3GPP TSG SA WG3 Security — S3#28 **S3-030177**
6 - 9 May 2003
Berlin, Germany

3GPP TSG SA2 #30 **S2-030995**
Milan, Italy, 24-28.2.2003

Title: LS on Incorporation of re-authentication into TS 33.234
Release: Release 6
Work Item: WLAN Interworking

Source: SA2
To: SA3
Cc:

Contact Person:
Name: Raquel Rodriguez
Tel. Number: + 358405259208
E-mail Address: Raquel.Rodriguez@nokia.com

Attachments: None

---

1. Overall Description:

SA3 and SA2 have agreed on a work split of WLAN interworking between them, where SA3 would focus on security issues and SA2 on architecture. SA2 has agreed to remove overlapping text between TS23.234 and TS33.234 from TS23.234.

SA2 would like to ask SA3 to incorporate re-authentication part of TS23.234 v1.4.0 (see below) into TS33.234.

2 TS23.234 v1.4.0, Section 5.3.5, Re-authentication

On some networks, EAP authentication may be performed frequently. For such cases, EAP SIM and EAP AKA include an optional re-authentication procedure. Re-authentication causes less load on the network and is faster to execute than the full SIM/USIM authentication procedure. Re-authentication is optional to implement for both the WLAN UE and 3GPP AAA server. On each EAP authentication, either one of the entities may also fall back on full authentication if they do not want to use re-authentication. Re-authentication is based on the keys derived on the preceding full authentication.

On re-authentication, the UE protects against replays with an unsigned 16-bit counter. The server includes an encrypted server nonce (NONCE_S) in the re-authentication request. The Message Authentication Code attribute in the client's response is calculated over NONCE_S to provide a challenge/response authentication scheme. The NONCE_S also contributes to the new session keys.

Because one of the objectives of the re-authentication procedure is to reduce load on the network, the re-authentication procedure does not require the 3GPP AAA server to contact a reliable database. Therefore, the re-authentication procedure makes use of separate re-authentication user identities. Pseudonyms and the permanent IMSI-based identity are reserved for full authentication only. The network does not need to store re-authentication identities as carefully as pseudonyms. If a re-authentication identity is lost and the network does not recognize it, the 3GPP AAA server can fall back on full authentication.

If the 3GPP server supports re-authentication, it may communicate an encrypted re-authentication identity for next re-authentication to the WLAN UE during full authentication. If the client wants to use re-authentication, it uses this re-authentication identity on next authentication.

[Editor's note: Section 5.3.5 on re-authentication may be removed once it is incorporated into TS 33.234]

2. Actions:

1. SA2 asks SA3 to consider re-authentication and include it in TS33.234, e.g., by direct incorporation of TS23.234 v1.4.0 Section 5.3.5, Re-authentication into TS33.234.
2. SA2 asks SA3 to inform SA2 of the outcome of the SA3 consideration to allow SA2 for removing Section 5.3.5 from the future versions of TS 23.234.

3. Date of Next TSG–SA2 Meetings:

SA2#31	07 - 11 April 2003,	Korea, Samsung
SA2#32	12 - 16 May 2003,	USA