. Sending "unknown" server certificates shall only be allowed when the client has sent no CA identifiers to the server at the same time as a non-anonymous handshake is suggested as one of the handshake options.

This has no impact on backward compatibility.

3.3 Change Description

Editor's note: On page 56 and 63

Add the following sentences to clarify when a WAP server shall sent a server certificate to a client:

10.5.1.2 Client Hello:

When this message will be sent:

> When a client first connects to a server it is required to send the client hello as its first message. The client can also send a client hello in response to a hello request or on its own initiative in order to renegotiate the security parameters in an existing secure connection.

Structure of this message:

The key exchange list contains the cryptographic key exchange algorithms supported by the client in decreasing order of preference. In addition, each entry defines the certificate or public key the client wishes to use. The server will select one or, if no acceptable choices are presented, return a *handshake_failure* alert and close the secure connection. The trusted authorities list with a similar format identifies the trusted certificates known by the client. Any server certificate sent in a subsequent Server Certificate message must be issued by one of the trusted authorities indicated in this message. The server is allowed to breach this rule only when the client suggests a non-anonymous handshake and leaves the trusted authorities list empty.

10.5.2 Server Certificate:

When this message will be sent:

If sent this message must always immediately follow the server hello message.

Meaning of this message:

The certificate type must be appropriate for the selected key exchange suite's algorithm. It can be a X.509v3 certificate [X509], a WTLS certificate which is optimised for size, or a X9.68 certificate (note: this certificate type has not been defined at the point of time of publication of this specification). Other certificate types may be added in the future. It must contain a key, which matches the key exchange method, as follows. Unless otherwise specified, the signing algorithm for the certificate must be the same as the algorithm for the key carried in the certificate. Unless otherwise specified, the public key may be of any length. The server certificate sent in this message must be issued by one of the trusted authorities indicated in the previous Client Hello. The server is allowed to breach this rule only when the client suggests a non-anonymous handshake and leaves the trusted authorities list empty.