TSGS#24(04)0388

Source: **SA WG3 (Security)**

Title: **CR to 33.234: Introduction of UE split alternative 2 in TS 33.234 (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-040388	33.234	005	-	Rel-6	Introduction of UE split alternative 2 in TS 33.234	F	6.0.0	S3-040437	WLAN

3GPP TSG SA WG3 Security — S3#33 *Tdoc ⌘S3-040437*
Beijing, China 10 - 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **005** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Introduction of UE split alternative 2 in TS 33.234
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 SA3#32 meeting it was agreed to use alternative 2 for the UE-split problem. This alternative claims that when the WLAN UE is split into a terminal equipment (e.g. a laptop) and a mobile terminal (e.g. a phone), the EAP procedures are terminated in the MT, and when they are finished, the master session key is derived and sent to the TE for usage in link layer security. The purpose of this CR is to reflect that decision in the TS 33.234.
Summary of change:	⌘	Section 4.2.4 removes several open issues, and new chapters 5.2 and 6.2 are created to reflect the mechanism.
Consequences if not approved:	⌘	A lack of definition of split of work between TE and MT can lead to proprietary solutions which may cause vulnerabilities in the TE-MT interface.

Clauses affected:	⌘	4.1.4, 4.2.4.1, 5.6 and 6.7 (both new)

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

Other comments:	⌘	

*** BEGIN SET OF CHANGES ***

4.1.4 Network elements

The list below describes the access control related functionality in the network elements of the 3GPP-WLAN interworking Reference Model:

- The **WLAN-UE**, equipped with a UICC (or SIM card), for accessing the WLAN interworking service):
  - May be capable of WLAN access only;
  - May be capable of both WLAN and 3GPP System access;
  - May be capable of simultaneous access to both WLAN and 3GPP systems;

NOTE: ~~Editors note~~: ~~definition~~ Definition of simultaneous access ~~still TBA with SA1 LS in S3-030169] Reply to SA2 in S3-030188 provides some clarification~~ is specified in TS 23.234 [13].

  - May be a laptop computer or PDA with a WLAN card, UICC (or SIM card) card reader, and suitable software applications;
  - May be functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface;

~~Editors note: All these alternatives must be carefully studied from a security perspective.~~

- The **AAA proxy** represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server. These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.
  The number of intermediate AAA proxies is not restricted by 3GPP specifications. The AAA proxy functionality can reside in a separate physical network node; it may reside in the 3GPP AAA server or any other physical network node;
- The **3GPP AAA server** is located within the 3GPP network. The 3GPP AAA server:
  - Retrieves authentication information from the HLR/HSS of the 3GPP subscriber's home 3GPP network;
  - Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies;
  - Communicates authorisation information to the WLAN potentially via AAA proxies.
- The **Packet Data Gateway (PDGW)** enforces tunnel authorization and establishment with the information received from the 3GPP AAA via the Wm interface.

NOTE: The **WLAN Access Gateway (WAG)** responsibilities for security issues are related to tunnel establishment but this decision is pending to be taken.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.2.4 WLAN-UE Functional Split

4.2.4.1 General

In the case when the WLAN-UE, equipped with a UICC (or SIM card), for accessing the WLAN interworking service, is functionally split over several physical devices, one device holding the card, and one device providing the WLAN access, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface, then is shall be:

- Possible to re-use existing UICC and GSM SIM cards; and
- The UE functional split shall be such that attacking the CS or PS domain of GSM or UMTS by compromising the device providing the WLAN access is at least as difficult as attacking the CS or PS domain by compromising the card holding device.

~~Editors note: The requirement is fulfilled if at least the master keys for EAP-AKA and EAP-SIM, as specified in [4] and [5], are computed either on the card or in the card holding device.~~

~~Editor's note: The termination point of EAP is for further study e.g. if EAP-AKA and EAP-SIM shall terminate in the TE e.g. laptop computer. The decision on the termination point shall take into account the requirements in this subsection.}. LS sent to Bluetooth Architecture Review Board (BARB), Bluetooth CAR group and Bluetooth Security Expert Group in S3-030780.~~

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.6 WLAN UE functionality split

The WLAN UE may consist of several devices. When there is more than one, it will be typically a WLAN Terminal Equipment (e.g. a laptop) and a Mobile Terminal (e.g. a mobile phone) equipped with a UICC or SIM card.

The WLAN TE will provide WLAN access, while the MT or UICC or SIM card will implement the authentication as the EAP termination, which includes key derivation and identity handling. The termination point of EAP shall always be the MT. When any authentication process is finished (in the MT), the resulting key will be sent to the WLAN TE in order to be used for link layer security in the WLAN access.

Note: It shall be possible to have the termination of EAP in the UICC (or SIM card). Details are FFS.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.7 WLAN UE split interworking

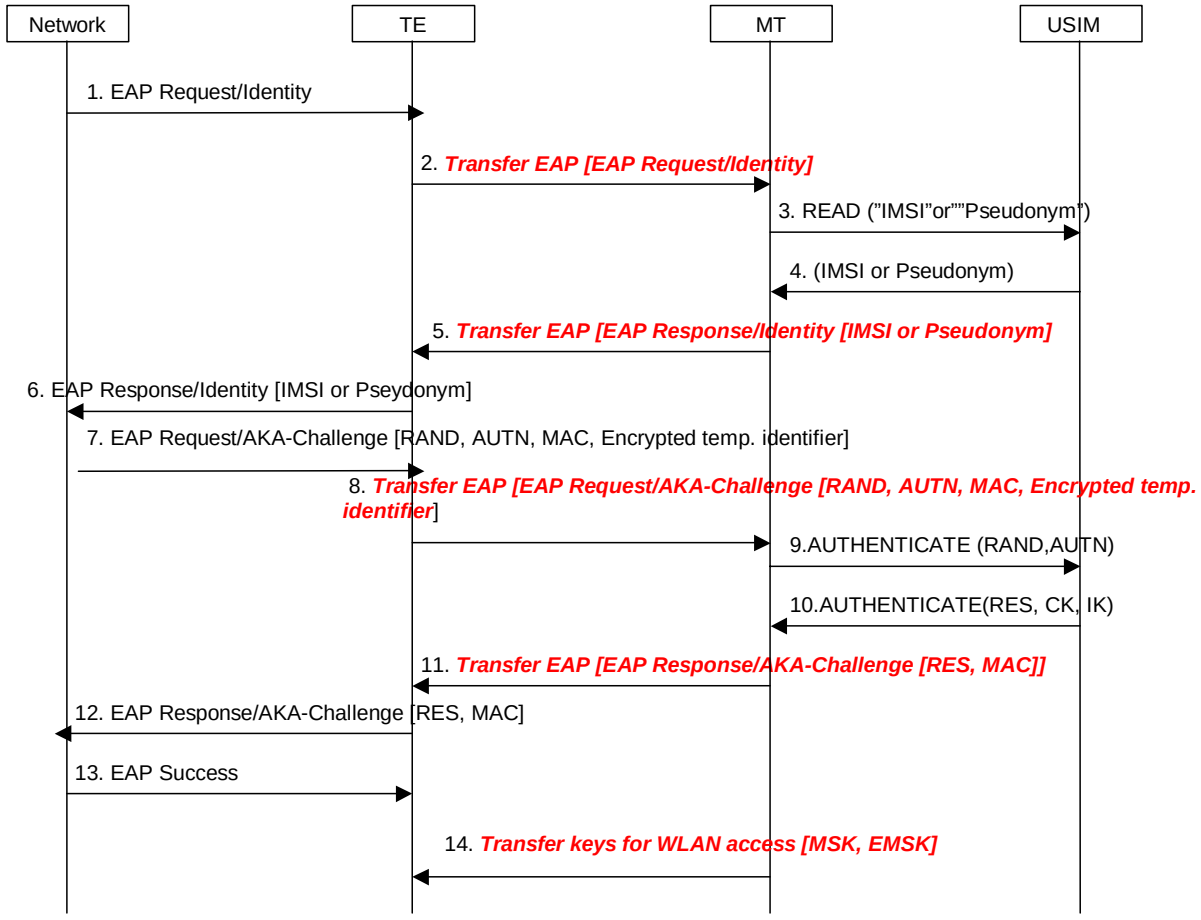
EAP-AKA/SIM procedures terminate in the MT, so the TE shall contact the MT via protected local interface (e.g. Bluetooth) at any authentication or re-authentication process. The Bluetooth interface acts as a transparent carrier of the EAP methods; the TE just forwards messages from the MT to the network (or in the opposite direction) and does not

take active part in the authentication process. The TE is not able to handle any key except the MSK and/or the EMSK when it receives them at the end of the authentication process. The EAP peer at the network side is any node in the WLAN AN, the VPLMN or the home network. Since the interworking to be described here is at the WLAN UE side, it is not relevant which node is sending/receiving any message in the network side.

Note: It shall be possible to have the termination of EAP in the UICC (or SIM card). Details are FFS.

6.7.1 Full authentication with EAP AKA

The process is shown in the following figure.



1. The network sends a EAP request identity (either a IMSI or a pseudonym) message to the TE (the device providing WLAN access) in order to initiate the procedure
2. The EAP request identity message is forwarded via the Bluetooth interface to the MT
3. If the MT does not have the identity available, it requests the identity from the USIM
4. The USIM returns the identity to the MT
5. The MT inserts the identity in the EAP response identity message and sends it to the network via the TE
6. The TE sends the EAP response identity message to the network
7. The network initiates the EAP AKA authentication process
8. The TE forwards the EAP request to the MT with all the parameters
9. The MT requests authentication vectors from the USIM

10. The USIM replies with the calculated keys CK and IK, which will be used by the MT to derive the Master Key (MK) according to ref. [4]. The USIM also returns RES. The MK is then used as input to generate the keys needed to calculate the MAC of message 8 (which will be checked against the received one) and the new MAC for the next message.

11. The EAP response message includes the RES and the calculated MAC

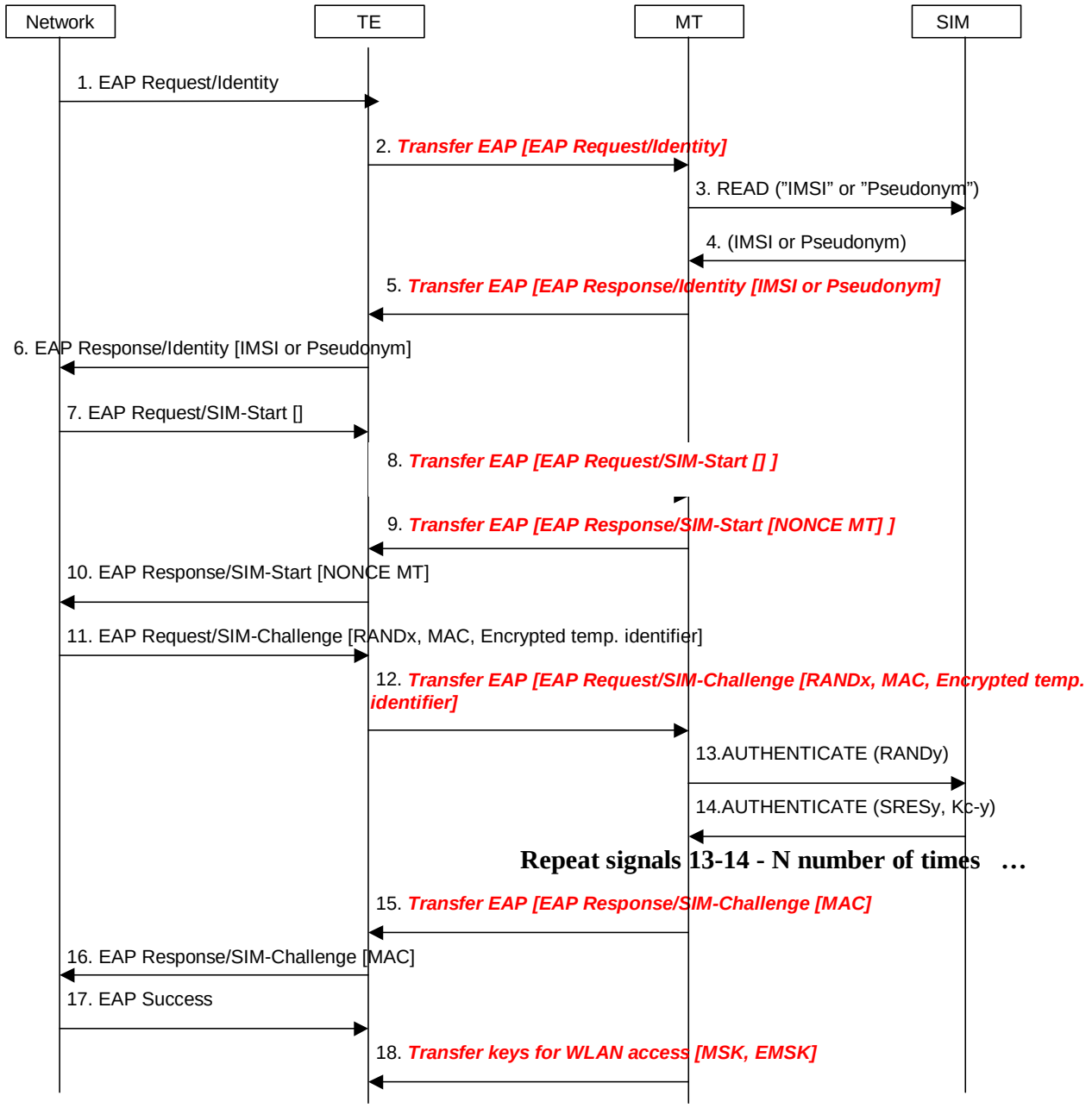
12. The TE forwards the response message to the network, which will check the validity of the RES and compute the MAC of the of the entire message received, comparing it with the received MAC

13. If both checks are correct, the network will send an EAP success message to the TE

14. The MT will derive according to ref. [4] the Master Session Key and Extended Master Session Key (MSK and EMSK) and send them to the TE. The TE uses them for security purposes, for example for WLAN link layer security

6.7.2 Full authentication with EAP SIM

The process is shown in the following figure, and it's very similar to EAP AKA (from MT-TE interface point of view).



1. The network sends a EAP request identity (either a IMSI or a pseudonym) message to the TE (the device providing WLAN access) in order to inititiate the procedure
2. The EAP request identity message is forwarded via the Bluetooth interface to the MT
3. If the MT does not have the identity available, it requests the identity from the USIM
4. The USIM returns the identity to the MT
5. The MT inserts the identity in the EAP response identity message and sends it to the network via the TE
6. The TE sends the EAP response identity message to the network
7. The network initiates the EAP SIM authentication process
8. The TE forwards the EAP SIMstart request to the MT
9. The MT generates a NONCE and sends it to the TE
10. The TE forwards the NONCE to the network, which uses the NONCE to calculate the MAC

11. The network sends an EAP SIM challenge request with the calculated MAC (over the whole EAP message and the NONCE) and the rest of parameters

12. The TE forwards the message to the MT

13. The MT extracts the RAND and sends it to the SIM for key calculation

14. The SIM responds with the calculated SRES and Kc (the two latter messages will be repeated two or three times). The MT will use the received Kcs (among other inputs) to derive the Master Key (MK) according to ref. [5]. The MK is then used as input to generate the keys needed to calculate the MAC of message 11 (which will be checked against the received one) and the new MAC for the next message.

15. The MT sends the EAP SIM challenge response with the MAC, calculated over the whole EAP message and the SRES (the SRES is the concatenated values of the individual SRESy received from the SIM)

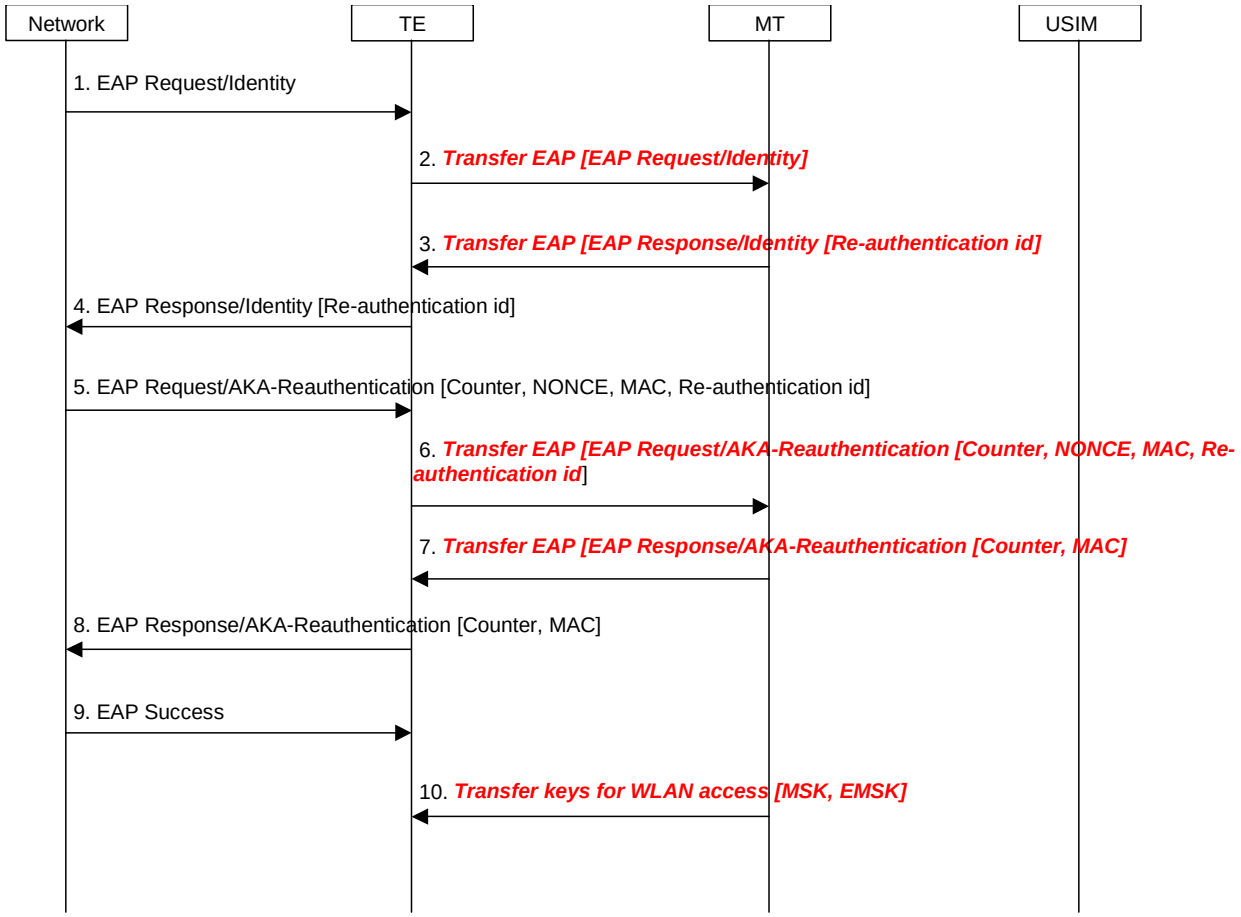
16. The TE forwards the message to the network

17. The network calculates its own copy of the MAC and if it matches the received one, it sends an EAP success message

18. The MT will derive according to ref. [5] the Master Session Key and Extended Master Session Key (MSK and EMSK) and send them to the TE, which will use them for other security purposes, for example WLAN link layer security

6.7.3 Fast re-authentication with EAP AKA

The keys needed to protect the EAP packets are re-used from the previous full authentication process. The MSK and EMSK are calculated again using the original MK, as specified in ref. [4]. For this reason, the new MSK and EMSK are transferred from the MT to the TE when the fast re-authentication process is finished. The process is shown in the following figure.

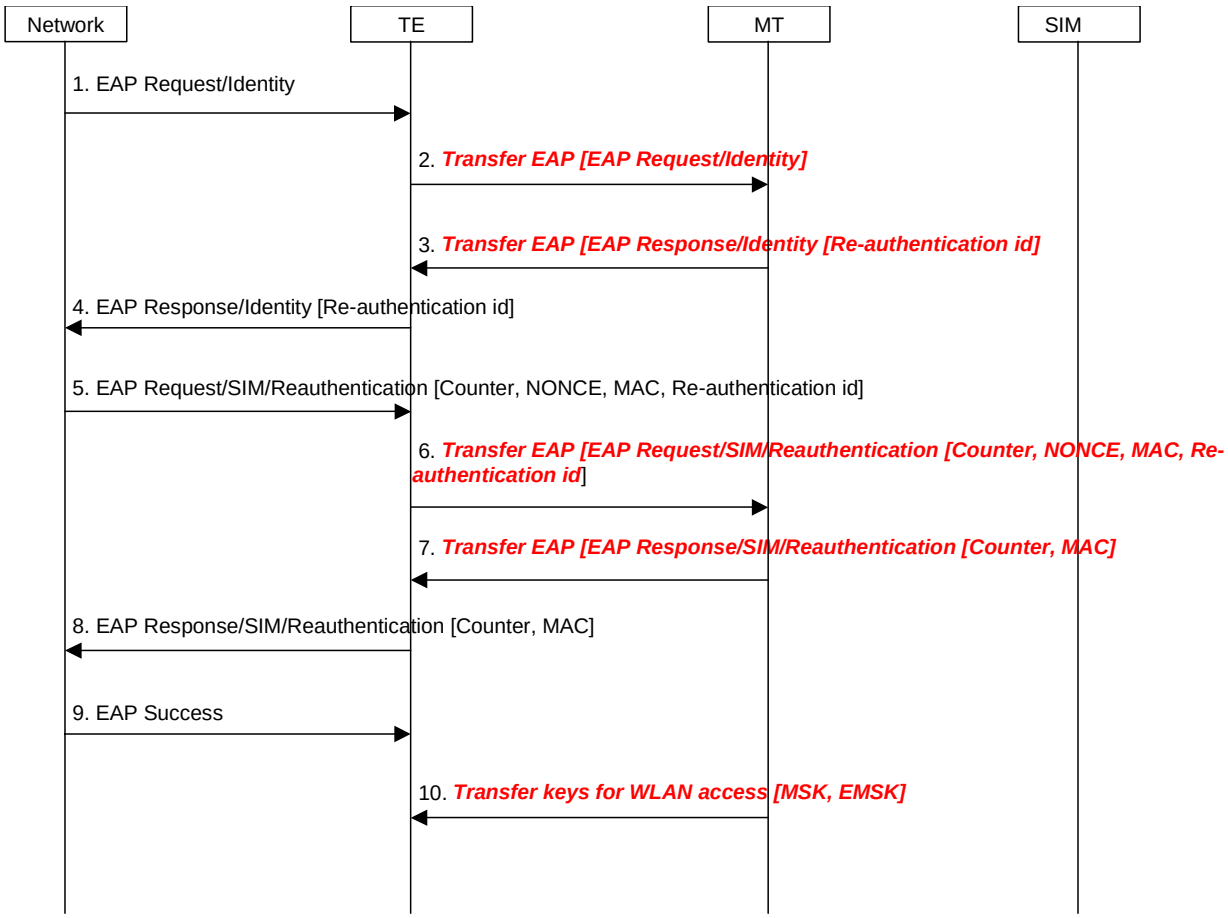


1. The network sends a EAP request identity message
2. The TE forwards the message to the MT via the Bluetooth interface
3. If the MT received a fast re-authentication identity in the last authentication process (either full or fast), it replies with this fast re-authentication identity in the EAP response identity message

   Note: the MT may need to access the USIM to check if there is a re-authentication id available. However, it is still to be decided whether the USIM will store the re-authentication identities
4. The MT forwards the message to the network
5. The network sends the EAP AKA challenge with the needed parameters
6. The TE transfers the message to the MT with the parameters
7. The MT uses the same keys as in the previous authentication process to calculate the MAC, and checks if it matches the received one. If it is correct, it calculates a new MAC and sends it in the response message with the Counter received from the network
8. The TE forwards the response message to the network
9. The network calculates its own copy of the MAC over the received message and checks it with the received one. If it is correct, it sends a EAP success message
10. The MT sends the new calculated MSK and EMSK and sends them to the TE

6.7.4 Fast re-authentication with EAP SIM

The keys needed to protect the EAP packets are re-used from the previous full authentication process, as in EAP AKA fast re-authentication. The MSK and EMSK are calculated again using the original MK, as specified in ref. [5]. The new MSK and EMSK are transferred from the MT to the TE when the fast re-authentication process is finished. The process is shown in the following figure.



1. The network sends a EAP request identity message
2. The TE forwards the message to the MT via the Bluetooth interface
3. If the MT received a fast re-authentication identity in the last authentication process (either full or fast), it replies with this fast re-authentication identity in the EAP response identity message

   Note: the MT may need to access the USIM to check if there is a re-authentication id available. However, it is still to be decided whether the USIM will store the re-authentication identities
4. The MT forwards the message to the network
5. The network sends the EAP AKA challenge with the needed parameters
6. The TE transfers the message to the MT with the parameters
7. The MT uses the same keys as in the previous authentication process to calculate the MAC, and checks if it matches the received one. If it is correct, it calculates a new MAC and sends it in the response message with the Counter received from the network
8. The TE forwards the response message to the network
9. The network calculates its own copy of the MAC over the received message and checks it with the received one. If it is correct, it sends a EAP success message

10. The MT sends the new calculated MSK and EMSK and sends them to the TE

*** END SET OF CHANGES ***