3GPP TSG SA WG3 Security — SA3#36 **S3-040962**
23 – 26 November 2004
Shenzhen, China

Source: **Ericsson**

Title: **Including AES in the TLS profile of TS 33.222**

Document for: **Discussion/Decision**

Agenda Item: **GAA/HTTPS**

1 Introduction

This contribution proposes to include an AES CipherSuite in the TLS profile of TS 33.222

2 Discussion

At SA3 #32, a TLS profile was agreed for TS 33.141 in S3-040169 [1]. The TLS profile was agreed also for TS 33.222 at SA3 #33 in S3-040323 [2]. Consequently, it was agreed to avoid overlaps between these two TSs, so the TLS profile in 33.141 was removed and replaced by a reference to TS 33.222

At SA3 #32, it was also agreed to ask OMA to update WAP profiles to include AES (LS in S3-040194) [2]. The response LS from OMA [3] informed that OMA are not working on updating WAP profiles. The LS however noted that "WAP-219 allows for other cipher suites, e.g., AES (see section 6.1)".

SA3 has thus far taken the approach that several algorithms should be supported by security mechanisms used in 3GPP. The IPsec/IKE profiles in TS 33.210 mandates the use of both 3DES and AES in CBC mode. Likewise, AES and 3DES are mandated for confidentiality protection using IPsec in TS 33.203.

TS 33.222 currently mandates support of "TLS_RSA_ WITH_3DES_EDE_CBC_SHA" for the UE. The NAF should support "TLS_RSA_ WITH_3DES_EDE_CBC_SHA" and "TLS_RSA_WITH_RC4_128_SHA". It is considered good security practice to support several security algorithms in a protocol. Thus, in-line with this security practice, and in-line with the SA3 practice used in TSs 33.210 and 33.203, we think that it would be useful to mandate the support of "TLS_RSA_WITH_AES_128_CBC_SHA" in the TLS profile of TS 33.222.

3 Proposal

We propose that the TLS profile in TS 33.222 should be amended with mandatory support for the "TLS_RSA_WITH_AES_128_CBC_SHA" CipherSuite. An accompanying CR implements the required changes.

4 References

[1] 3GPP SA WG3, Security Mechanisms for Presence, S3-040169, 2004

[2] 3GPP SA WG3, Definition of TLS profile for shared key based UE authentication according to clause 5.3 of TS 33.222 – Pseudo-CRs to 33.222 and 33.141, S3-040323, 2004

[3] 3GPP SA WG3, LS on Presence Security, S3-040194, 2004