3GPP TSG SA WG3 Meeting S3#35
St Paul's Bay, Malta, 5 – 8 October 2004

Tdoc ⌘S3-040759

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**027**	⌘**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:	⌘	Correction of WLAN UE function split		
Source:	⌘	Axalto, Gemplus		
Work item code:	⌘	WLAN	***Date:*** ⌘	07/09/2004
Category:	⌘	**F**	***Release:*** ⌘	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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	In SA3#32 alternative 2 was chosen as the working assumption for WLAN UE functional split (see S3-040197). However, alternative 2, as presently defined in TS 33.234 is not technically feasible in release 6 since the required standardized API between the TE and the ME does not exist. Therefore, this CR proposes a technically feasible solution to implement WLAN UE functional split as described in alternative 2.
Summary of change:	⌘	Modify the WLAN UE functionnal split to have the termination of EAP in the smart card.
Consequences if not approved:	⌘	Functional split cannot be implemented in release 6 in a standardized manner. This will lead to proprietary implementations, jeopardizing the network and user security as well as interoperability and wide service deployment.

Clauses affected:	⌘	2, 5.6, 6.1.3, 6.1.3.1, 6.1.3.2, 6.7, 6.7.1, 6.7.2, 6.7.3, 6.7.4				
		Y	**N**			
Other specs affected:	⌘			Other core specifications	⌘	
				Test specifications		
				O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 22.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[2] 3GPP TR 23.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] IETF RTC 3748: "Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-12, April 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-13, April 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[7] RFC 2716, October 1999: "PPP EAP TLS Authentication Protocol".

[8] SHAMAN/SHA/DOC/TNO/WP1/D02/v050, 22-June-01: "Intermediate Report: Results of Review, Requirements and Reference Architecture".

[9] ETSI TS 101 761-1 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".

[10] ETSI TS 101 761-2 v1.2.1C: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".

[11] ETSI TS 101 761-4 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".

[12] ETSI TR 101 683 v1.1.1: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[13] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[14] RFC 2486, January 1999: "The Network Access Identifier".

[15] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

[16] RFC 1421, February 1993: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".

[17] Federal Information Processing Standard (FIPS) draft standard: "Advanced Encryption Standard (AES)", November 2001.

[18] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[19] IEEE P802.1X/D11 June 2001: "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[22] CAR 020 SPEC/0.95cB: "SIM Access Profile, Interoperability Specification", version 0.95VD.

[23] draft-ietf-aaa-eap-08.txt, June 2004: "Diameter Extensible Authentication Protocol (EAP) Application". IETF Work in progress

[24] RFC 3588, September 2003: "Diameter base protocol".

[25] RFC 3576, July 2003: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[26] RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".

[27] draft-ietf-eap-keying-02.txt, June 2004: "EAP Key Management Framework". IETF Work in progress

[28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.

[29] draft-ietf-ipsec-ikev2-14.txt, May 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-06.txt, April 2004: "Cryptographic Suites for IPsec". IETF Work in progress

[32] draft-ietf-ipsec-udp-encaps-09.txt, May 2004: "UDP Encapsulation of IPsec Packets". IETF Work in progress

[33] draft-ietf-ipsec-ikev2-algorithms-05.txt, April 2004: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2". IETF Work in progress

[34] RFC 2104, February 1997: "HMAC: Keyed-Hashing for Message Authentication".

[35] RFC 2404, November 1998: "The Use of HMAC-SHA-1-96 within ESP and AH".

[36] RFC 2548, March 1999: " Microsoft Vendor-specific RADIUS Attributes".

[37] draft-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

[xx] 3GPP TS 27.007: "Technical Specification Group Terminals; AT command set for User Equipment (UE)".

[yy] ETSI TS 102.310: "Smart Cards; Extensible Authentication Protocol support in the UICC".

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~~ provides WLAN access, while the MT or UICC or SIM card ~~will~~ implements the authentication as the EAP termination, which includes key derivation and identity handling. The termination point of EAP shall always be the ~~MT~~UICC. When any authentication process is finished (in the UICC~~MT~~), the resulting keys ~~will~~ can be retreived by ~~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~~ MT~~(or SIM card)~~. Details are FFS.

6.1.3 EAP support in Smart Cards

Editors note: LS (S3-030187/ S1-030546) from SA1 has stated, "There are requests from operators for a secure SIM based WLAN authentication solution". SA3 has asked SA1 in an LS (S3-030306) if this request is confirmed. The input paper to SA3 on this can be found at: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_28_Berlin/Docs/ZIP/S3-030198.zip

6.1.3.1 EAP-AKA procedure

It shall be possible to have the termination of EAP in the UICC. For this purpose, all steps of the EAP-AKA authentication mechanism described in 6.1.1.1 apply with the exception of step 15 that shall be replaced with the following:

> The WLAN-UE runs EAP authentication method on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the USIM rejects the authentication (not shown in this example). If the sequence number is out of synch, USIM initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the USIM computes the Master Session Key and Extended Master Session Key and checks the received MAC with the new derived keying material.

6.1.3.2 EAP-SIM procedure

It shall be possible to have the termination of EAP in the UICC. To handle EAP-SIM the USIM uses GSM AKA by applying conversion functions c2 and c3 (as defined in 33.102 [21]). For this purpose, all steps of the EAP-SIM authentication mechanism described in 6.1.2.1 apply with the exception of step 14 that shall be replaced with the following:

> The WLAN-UE runs EAP authentication method (see TS 102.310 [yy]) on the USIM. The WLAN-UE continues the authentication exchange only if the MAC is correct.
>
> If a protected pseudonym was received, then the UICC stores the pseudonym for future authentications.

6.7 WLAN-UE split interworking

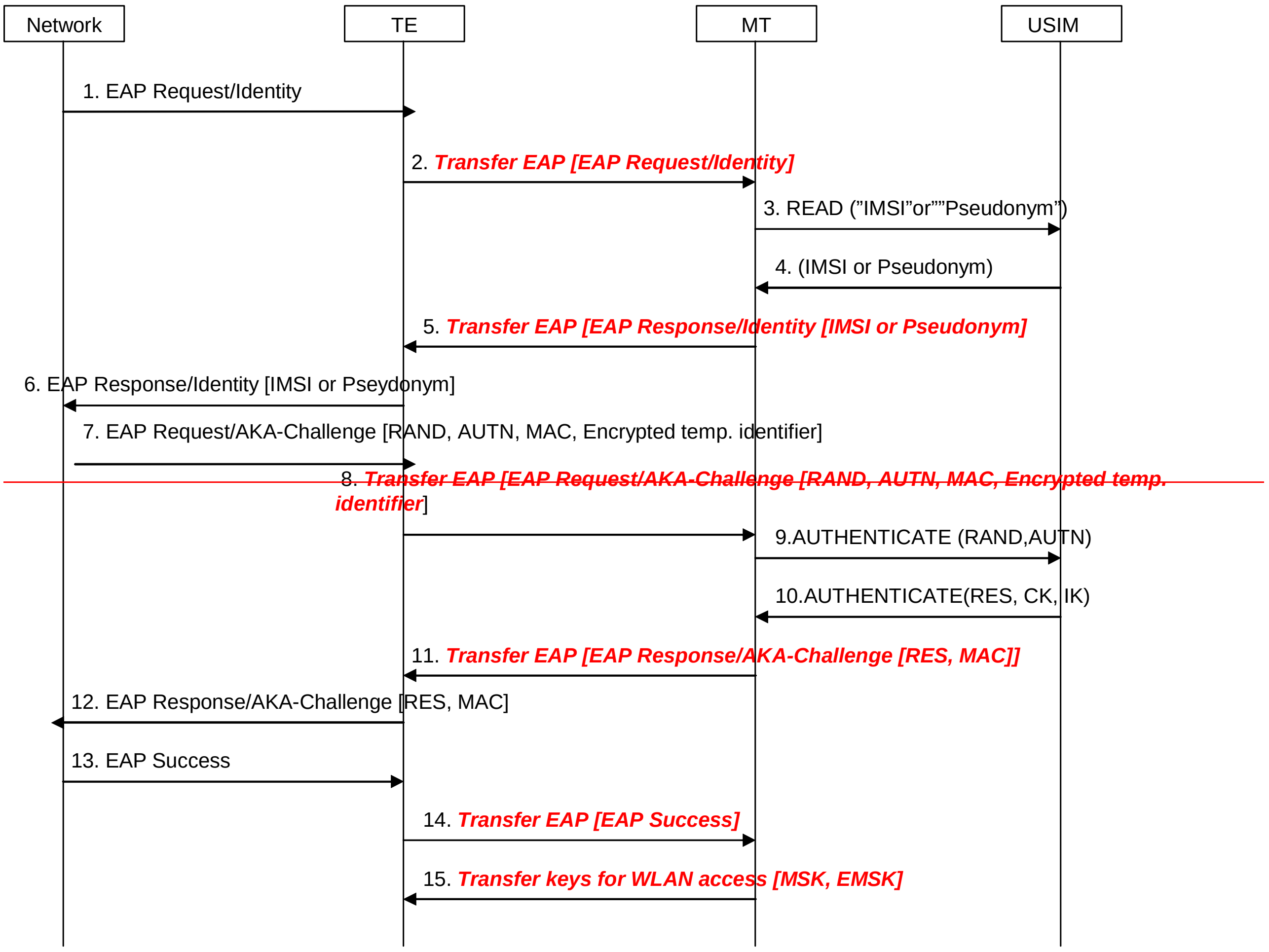
EAP-AKA/SIM procedures terminate in the UICC~~MT~~, so the TE shall contact the MT via protected local interface (e.g. Bluetooth) at any authentication or re-authentication process, using +CRLA and +CGLA AT commands as defined in TS 27.007 [xx]. The ~~Bluetooth~~ local interface (e.g. Bluetooth, IrDa, RS232, USB, …) acts as a transparent carrier of the EAP methods; the TE just forwards messages from the ~~MT~~ UICC 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 MT shall forbid the transfer of RUN GSM ALGO command, and the AUTHENTICATE command in GSM security context. 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 1: It shall be possible to have the termination of EAP in the MT.~~UICC (or SIM card).~~ Details are FFS.

NOTE 2: The SIM Acces Profile may be used to access the UICC EAP capabilities. In this case, the usage of AT commands may be substituted by the usage of the Transfer APDU command (see CAR 020 SPEC/0.95cB [22]) all over this section. However, specific SAP requirements defined in the present document shall be fulfilled.

6.7.1 Full authentication with EAP-AKA

The process is shown in figure 11.


Network
TE
MT
USIM
1. EAP Request/Identity
2. *Transfer EAP [EAP Request/Identity]*
3. READ ("IMSI"or""Pseudonym")
4. (IMSI or Pseudonym)
5. *Transfer EAP [EAP Response/Identity [IMSI or Pseudonym]*
6. EAP Response/Identity [IMSI or Pseydonym]
7. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
~~8. *Transfer EAP [EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier*]~~
9.AUTHENTICATE (RAND,AUTN)
10.AUTHENTICATE(RES, CK, IK)
11. *Transfer EAP [EAP Response/AKA-Challenge [RES, MAC]]*
12. EAP Response/AKA-Challenge [RES, MAC]
13. EAP Success
14. *Transfer EAP [EAP Success]*
15. *Transfer keys for WLAN access [MSK, EMSK]*

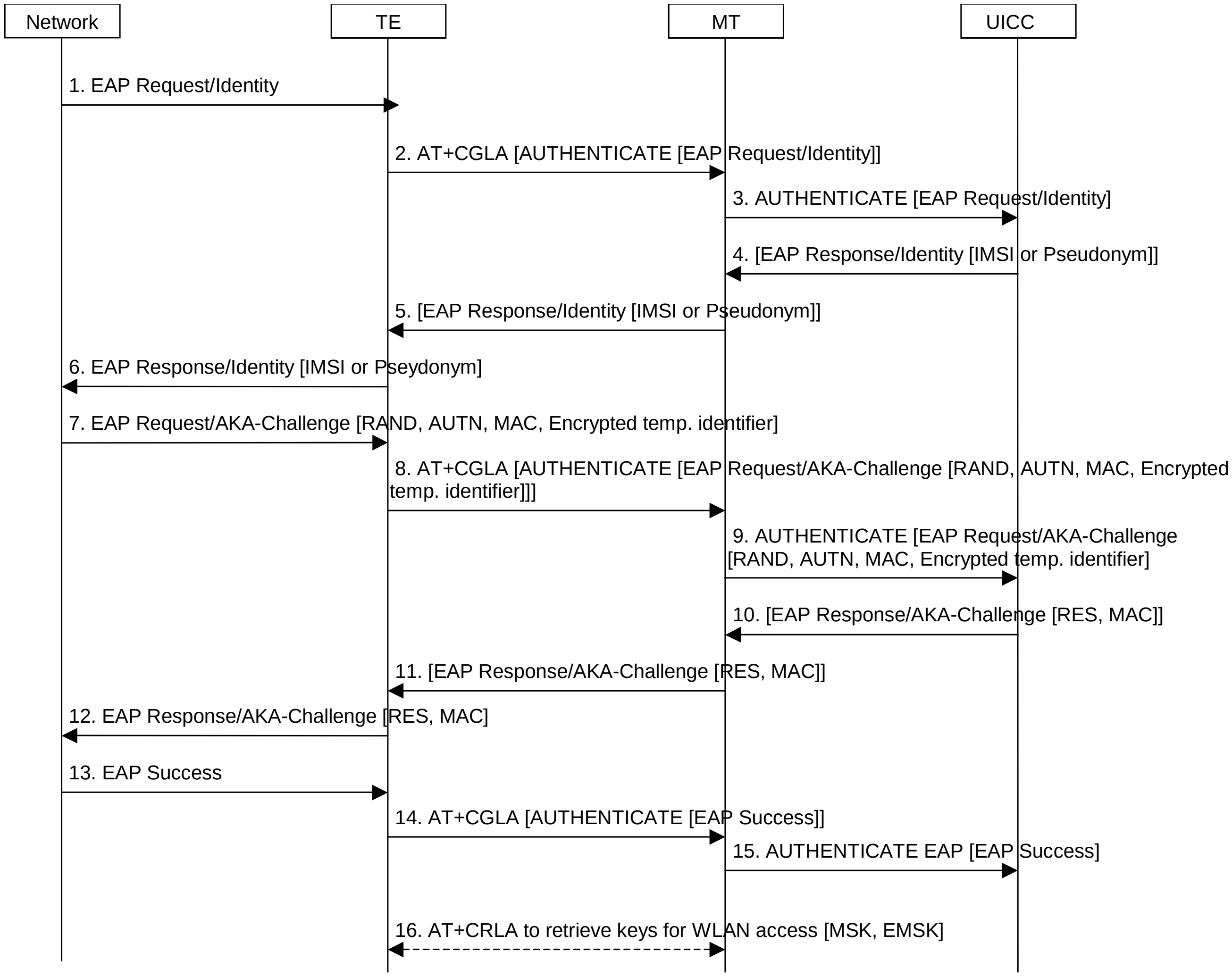

Network
TE
MT
UICC
1. EAP Request/Identity
2. AT+CGLA [AUTHENTICATE [EAP Request/Identity]]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [IMSI or Pseudonym]]
5. [EAP Response/Identity [IMSI or Pseudonym]]
6. EAP Response/Identity [IMSI or Pseydonym]
7. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
8. AT+CGLA [AUTHENTICATE [EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]]]
9. AUTHENTICATE [EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
10. [EAP Response/AKA-Challenge [RES, MAC]]
11. [EAP Response/AKA-Challenge [RES, MAC]]
12. EAP Response/AKA-Challenge [RES, MAC]
13. EAP Success
14. AT+CGLA [AUTHENTICATE [EAP Success]]
15. AUTHENTICATE EAP [EAP Success]
16. AT+CRLA to retrieve keys for WLAN access [MSK, EMSK]

Figure 11: Full authentication with EAP-AKA

1. The network sends an 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 TE builds an EAP Authenticate command using the EAP packet received in message 1 then sends this command to the USIM using +CGLA AT command. The EAP request identity message is forwarded via the MT to the USIM. ~~Bluetooth interface to the MT.~~ Prior to step 2, the TE shall open a communication session with the USIM, as indicated in TS 27.007 [xx], and then shall select the appropriate DF, as indicated in TS 102.310 [yy].

3. ~~If t~~The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).~~does not have the identity available, it requests the identity from the USIM.~~

4. The USIM returns the EAP Response/Identity packet to the MT, in the Authenticate command response data.~~identity to the MT.~~

5. The MT returns the EAP Response/Identity packet to the TE, in the +CGLA AT command response data.~~ inserts the identity in the EAP response identity message and sends it to the network via the TE.~~

6. The TE sends the EAP R~~r~~esponse/~~ i~~Identity packet~~message~~ to the network.

7. The network initiates the EAP AKA authentication process.

8. The TE builds an EAP Authenticate command using the EAP packet received in message 7 then sends this command to the USIM via the ME using +CGLA AT command.~~The TE forwards the EAP request to the MT with all the parameters.~~

9. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).~~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.~~ The USIM returns the EAP Response/AKA-Challenge packet to the MT, in the Authenticate command response data.

11. The MT returns the EAP Response/AKA-Challenge packet to the TE, in the +CGLA AT command response data.~~The EAP response message includes the RES and the calculated MAC.~~

12. The TE ~~forwards the response message~~ sends the EAP Response/AKA-Challenge packet to the network, which ~~will~~ checks 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~~ sends an EAP S~~s~~uccess ~~message~~packet to the TE.

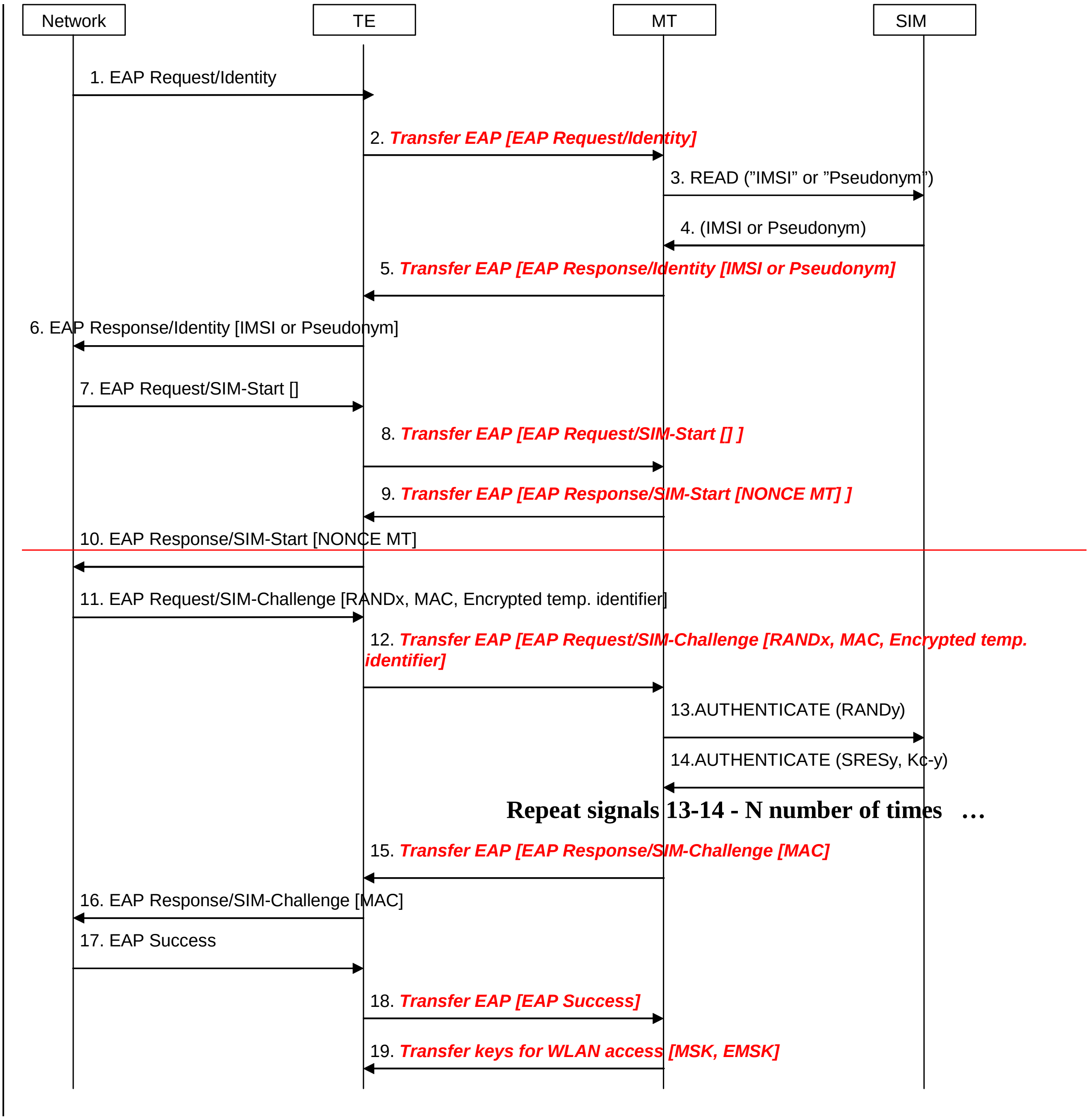
14. The TE builds an EAP Authenticate command using the EAP packet received in message 13 then sends this command to the USIM using +CGLA AT command.~~TE forwards the EAP success to the MT as a success indication.~~

15. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).~~-~~

16. After a successful EAP authentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from EF$_{EAPKEYS}$ (for this purpose, the TE uses the +CRLA AT command). ~~After receiving the success indication, 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~~ MSK and EMSK for security purposes, for example for WLAN link layer security

6.7.2 Full authentication with EAP-~~-~~SIM

The process is shown in figure 12, and it’s very similar to EAP AKA (from MT-TE interface point of view).


Network
TE
MT
SIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. READ (”IMSI” or ”Pseudonym”)
4. (IMSI or Pseudonym)
5. Transfer EAP [EAP Response/Identity [IMSI or Pseudonym]
6. EAP Response/Identity [IMSI or Pseudonym]
7. EAP Request/SIM-Start []
8. Transfer EAP [EAP Request/SIM-Start []]
9. Transfer EAP [EAP Response/SIM-Start [NONCE MT]]
10. EAP Response/SIM-Start [NONCE MT]
11. EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
12. Transfer EAP [EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
13.AUTHENTICATE (RANDy)
14.AUTHENTICATE (SRESy, Kc-y)
Repeat signals 13-14 - N number of times …
15. Transfer EAP [EAP Response/SIM-Challenge [MAC]
16. EAP Response/SIM-Challenge [MAC]
17. EAP Success
18. Transfer EAP [EAP Success]
19. Transfer keys for WLAN access [MSK, EMSK]

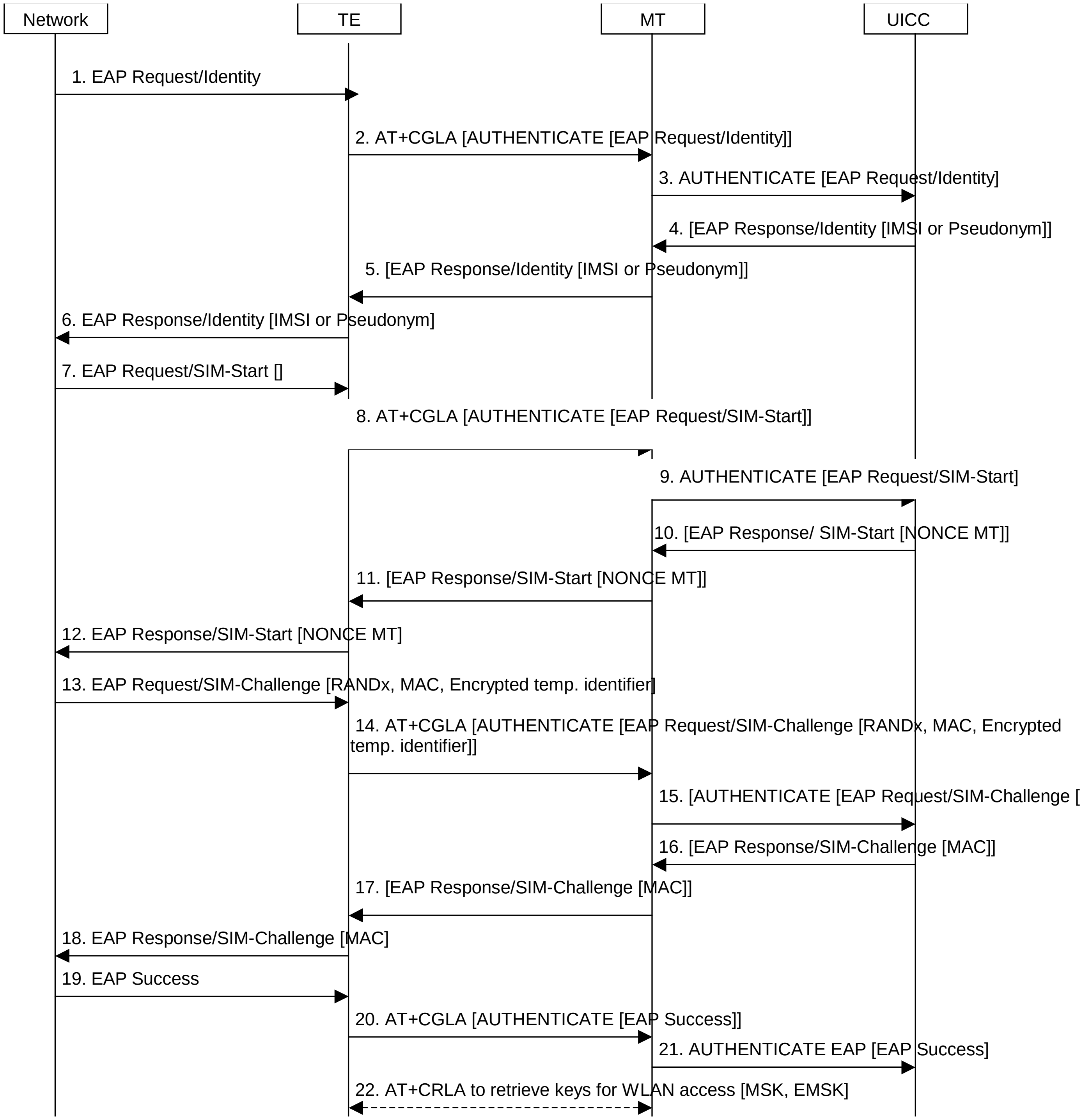

Network
TE
MT
UICC
1. EAP Request/Identity
2. AT+CGLA [AUTHENTICATE [EAP Request/Identity]]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [IMSI or Pseudonym]]
5. [EAP Response/Identity [IMSI or Pseudonym]]
6. EAP Response/Identity [IMSI or Pseudonym]
7. EAP Request/SIM-Start []
8. AT+CGLA [AUTHENTICATE [EAP Request/SIM-Start]]
9. AUTHENTICATE [EAP Request/SIM-Start]
10. [EAP Response/ SIM-Start [NONCE MT]]
11. [EAP Response/SIM-Start [NONCE MT]]
12. EAP Response/SIM-Start [NONCE MT]
13. EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
14. AT+CGLA [AUTHENTICATE [EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]]
15. [AUTHENTICATE [EAP Request/SIM-Challenge [
16. [EAP Response/SIM-Challenge [MAC]]
17. [EAP Response/SIM-Challenge [MAC]]
18. EAP Response/SIM-Challenge [MAC]
19. EAP Success
20. AT+CGLA [AUTHENTICATE [EAP Success]]
21. AUTHENTICATE EAP [EAP Success]
22. AT+CRLA to retrieve keys for WLAN access [MSK, EMSK]

Figure 12: Full authentication with EAP-~~-~~SIM

1. The network sends an 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 TE builds an EAP Authenticate command using the EAP packet received in message 1 then sends this command to the USIM using +CGLA AT command. The EAP request identity message is forwarded via the MT to the USIM. Prior to step 2, the TE shall open a communication session with the USIM, as indicated in TS 27.007 [xx], and shall select the appropriate DF, as indicated in TS 102.310 [yy].~~The EAP request identity message is forwarded via the Bluetooth interface to the MT.~~

3. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx])~~If the MT does not have the identity available, it requests the identity from the USIM.~~

4. The USIM returns the EAP Response/Identity packet to the MT, in the Authenticate command response data.~~The USIM returns the identity to the MT.~~

5. The MT returns the EAP Response/Identity packet to the TE, in the +CGLA AT command response data.~~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 R~~r~~esponse~~-~~/~~i~~Identity ~~message~~ packet to the network.

7. The network initiates the EAP SIM authentication process.

8. The TE builds an EAP Authenticate command using the EAP packet received in message 7 then sends this command to the USIM via the ME using +CGLA AT command.~~The TE forwards the EAP SIMstart request to the MT.~~

9. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).

10. The USIM returns the EAP Response/SIM-Start packet to the MT, in the Authenticate command response data.

11. The MT returns the EAP Response/SIM-Start packet to the TE, in the +CGLA AT command response data.

12. The TE sends the EAP Response/SIM-Start packet to the network, which uses the NONCE to calculate the MAC.~~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.~~

13~~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.

14~~12~~. The TE builds an EAP Authenticate command using the EAP packet received in message 13 then sends this command to the USIM via the ME using +CGLA AT command.~~The TE forwards the message to the MT.~~

15. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).

16. The USIM returns the EAP Response/SIM-Challenge packet to the MT, in the Authenticate command response data.

17. The MT returns the EAP Response/SIM-Challenge packet to the TE, in the +CGLA AT command response data.

18. The TE sends the EAP Response/SIM-Challenge packet to the network, which computes the MAC and compares it with the received MAC.

19. If checks are correct, the network sends an EAP Success packet to the TE.

20. The TE builds an EAP Authenticate command using the EAP packet received in message 19 then sends this command to the USIM using +CGLA AT command.

21. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).

22. After a successful EAP authentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from $EF_{EAPKEYS}$ (for this purpose, the TE uses the +CRLA AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

~~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.~~

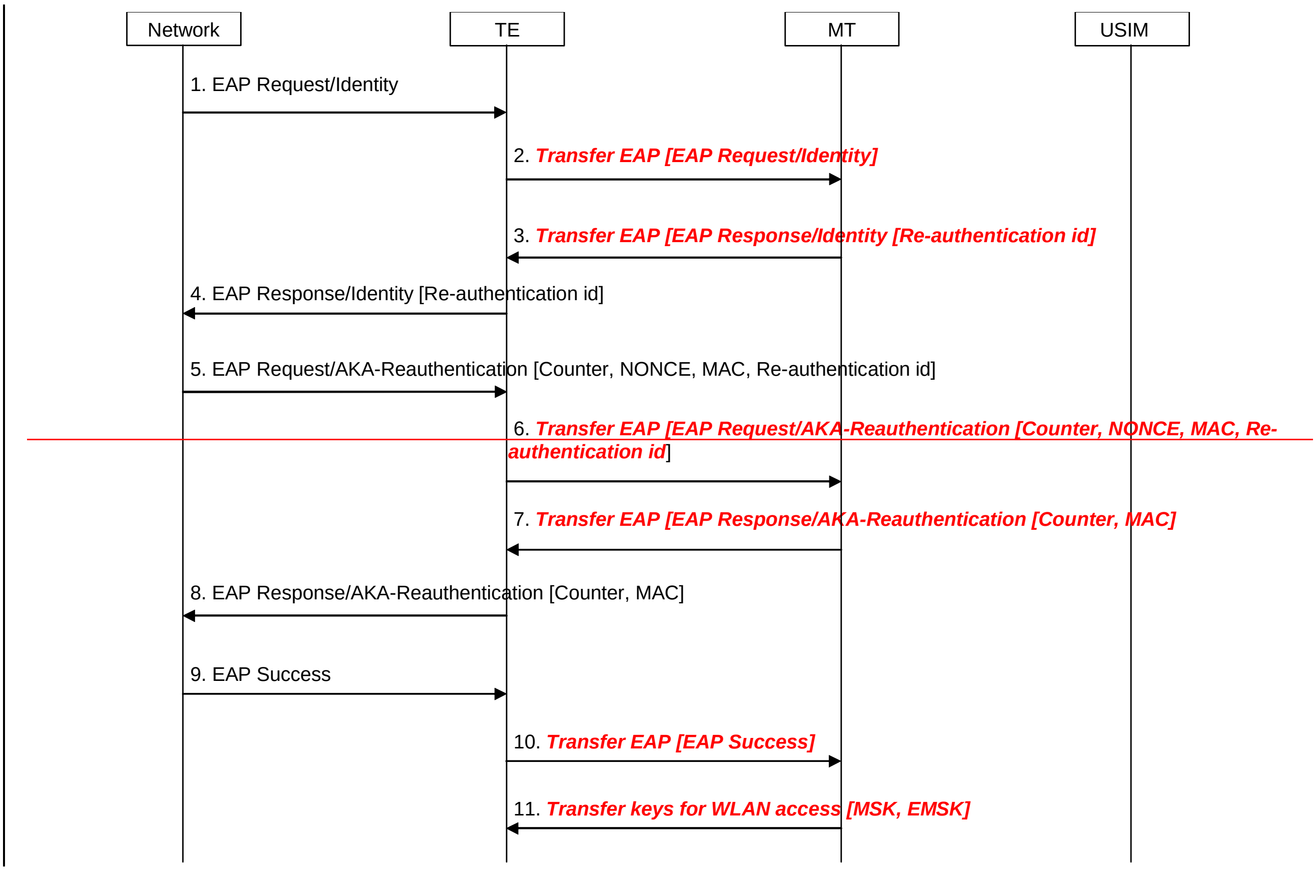
~~17. The network calculates its own copy of the MAC and if it matches the received one, it sends an EAP success message.~~

~~18. TE forwards the EAP success to the MT as a success indication~~

~~19. After receiving the success indication, 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~~ USIM to the TE when the fast re-authentication process is finished. The process is shown in figure 13.


Network
TE
MT
USIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. Transfer EAP [EAP Response/Identity [Re-authentication id]
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. Transfer EAP [EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
7. Transfer EAP [EAP Response/AKA-Reauthentication [Counter, MAC]
8. EAP Response/AKA-Reauthentication [Counter, MAC]
9. EAP Success
10. Transfer EAP [EAP Success]
11. Transfer keys for WLAN access [MSK, EMSK]

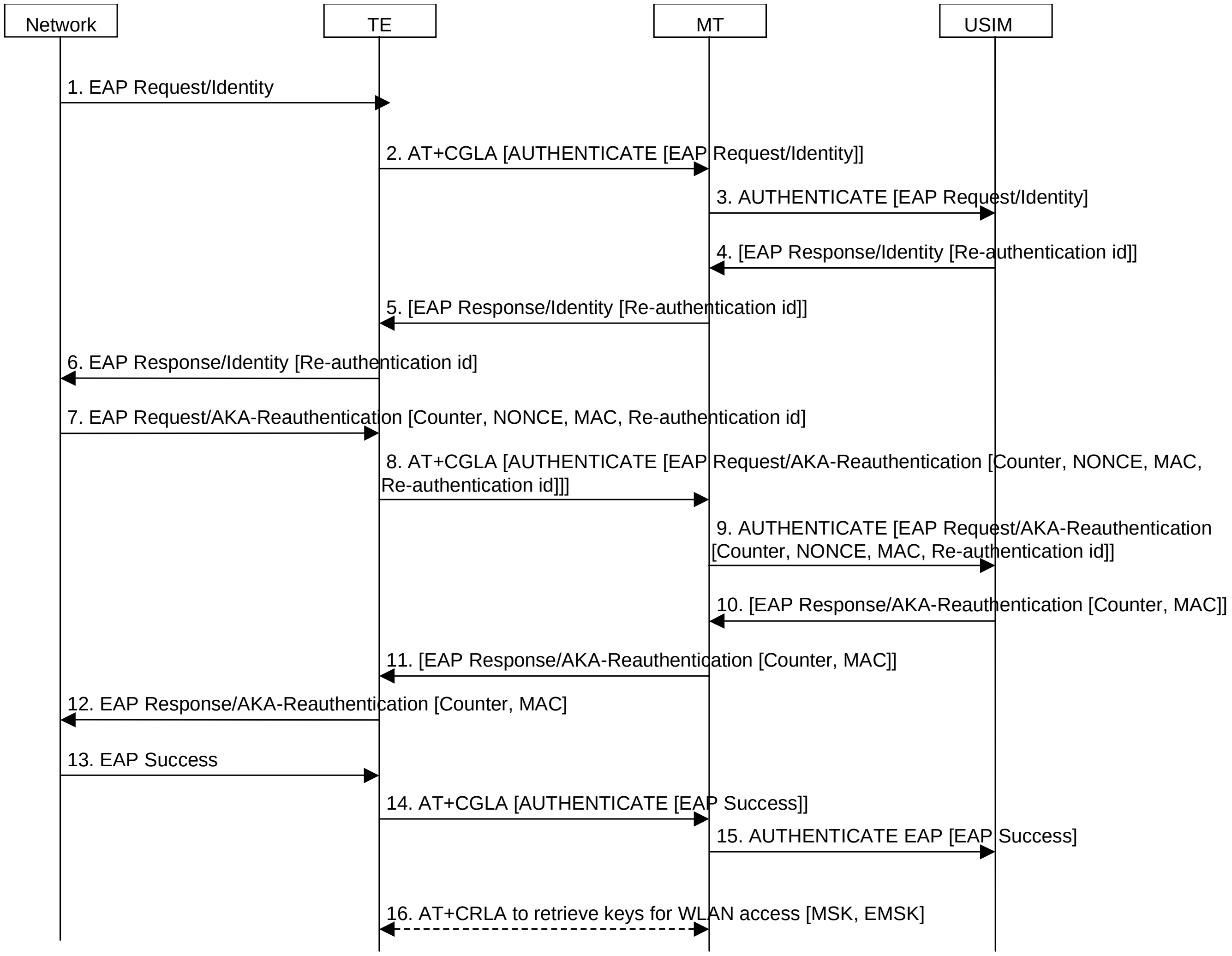

Network
TE
MT
USIM
1. EAP Request/Identity
2. AT+CGLA [AUTHENTICATE [EAP Request/Identity]]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [Re-authentication id]]
5. [EAP Response/Identity [Re-authentication id]]
6. EAP Response/Identity [Re-authentication id]
7. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
8. AT+CGLA [AUTHENTICATE [EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]]
9. AUTHENTICATE [EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]
10. [EAP Response/AKA-Reauthentication [Counter, MAC]]
11. [EAP Response/AKA-Reauthentication [Counter, MAC]]
12. EAP Response/AKA-Reauthentication [Counter, MAC]
13. EAP Success
14. AT+CGLA [AUTHENTICATE [EAP Success]]
15. AUTHENTICATE EAP [EAP Success]
16. AT+CRLA to retrieve keys for WLAN access [MSK, EMSK]

Figure 13: Fast re-authentication with EAP AKA

1. The network sends an EAP request identity message.

2. The TE builds an EAP Authenticate command using the EAP packet received in message 1 then sends this command to the USIM using +CGLA AT command.~~The TE forwards the message to the MT via the Bluetooth interface.~~

3. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).~~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. If the USIM received a fast re-authentication identity in the last authentication process (either full or fast), it shall reply with this fast re-authentication identity in the EAP response identity message. Consequently, the USIM returns the EAP Response/Identity packet to the MT, in the Authenticate command response data.

5. The MT returns the EAP Response/Identity packet to the TE, in the +CGLA AT command response data.

6. The TE sends the EAP Response/Identity packet to the network.

7. The network initiates the EAP AKA reauthentication process.

8. The TE builds an EAP Reauthenticate command using the EAP packet received in message 7 then sends this command to the USIM via the ME using +CGLA AT command.

9. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).

10. The USIM returns the EAP Response/AKA-Reauthentication packet to the MT, in the Authenticate command response data.

11. The MT returns the EAP Response/AKA-Reauthentication packet to the TE, in the +CGLA AT command response data.

12. The TE sends the EAP Response/AKA-Reauthentication packet to the network, which computes the MAC of the entire received message, and comapres it with the received MAC.

13. If checks are correct, the network sends an EAP Success packet to the TE.

14. The TE builds an EAP Authenticate command using the EAP packet received in message 13 then sends this command to the USIM using +CGLA AT command.

15. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).

16. After a successful EAP reauthentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from $EF_{EAPKEYS}$ (for this purpose, the TE uses the +CRLA AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

~~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.~~

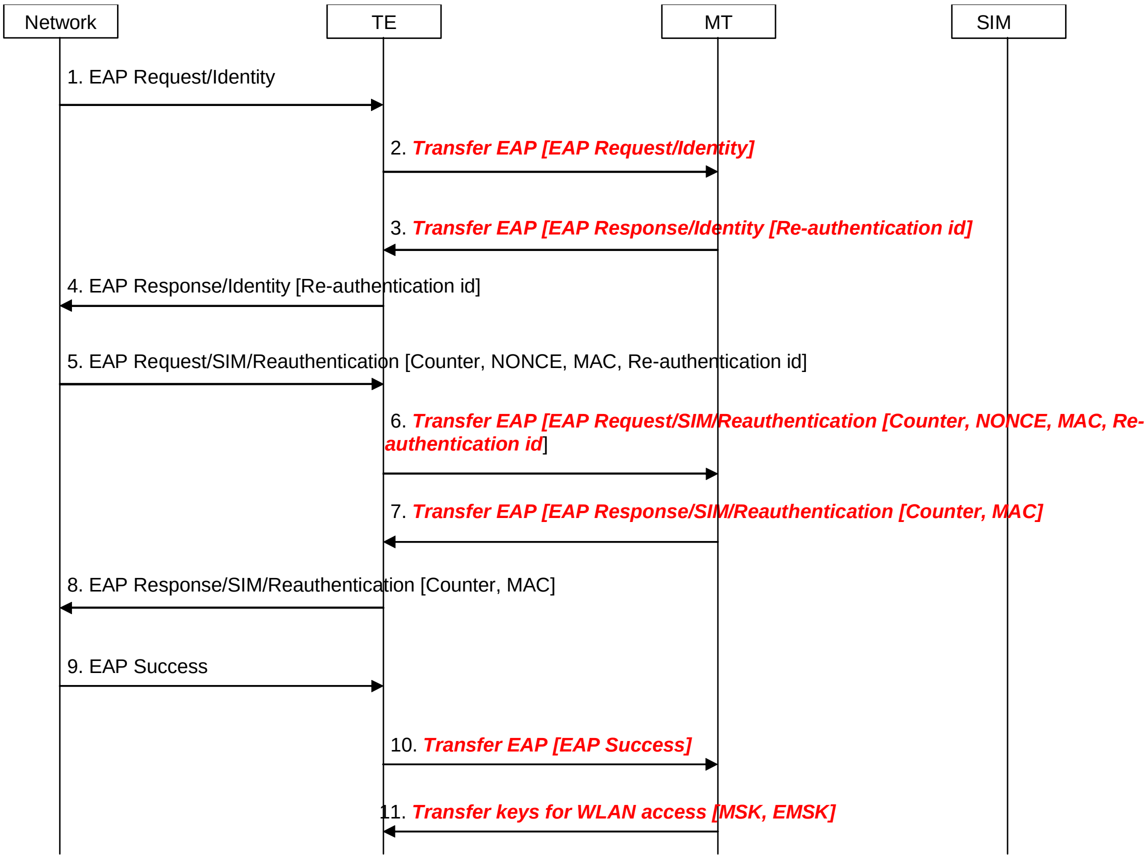
~~9. The network calculates its own copy of the MAC over the received message and checks it with the received one. If it is correct, it sends a EAP success message.~~

~~10. TE forwards the EAP success to the MT as a success indication.~~

~~11. After receiving the success indication, 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~~ USIM to the TE when the fast re-authentication process is finished. The process is shown in figure 14.


Network
TE
MT
SIM
1. EAP Request/Identity
2. *Transfer EAP [EAP Request/Identity]*
3. *Transfer EAP [EAP Response/Identity [Re-authentication id]*
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/SIM/Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. *Transfer EAP [EAP Request/SIM/Reauthentication [Counter, NONCE, MAC, Re-authentication id*]
7. *Transfer EAP [EAP Response/SIM/Reauthentication [Counter, MAC]*
8. EAP Response/SIM/Reauthentication [Counter, MAC]
9. EAP Success
10. *Transfer EAP [EAP Success]*
11. *Transfer keys for WLAN access [MSK, EMSK]*

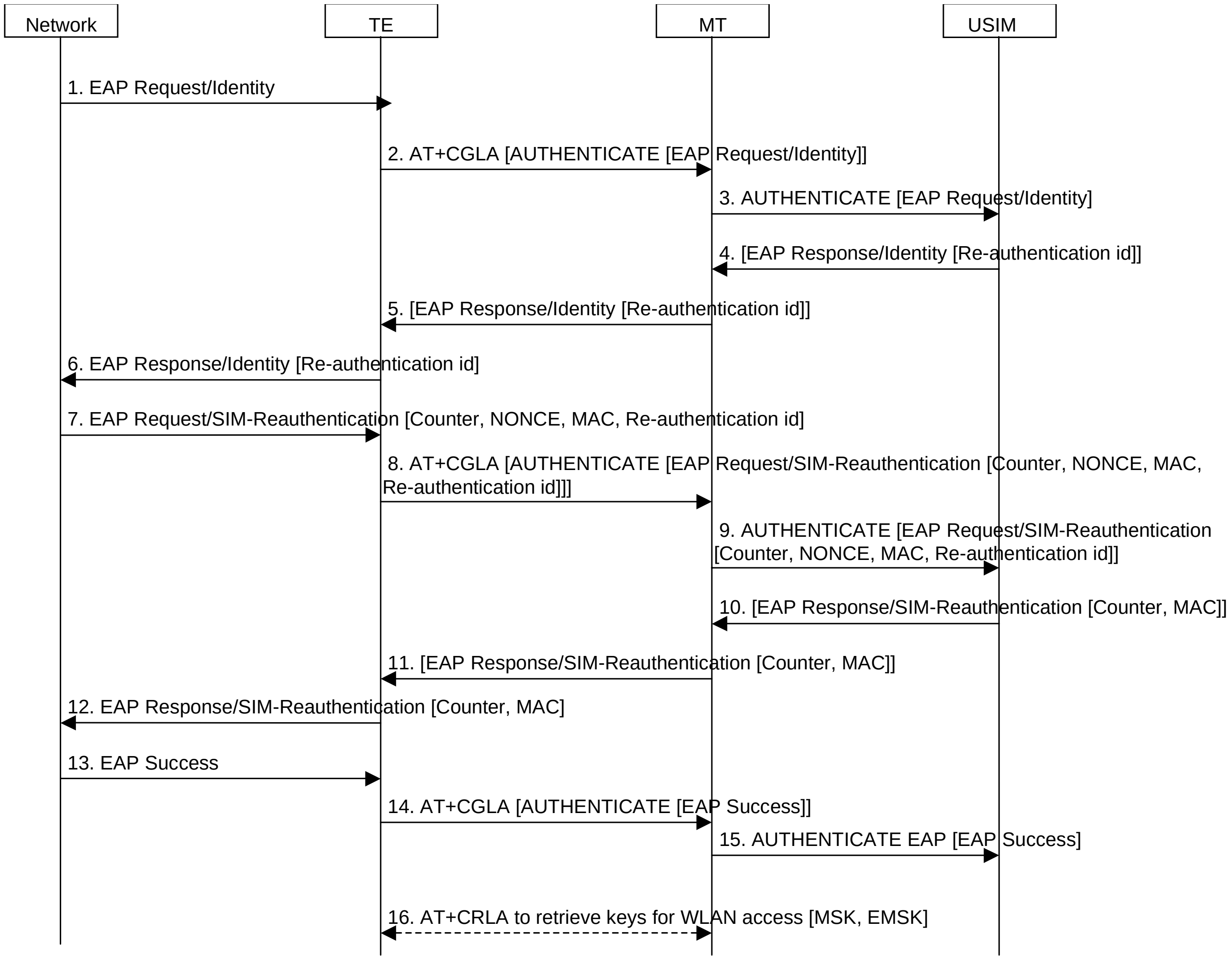

Network
TE
MT
USIM
1. EAP Request/Identity
2. AT+CGLA [AUTHENTICATE [EAP Request/Identity]]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [Re-authentication id]]
5. [EAP Response/Identity [Re-authentication id]]
6. EAP Response/Identity [Re-authentication id]
7. EAP Request/SIM-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
8. AT+CGLA [AUTHENTICATE [EAP Request/SIM-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]]
9. AUTHENTICATE [EAP Request/SIM-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]
10. [EAP Response/SIM-Reauthentication [Counter, MAC]]
11. [EAP Response/SIM-Reauthentication [Counter, MAC]]
12. EAP Response/SIM-Reauthentication [Counter, MAC]
13. EAP Success
14. AT+CGLA [AUTHENTICATE [EAP Success]]
15. AUTHENTICATE EAP [EAP Success]
16. AT+CRLA to retrieve keys for WLAN access [MSK, EMSK]

Figure 14: Fast re-authentication with EAP SIM

1. The network sends an EAP request identity message.

2. The TE builds an EAP Authenticate command using the EAP packet received in message 1 then sends this command to the USIM using +CGLA AT command.

3. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).

4. If the USIM received a fast re-authentication identity in the last authentication process (either full or fast), it shall reply with this fast re-authentication identity in the EAP response identity message. Consequently, the USIM returns the EAP Response/Identity packet to the MT, in the Authenticate command response data.

5. The MT returns the EAP Response/Identity packet to the TE, in the +CGLA AT command response data.

6. The TE sends the EAP Response/Identity packet to the network.

7. The network initiates the EAP SIM reauthentication process.

8. The TE builds an EAP Authenticate command using the EAP packet received in message 7 then sends this command to the USIM via the ME using +CGLA AT command.

9. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [xx]).

10. The USIM returns the EAP Response/SIM-Reauthentication packet to the MT, in the Authenticate command response data.

11. The MT returns the EAP Response/SIM-Reauthentication packet to the TE, in the +CGLA AT command response data.

12. The TE sends the EAP Response/SIM-Reauthentication packet to the network, which computes the MAC of the entire received message, and compares it with the received MAC.

13. If checks are correct, the network sends an EAP Success packet to the TE.

14. The TE builds an EAP Authenticate command using the EAP packet received in message 13 then sends this command to the USIM using +CGLA AT command.

15. The MT performs the received +CGLA AT command i.e. the MT sends the Authenticate command as it is to the USIM (see TS 27.007 [xx]).

16. After a successful EAP reauthentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from EF$_{EAPKEYS}$ (for this purpose, the TE uses the +CRLA AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

~~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. TE forwards the EAP success to the MT as a success indication~~

~~11. After receiving the success indication, the MT sends the new calculated MSK and EMSK and sends them to the TE.~~