# Specification Information Note

## WAP-261_101-WTLS-20011027-a

Version 27-Oct-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.

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** ........ **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**

| Item | Description |
|---|---|
| identifier_type | Type of identifier used<br>0 = no identity supplied<br>1 = textual name with character set<br>2 = binary identity<br>254 = SHA-1 hash of the public key<br>255 = X.509 distinguished name |
| character_set | Maps to IANA defined character set. |
| Name | Textual name. |
| Identifier | Binary identifier. |
| key_hash | Hash of the public key of the key pair which the client intends to use in the handshake to prove its identity.<br>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.<br>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]. |
| distinguished_name | X.509 distinguished name. |