3GPP TSG SA WG3 Security — S3#32 **S3-040090**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: **6.10 (WLAN)**

Source: **Siemens**

Title: **PDG authentication with IKEv2 in scenario 3: clarification - Pseudo-CR**

Document for: **Discussion and decision**

Abstract

It has been clarified at the IETF that IKEv2 with EAP always requires authentication of the server by means of a public key signature. Therefore, the corresponding Editor's note in TS 33.234 can be removed.

Clarification

Section 6.1.5 of TS 33.234 v100 says in an Editor's note that " It is for further study whether Public Key signatures for PDG authentication are needed ".

There has been a discussion on this issue on the IPsec-mailing list of the IETF. The results are contained in a new version of the Internet draft on IKEv2, draft-ietf-ipsec-ikev2-12.txt. This new version contains the following statement which resolves the editor's note:

"An implementation using EAP MUST also use a public key based

authentication of the server to the client before the EAP exchange

begins, even if the EAP method offers mutual authentication. This

avoids having additional IKEv2 protocol variations and protects the

EAP data from active attackers."

The editor's note can therefore be removed.

Remark: the above text does not rule out that it may be possible to define a protocol using IKEv2 with EAP without public key based authentication of the server, but such a protocol would have to be the subject of a new Internet draft.

Proposed Change

6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- The WLAN UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG.

~~Editor's note: It is for further study whether Public Key signatures for PDG authentication are needed.~~

- EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a USIM.

- EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a SIM and no USIM.

- A profile for IKEv2 is defined in section 6.5.

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex X. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex X will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management, in particular, the use of EAP-AKA and EAP-SIM will be studied.