Specification Information Note
WAP-261_101-WTLS-20011027-a

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.

Contents

1. SCOPE..................................................................................................................................................................................4

2. NOTATION .............................................................................................................................................................................4

3. CLARIFICATION OF HOW TO CALCULATE THE HASH OF A PUBLIC KEY FOR THE
   KEY_HASH IDENTIFIER TYPE ................................................................................................................................................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-261-WTLS-20010406-a

It includes changes from the following change requests:
- Change Request Ericsson-Bangkok-2001-CR-No1 2001-09-26

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 of how to calculate the hash of a public key for the key_hash identifier type

3.1 Change Classification

Class 3 – Clerical Corrections

3.2 Change Summary

The current description of the public key hash calculation is quite open for interpretation.

We have interpreted the specifications in that the hash is calculated on the raw (unsigned) public key modulus as it is stored in a WTLS certificate. The rationale for regarding it that way is that the public key identifier is the same for the same key stored in both a WTLS and a X.509 certificate.

This has no impact on backward compatibility.

3.3 Change Description

Editor's note: On page 60

Add the following sentences to clarify how to calculate the hash of a public key for the key_hash identifier type:

10.5.1.2 Client Hello

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identifier_type</td>
<td>Type of identifier used</td>
</tr>
<tr>
<td></td>
<td>0 = no identity supplied</td>
</tr>
<tr>
<td></td>
<td>1 = textual name with character set</td>
</tr>
<tr>
<td></td>
<td>2 = binary identity</td>
</tr>
<tr>
<td></td>
<td>254 = SHA-1 hash of the public key</td>
</tr>
<tr>
<td></td>
<td>255 = X.509 distinguished name</td>
</tr>
<tr>
<td>character_set</td>
<td>Maps to IANA defined character set.</td>
</tr>
<tr>
<td>Name</td>
<td>Textual name.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Binary identifier.</td>
</tr>
<tr>
<td>key_hash</td>
<td>Hash of the public key of the key pair which the client intends to use in the handshake to prove its identity.</td>
</tr>
<tr>
<td></td>
<td>For RSA, the SHA-1 hash is to be done on the byte string representation of the public modulus [PKCS1], i.e. the hash is calculated on the raw value of the public key omitting the sign byte and ASN.1 encoding.</td>
</tr>
<tr>
<td></td>
<td>For ECC, the SHA-1 hash is to be done on the byte string representation of the x-coordinate of the elliptic curve point [X9.62].</td>
</tr>
<tr>
<td>distinguished_name</td>
<td>X.509 distinguished name.</td>
</tr>
</tbody>
</table>