3GPP TSG SA WG3 Security — SA3#36 **S3-040964**
23 – 26 November 2004
Shenzhen, China

Source:	**Ericsson**
Title:	**Postponing PSK TLS to 3GPP rel-7**
Document for:	**Discussion/Decision**
Agenda Item:	**GAA/HTTPS**

1 Introduction

This contribution proposes to postpone PSK TLS to release 7, according to the SA3 agreement that PSK TLS should be postponed if the Internet Draft [1] is not ready when release 6 is frozen.

2 Discussion

TS 33.220 v 6.1.0 contains the following editor's note in section 5.4:

> Editor's note: If the "Pre-Shared Key Ciphersuites for TLS" Internet Draft [15] does not reach the RFC status by the time when Release 6 is frozen, this subclause shall be removed and the support for the Pre-Shared Key TLS is postponed to Release 7.

The PKS TLS Internet Draft [1] has undergone Working Group Last Call and a new version of the Internet Draft needs to be prepared based on the comments from the Last Call. After the new draft has been composed based on the new comments, the Area Director needs to approve the document for IESG evaluation. The IESG needs to evaluate and approve the draft. The draft finally needs to be sent to the RFC editor, and the editor needs to take the necessary steps required for publication as an RFC.

Although PSK TLS has made good progress within IETF, it is still uncertain whether PSK TLS will reach RFC status in release 6 time frame. Therefore, we think that TS 33.222 should be updated to remove PSK TLS from release 6, according to earlier SA3 agreements as indicated in the editor's note of section 5.4.

Consequently, to clean up TS 33.222 for release 6, we propose that all the editor's notes related to PSK TLS are removed.

3 Proposal

We propose to postpone introduction of PSK TLS to release 7 in case PSK TLS has not reached RFC status until SA #26, according to the earlier SA3 agreement to postpone PSK TLS unless the Internet Draft has reached RFC status when rel-6 is frozen. We also propose to remove editor's notes related to PSK TLS from TS 33.222. The accompanying CR implements these changes.

4 References

[1] IETF Internet-Draft: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", September 28, 2004, URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-psk-02.txt.