3GPP TSG SA WG3 Security — S3#35 *Tdoc ⌘S3-040763*
October 5 – 8, 2004

St Paul's Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **028** ⌘**rev** **-** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Passing keying material to the WLAN-AN during the Fast re-authentication procedure
Source:	⌘	Samsung
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:	⌘	According to the current specification, the newly generated keying material after the fast re-authentication is not transmitted to the WLAN-AN. WLAN-AN cannot refresh the WEP key after the fast re-authentication procedure.
Summary of change:	⌘	It is necessary to pass the newly derived key materials from the AAA server to the WLAN AN with the EAP-success message after the Fast re-authentication procedure, so that WLAN AN stores the keying material to be used in communication with the authenticated WLAN-UE.
Consequences if not approved:	⌘	UE and WLAN AN will have different keying material after Fast re-authentication procedure. So communcation with the authenticated WLAN-UE is not possible.

Clauses affected:	⌘	6.1.4

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

*** BEGIN SET OF CHANGES ***

6.1.4 Fast re-authentication mechanisms in WLAN Access

When authentication processes have to be performed frequently, it can lead to a high network load especially when the number of connected users is high. Then it is more efficient to perform fast re-authentications. Thus the re-authentication process allows the WLAN-AN to authenticate a certain user in a lighter process than a full authentication, thanks to the re-use of the keys derived on the previous full authentication.

The re-use of keys from previous authentication process shall be performed as follows: the "old" Master Key is fed into a pseudo-random function (as in full authentication) to generate a new Master Session Key (MSK) and a new Extended MSK. In this process, new Transient EAP Keys (TEKs) are generated but shall be discarded. The TEKs, needed to protect the EAP packets, shall be the "old" ones. So the EAP packets shall be protected with the same keys as in the previous full authentication process but the link layer key in the WLAN access network are renewed as the MSK (from which the link layer key is extracted) is generated again.

This process implies that the AAA server, after a full authentication process when a re-authentication identity has been issued, shall store the keys needed in case the next authentication is fast re-authentication: MK, TEKs and Counter (in case there has been previous fast-authentications). When the WLAN-UE has completed a full authentication where it has received the re-authentication identity, it shall store the same data in order to be prepared for fast re-authentication.

6.1.4.1 EAP/AKA procedure

The implementation of EAP/AKA must include the fast re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies, which shall be enforced by the AAA server by means of sending the re-authentication identity in any authentication process. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

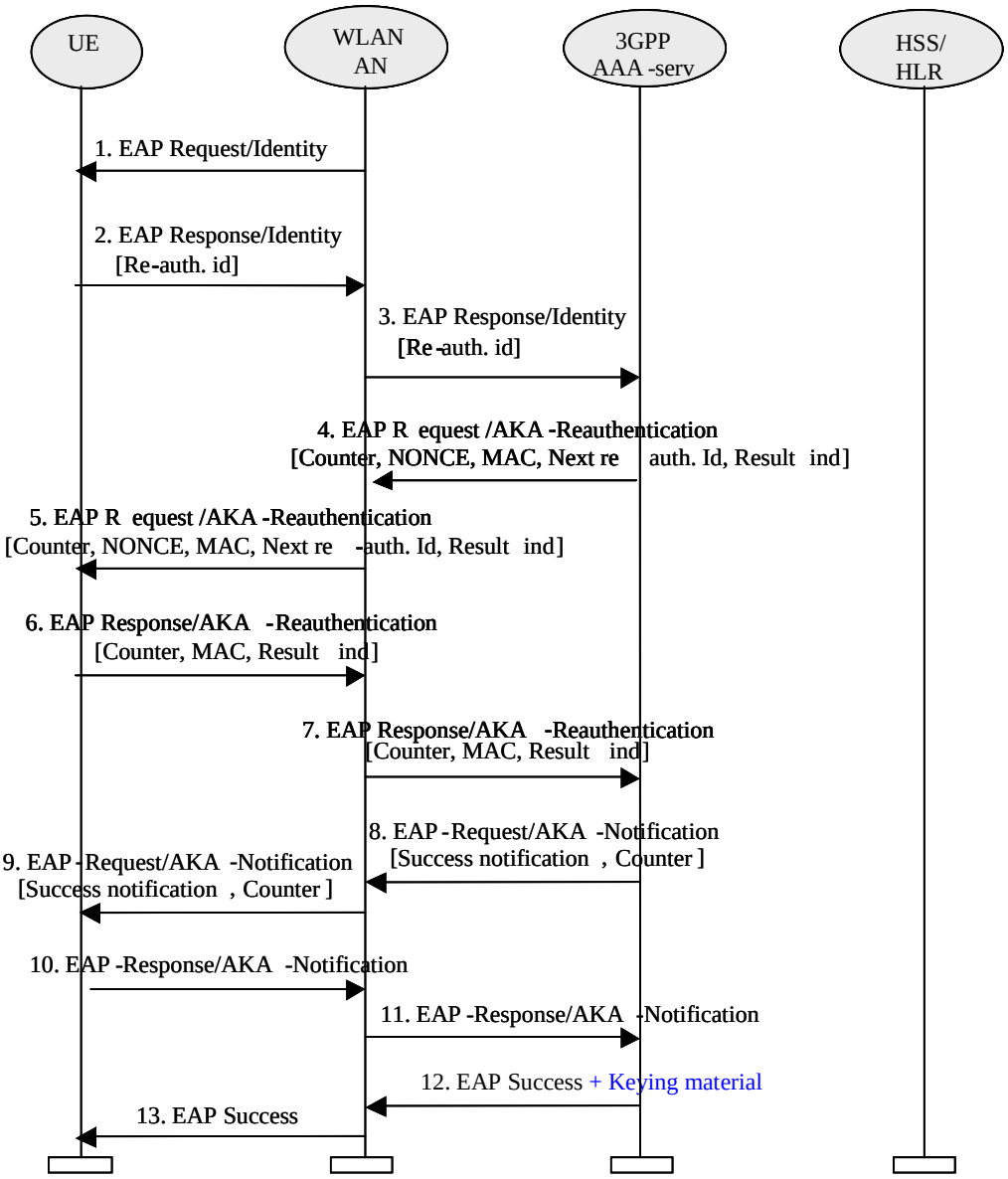

Figure 6: EAP-AKA fast re-authentication

1. WLAN-AN sends an EAP Request/Identity to the WLAN-UE.

2. WLAN-UE replies with an EAP Response/Identity containing a re-authentication identity (this identity was previously delivered by AAA server in a full authentication procedure).

3. The WLAN-AN forwards the EAP Response/Identity to the AAA server.

4. The AAA server initiates the Counter (which was initialized to one in the full authentication process) and sends it in the EAP Request message, together with the NONCE, the MAC (calculated over the NONCE) and a re-authentication id for a next fast re-authentication. 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).

   The 3GPP AAA Server may send as well a result indication to the WLAN-UE, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator's policies.

5. The WLAN-AN forwards the EAP Request message to the WLAN-UE.

6. The WLAN-UE verifies that the Counter value is fresh and the MAC is correct, and it sends the EAP Response message with the same Counter value (it is up to the AAA server to step it up) and a calculated MAC.

The WLAN-UE shall include in this message the result indication if it received the same indication from the 3GPP AAA. Otherwise, the WLAN-UE shall omit this indication.

7. The WLAN-AN forwards the response to the AAA server.
8. The AAA server verifies that the Counter value is the same as it sent, and the MAC is correct, and sends the message EAP Request/AKA-Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected success result indications. The message EAP Request/AKA-Notification is MAC protected, and includes an encrypted copy the Counter used in the present re-authentication process.
9. The WLAN AN forwards the EAP Request/AKA-Notification message to the WLAN-UE.
10. The WLAN-UE sends the EAP Response/AKA-Notification.
11. The WLAN AN forwards the EAP Response/AKA-Notification message to the 3GPP AAA server. The 3GPP AAA Server shall ignore the contents of this message.
12. The AAA server sends an EAP Success message. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection, then the 3GPP AAA Server includes this derived keying material in the underlying AAA protocol message. (i.e. not at EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.
13. The EAP Success message is forwarded to the WLAN-UE.

The re-authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP-AKA process will be terminated as specified in ref. [4] and an indication shall be sent to HSS/HLR.

6.1.4.2 EAP/SIM procedure

The implementation of EAP/SIM must include the fast re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies, which shall be enforced by the AAA server by means of sending the re-authentication identity in any authentication process. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

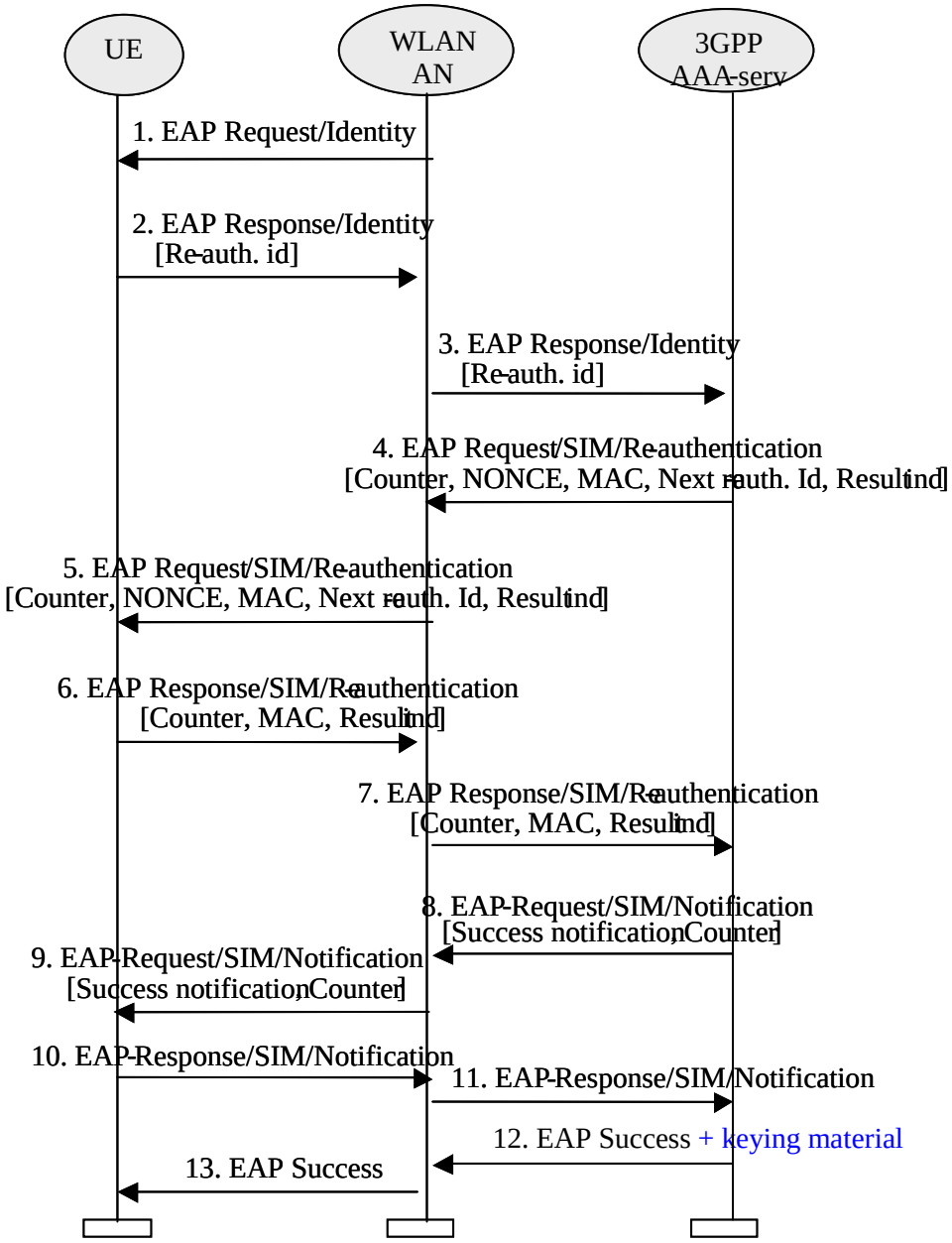

Figure 7: EAP SIM Fast re-authentication

1. WLAN-AN sends an EAP Request/Identity to the WLAN-UE.
2. WLAN-UE replies with an EAP Response/Identity containing a re-authentication identity (this identity was previously delivered by AAA server in a full authentication procedure).
3. The WLAN-AN forwards the EAP Response/Identity to the AAA server.
4. The AAA server initiates the Counter (which was initialised to one in the full authentication process) and sends it in the EAP Request message, together with the NONCE, the MAC (calculated over the NONCE) and a re-authentication id for a next fast re-authentication. 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).

   The 3GPP AAA Server may send as well a result indication to the WLAN-UE, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator's policies.
5. The WLAN-AN forwards the EAP Request message to the WLAN-UE.

6. The WLAN-UE verifies that the Counter value is fresh and the MAC is correct, and it sends the EAP Response message with the same Counter value (it is up to the AAA server to step it up) and a calculated MAC.

   The WLAN-UE shall include in this message the result indication if it received the same indication from the 3GPP AAA server. Otherwise, the WLAN-UE shall omit this indication.

7. The WLAN-AN forwards the response to the AAA server.

8. The AAA server verifies that the Counter value is the same as it sent, and the MAC is correct, and sends the message EAP Request/SIM/Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected success result indications. The message EAP Request/SIM/Notification is MAC protected, and includes an encrypted copy the Counter used in the present re-authentication process.

9. The WLAN AN forwards the EAP Request/AKA-Notification message to the WLAN-UE.

10. The WLAN-UE sends the EAP Response/SIM/Notification.

11. The WLAN AN forwards the EAP Response/SIM/Notification message to the 3GPP AAA server. The 3GPP AAA Server shall ignore the contents of this message.

12. The AAA server sends an EAP Success message. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection, then the 3GPP AAA Server includes this derived keying material in the underlying AAA protocol message. (i.e. not at EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

13. The EAP Success message is forwarded to the WLAN-UE.

The re-authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP SIM process will be terminated as specified in ref. [5] and an indication shall be sent to HSS/HLR.

*** END SET OF CHANGES ***