3GPP TSG SA WG3 Security — S3#34 *Tdoc ⌘S3-040512*
Acapulco, Mexico 6 – 9 July 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR CRNum** ⌘**rev -** ⌘ Current version: **6.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title: ⌘	Sending of temporary identities from WLAN UE	
Source: ⌘	Samsung, Huawei	
Work item code: ⌘	WLAN	***Date:*** ⌘ 23/06/2004
Category: ⌘	**F**	***Release:*** ⌘ Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘	In EAP AKA/SIM internet drafts, it is stated that the WLAN UE can choose whether to use identity privacy support or not. And in the EAP AKA/SIM fast authentication procedure, it is stated that "4 … If the AAA server is not able to deliver a re-authentication identity, next time the WLAN-UE shall force a full-authentication (to avoid the use of the re-authentication identity more than once)." This means that when the AAA server has sent a temporary identity to the WLAN UE, the WLAN UE shall use the re-authentication id only once and mark it as deleted after use. There has been no mention about the case when pseudonym received in the last re-authentication procedure is not used in the next re-authentication attempt either because a re-authentication id is being sent or a permanent id is being requested by the AAA-Server. In these cases the unused pseudonym can be used in the next full re-authentication procedure.
Summary of change: ⌘	It should be stated in 33.234 that the WLAN UE must send a temporary identity whenever it is available and not used in the previous authentication. So a pseudonym received in the previous re-authentication procedure can be used in the full re-authentication procedure if it is not used in earlier re-authentication attempts.
Consequences if not approved: ⌘	WLAN UE may decide to send permanent user identity even unused temporary available, which can end up in passive or active attacks.

Clauses affected: ⌘	5.1.6			
Other specs affected: ⌘	**Y**	**N**		
		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	
Other comments: ⌘				

*** BEGIN SET OF CHANGES ***

5.1.6 User Identity Privacy in WLAN Access

User identity privacy (Anonymity) is used to avoid sending any cleartext permanent subscriber identification information which would compromise the subscriber's identity and location on the radio interface, or allow different communications of the same subscriber on the radio interface to be linked.

User identity privacy is based on temporary identities (pseudonyms or re-authentication identities). The procedures for distributing, using and updating temporary identities are described in ref. [4] and [5]. Support of this feature is mandatory for implementation in the network and WLAN UE. The use of this feature is optional in the network, but mandatory in the WLAN UE.

The AAA server generates and delivers the temporary identity and/or the re-authentication identity to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the temporary identity; it shall just store the received identifier and use it at the next authentication. Clause 6.4 describes a mechanism that allows the home network to include the user's identity (IMSI) encrypted within the temporary identity.

When the WLAN-UE receives one temporary identity issued by the AAA server, it shall use it in the next authentication. The WLAN-UE can only use the permanent identity when there is no temporary identity available in the WLAN-UE. A temporary identity is available for use when it has been received in last authentication process. Temporary identities received in earlier authentication processes have to be cleared in the WLAN-UE or marked so that they can only be used once.

If the WLAN-UE receives from the AAA server more than one temporary identity (a pseudonym and a re-authentication identity), in the next authentication procedure, it will use the re-authentication identity, so that the AAA server is able to decide either to go on with a fast re-authentication or to fallback to a full re-authentication (by requesting the pseudonym to the WLAN-UE). This capability of decision by the AAA server is not possible if the WLAN-UE sends the pseudonym, since the AAA server is not able to request the re-authentication identity if it decides to change to fast re-authentication. If the WLAN UE does not receive any new pseudonym and/or re-authentication id during a re-authentication procedure, the WLAN UE can use a previously unused pseudonym for the next full re-authentication attempt.

For tunnel establishment in scenario 3, fast re-authentication may be used for speed up the procedure. In this case, the WLAN-UE shall use the fast re-authentication identities (as long as the re-authentication identity has been received in the last authentication process).

An exception is when the full authentication is being performed for tunnel establishment in scenario 3, in which case the IMSI may be sent even if identity privacy support was activated by the home network. In this situation, the authentication exchange is performed in a protected tunnel which provides encryption and integrity protection, as well as replay protection.

NOTE: There exist the following risks when sending the IMSI in the tunnel set-up procedure:

- the protected tunnel is encrypted but not authenticated at the moment of receiving the user identity (IMSI). The IKEv2 messages, when using EAP, are authenticated at the end of the EAP exchange. So in case of a man-in-the-middle attack the attacker could be able to see the IMSI in clear text, although the attack would eventually fail at the moment of the authentication;
- the IMSI would be visible for the PDG, which in roaming situations may be in the VPLMN. This is not a significant problem if the home network operator trusts the PDGs owned by the visited network operators.

To avoid user traceability, the user should not be identified for a long period by means of the same temporary identity. On the other hand, the AAA server should be ready to accept at least two different pseudonyms, in case the WLAN-UE fails to receive the new one issued from the AAA server. The mechanism described in Clause 6.4 also includes facilities to maintain more than one allowed pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user to send its permanent identity. This represents a breach in the provision of user identity privacy. It is a matter of the operator's security policy whether to allow clients to accept requests from the network to send the cleartext permanent identity. If the client rejects a legitimate request from the AAA server, it shall be denied access to the service.

Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.

*** END SET OF CHANGES ***