TSGS#24(04)0385

Source: SA WG3 (Security)

Title: CR to 33.234: Sending of temporary identities from WLAN UE (Rel-6)

Document for: Approval

Agenda Item: 7.3.3

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-040385	33.234	002	-	Rel-6	Sending of temporary identities from WLAN UE	F	6.0.0	S3-040416	WLAN

3GPP TSG SA WG3 Security — S3#33 *Tdoc ⌘S3-040416*
Beijing, China 10 - 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Sending of temporary identities from WLAN UE
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	03/05/2004
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. This means that when the AAA server has sent a temporary identity to the WLAN UE, the latter can choose to use a permanent identity in the next authentication process instead of the temporary identity. The sending of the permanent user identity (the IMSI) has to be avoided as much as possible, so that a passive or active attacker is not able to trace user's activity or launch any other kind of attack.
Summary of change:	⌘	It will be stated in 33.234 that the WLAN UE must send a temporary identity whenever it is available. The use of a permanent user identity will be done only when a temporary identity is not available, or when the AAA server requests it explicitly.
Consequences if not approved:	⌘	WLAN UE may decide to send permanent user identity, which can end up in passive or active attacks.

Clauses affected:	⌘	4.2.3 and 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 ***

4.2.3 User identity privacy

- ~~-~~Any secret keys used in 3G AAA servers for the generation of ~~pseudonyms~~ temporary identities should be infeasible for an attacker to recover.
- It shall be infeasible for an attacker to recover the corresponding permanent identity, given any ~~pseudonym~~temporary identity(s).
- It should be infeasible for an attacker to determine whether or not two ~~pseudonyms~~ temporary identities correspond to the same permanent identity.
- ~~-~~It shall be infeasible for an attacker to generate a valid ~~pseudonym~~temporary identity.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.6 User Identity Privacy in WLAN Access

User identity privacy (Anonymity) is used to avoid sending the cleartext permanent subscriber identity (NAI) and make the subscriber's connections unlinkable to eavesdroppers.

User identity privacy is based on temporary identities~~, or~~ (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 implementations, but optional for use.

The AAA server generates and delivers the ~~pseudonym~~ temporary identity to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the ~~pseudonym~~temporary identity, it will 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 ~~pseudonym~~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.

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 will be denied access to the service.

*** END SET OF CHANGES ***