3GPP TSG SA WG3 Meeting SA3#36
Shenzhen, China, 23 – 26 November, 2004

Tdoc ⌘ S3-041103

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **027** ⌘ **rev** **4** ⌘ 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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction of WLAN UE function split
Source:	⌘	Axalto, Gemplus, Siemens
Work item code:	⌘	WLAN
Date:	⌘	25/11/2004
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:

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:	⌘	At SA3#32 alternative 2 was chosen as the working assumption for WLAN UE functional split (see S3-040197). However, the required standardized API for local interface between the TE and the ME did not exist yet. But at T2#27, the CRs T2-040439 and T2-040468 to TS 27.007 were agreed, which introduced the new AT commands +CUAD, +CEAP and +CERP. The present CR implements solutions for WLAN UE functional split, using these commands.
Summary of change:	⌘	Modify the WLAN UE functional split to include the termination of EAP in the UICC or in the MT by the new AT commands +CUAD, +CEAP and +CERP.
Consequences if not approved:	⌘	Functional split cannot be implemented in release 6 in a standardized manner.

Clauses affected:	⌘	2, 5.6, 6.1.3, (new) 6.1.3.1, (new) 6.1.3.2, 6.7, 6.7.1, 6.7.2, 6.7.3, 6.7.4

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

Other comments:	⌘	The final approval of this CR is conditional on the approval of T2-040439 and T2-040468 by the T-plenary (8 - 10 Dec 2004).

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".

[38] 3GPP TS 27.007: "Technical Specification Group Terminals; AT command set for User Equipment (UE)".

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

[40] ETSI TS 102.221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

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

6.1.3 EAP support in UICC~~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 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 as an implementation option 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 (see TS 102.310 [39~~yy~~]) on the UICC. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the UICC rejects the authentication (not shown in this example). If the sequence number is out of synch, UICC initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the UICC computes the Master Session Key and Extended Master Session Key and checks the received MAC with the new derived keying material.

If a protected pseudonym was received, then the WLAN-UE stores the pseudonym for future authentications.

6.1.3.2 EAP-SIM procedure

It shall be possible as an implementation option to have the termination of EAP in the UICC. To handle EAP-SIM the UICC 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 [398~~yy~~]) on the UICC. 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 or MT, so the TE shall contact the MT via protected local interface (e.g. Bluetooth, IrDa, RS232, USB, …) at any authentication or re-authentication process, using the AT commands +CUAD, +CEAP and +CERP, as defined in TS 27.007 [387xx]. 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 or 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/UMTS security context, from any TE involved in WLAN-UE split interworking. 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.

Editor's NOTEnote 1: It shall be possible to have the termination of EAP in the UICC (or SIM card). Details are FFS.AT command set for the termination of EAP in the MT does not currently exist. SA3 has requested T2 (S3-040840) to investigate the suitability to define a new AT command set for this purpose or to utilize existing commands used for the UICC termination (i.e. +CGLA AT, +CRLA AT). In this latter case, a specific behaviour in the MT may be defined in order to handle EAP packets whenever the UICC is not capable of doing so (i.e. SIM or USIM not EAP capable).

Editor's note 2: it is highly desirable to have a unified procedure for both, cases 1 and 2. It should not be required that the TE is aware of the particular function split in the MT. Therefore the TE should use the same commands in both cases.

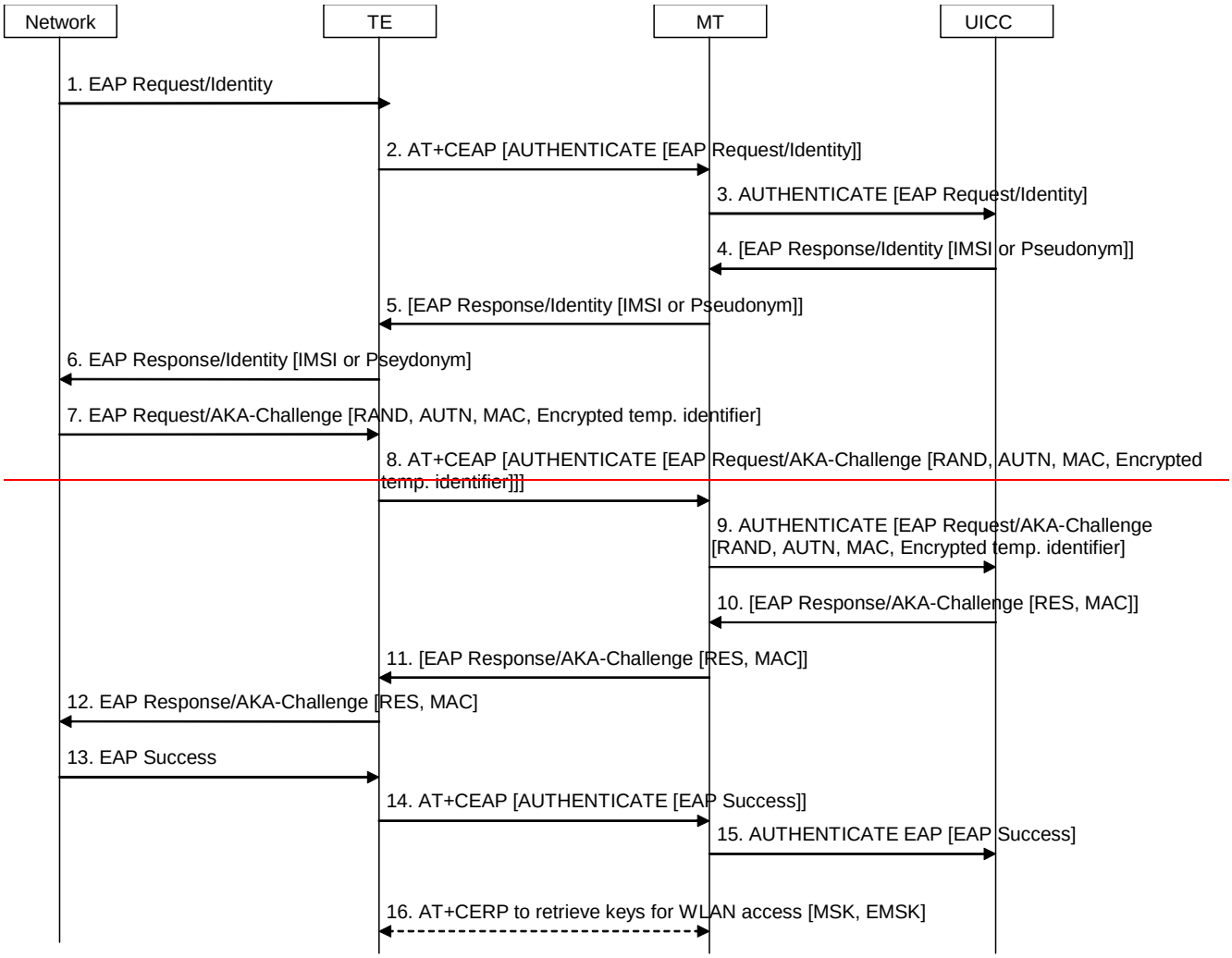
: The SIM Acces Profile may be used to access the UICC EAP capabilities. In this case, the usage of AT commands may be substituted by the usage of the Transfer APDU command (see CAR-020-SPEC/0.95cB [22]) all over this section. However, specific SAP requirements defined in the present document shall be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

6.7.1 Full authentication with EAP AKA

The procedures specified in subsections 6.7.1.1 and 6.7.1.2 have in common that, prior to the exchange of EAP messages, the appropriate USIM application on the UICC needs to be selected. For this purpose, the TE may runs the AT command +CUAD to discover what applications are available for selection on the UICC, so that the user can be prompted, if necessary, to perform the selection, as specified in [40].

6.7.1.1 Termination in the UICC

The process is shown in figure 11.



~~Figure 11: Full authentication with EAP-AKA~~

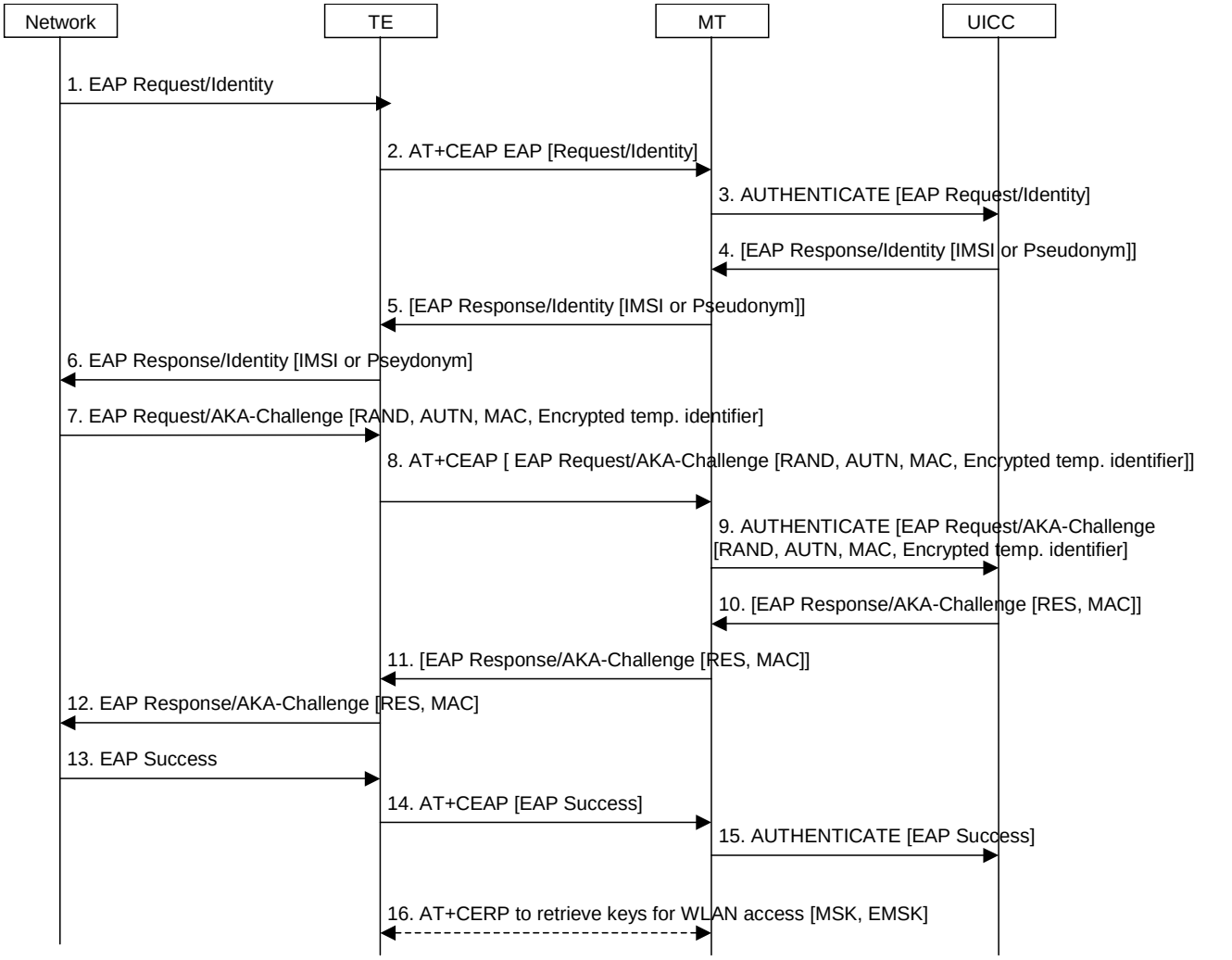


Figure 11: Full authentication with EAP-AKA

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~~sends the EAP packet received in message 1 ~~then sends this command~~ to the UICC application ~~USIM~~ using +CEAP~~GLA~~ AT command. The EAP request identity message is forwarded via the MT to the UICC application~~USIM~~. Prior to step 2, the TE shall open a communication session with the UICC application~~USIM~~, as indicated in TS 27.007 [38~~7xx~~], and then shall select the appropriate DF, as indicated in TS 102.310 [39~~8yy~~].

3. The MT performs the received +CEAP~~GLA~~ AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [38~~7xx~~]).

4. The UICC application ~~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 +CEAP~~GLA~~ AT command response data.

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

7. The network initiates the EAP AKA authentication process.

8. The TE ~~builds an EAP Authenticate command using~~sends the EAP packet received in message 7 ~~then sends this command~~ to the UICC application ~~USIM~~ via the MT~~ME~~ using +CEAP~~GLA~~ AT command.

9. The MT performs the received +CEAPGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [387xx]).

10. The UICC application 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 +CEAPGLA AT command response data.

12. The TE sends the EAP Response/AKA-Challenge packet to the network, which checks the validity of the RES and compute the MAC of the entire message received, comparing it with the received MAC.

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

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

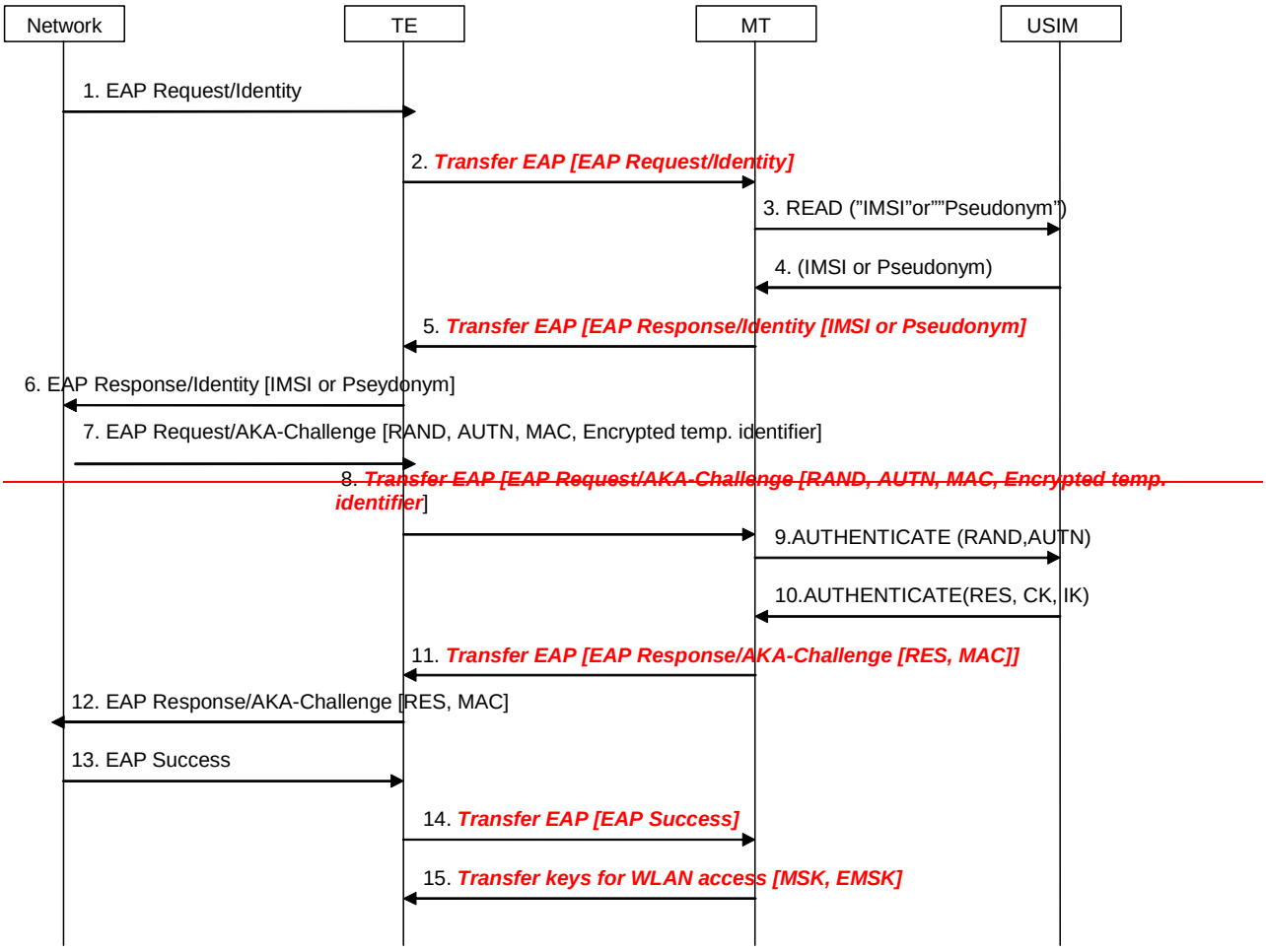
15. The MT performs the received +CEAPGLA AT command i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (see TS 27.007 [387xx]).

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 +CERPRLA AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

6.7.1.2 Termination in the MT

The process is shown in figure 121.

Editor's Note: AT command set for EAP termination in the MT is not yet defined.



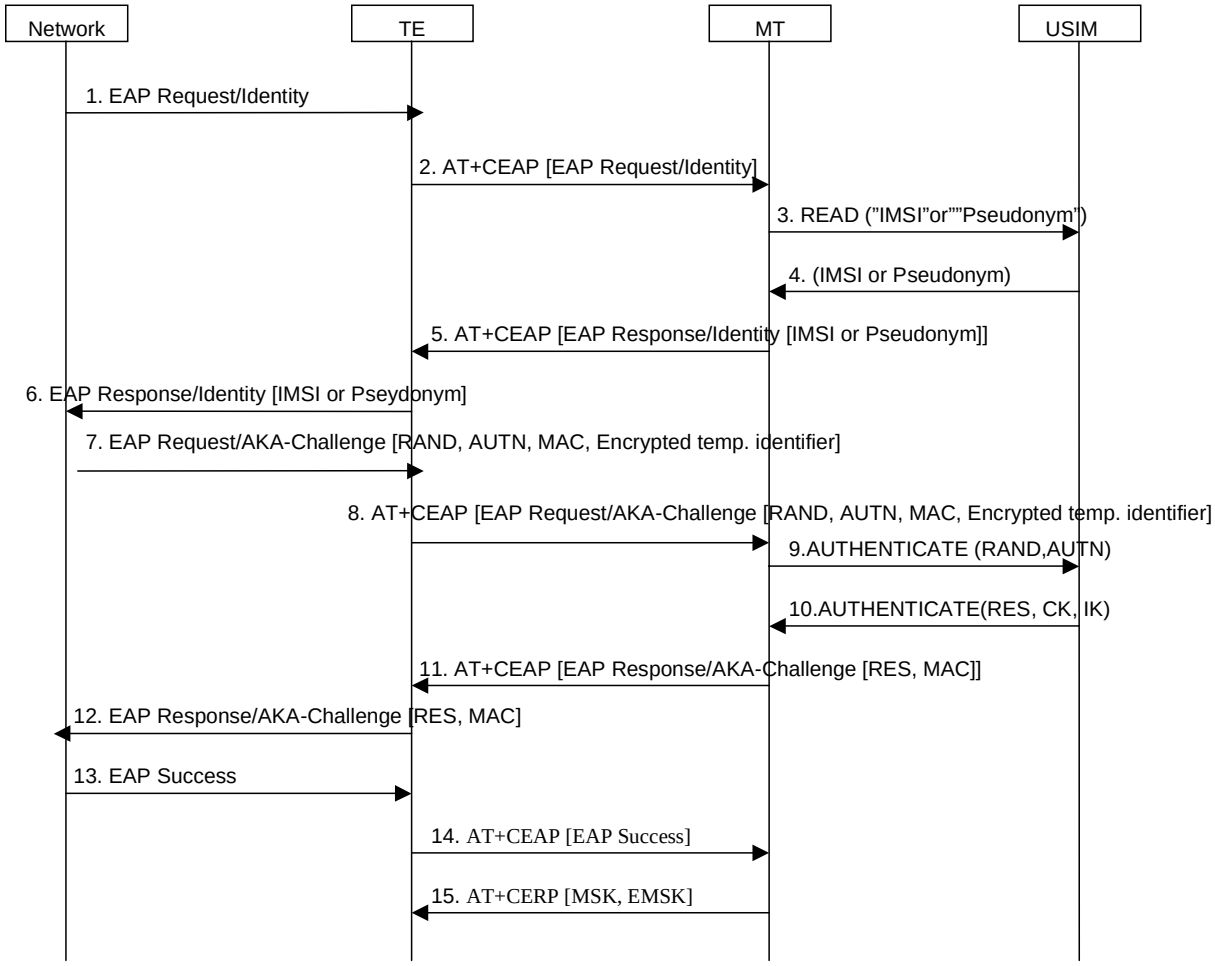


Figure 121: Full authentication with EAP AKA

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.~~The TE sends the EAP packet received in message 1 to the MT using +CEAP AT command.
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, using the +CEAP AT command.~~-~~
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, using the +CEAP AT command..
9. The MT ~~requests~~ sends the authentication ~~vectors from~~challenge to the USIM, using the AUTHENTICATE command.
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, sent by the MT to the TE using the +CEAP AT command, 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.

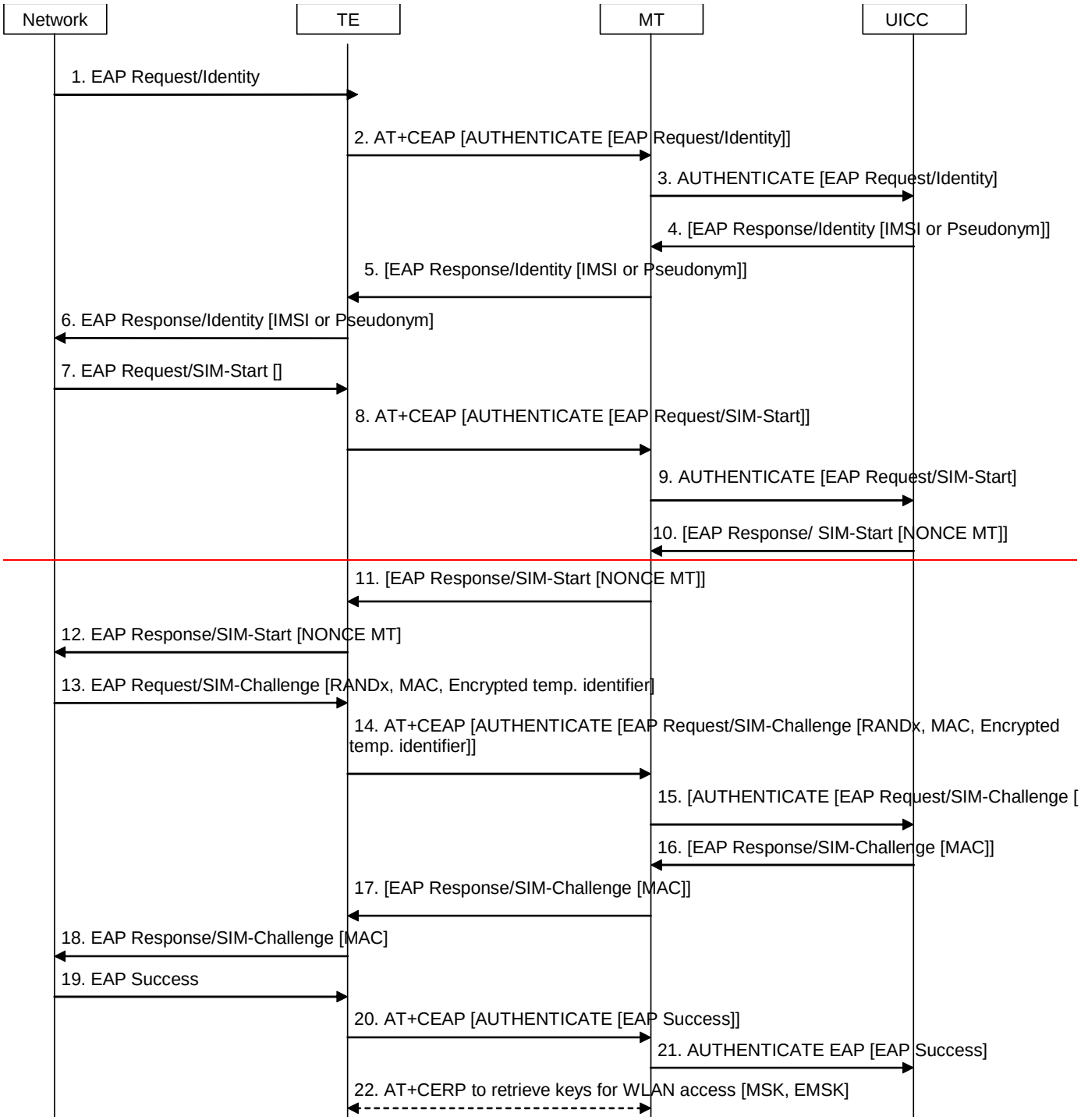
14. The TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.

15. 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). The TE requests these keys ~~and send them to the TE~~, using the +CERP AT command. ~~The TE uses them for security purposes, for example for WLAN link layer security~~

6.7.2 Full authentication with EAP SIM

6.7.2.1 Termination in the UICC

The process is shown in figure 13, and it's very similar to EAP AKA (from MT-TE interface point of view).



~~Figure 13: Full authentication with EAP-SIM~~

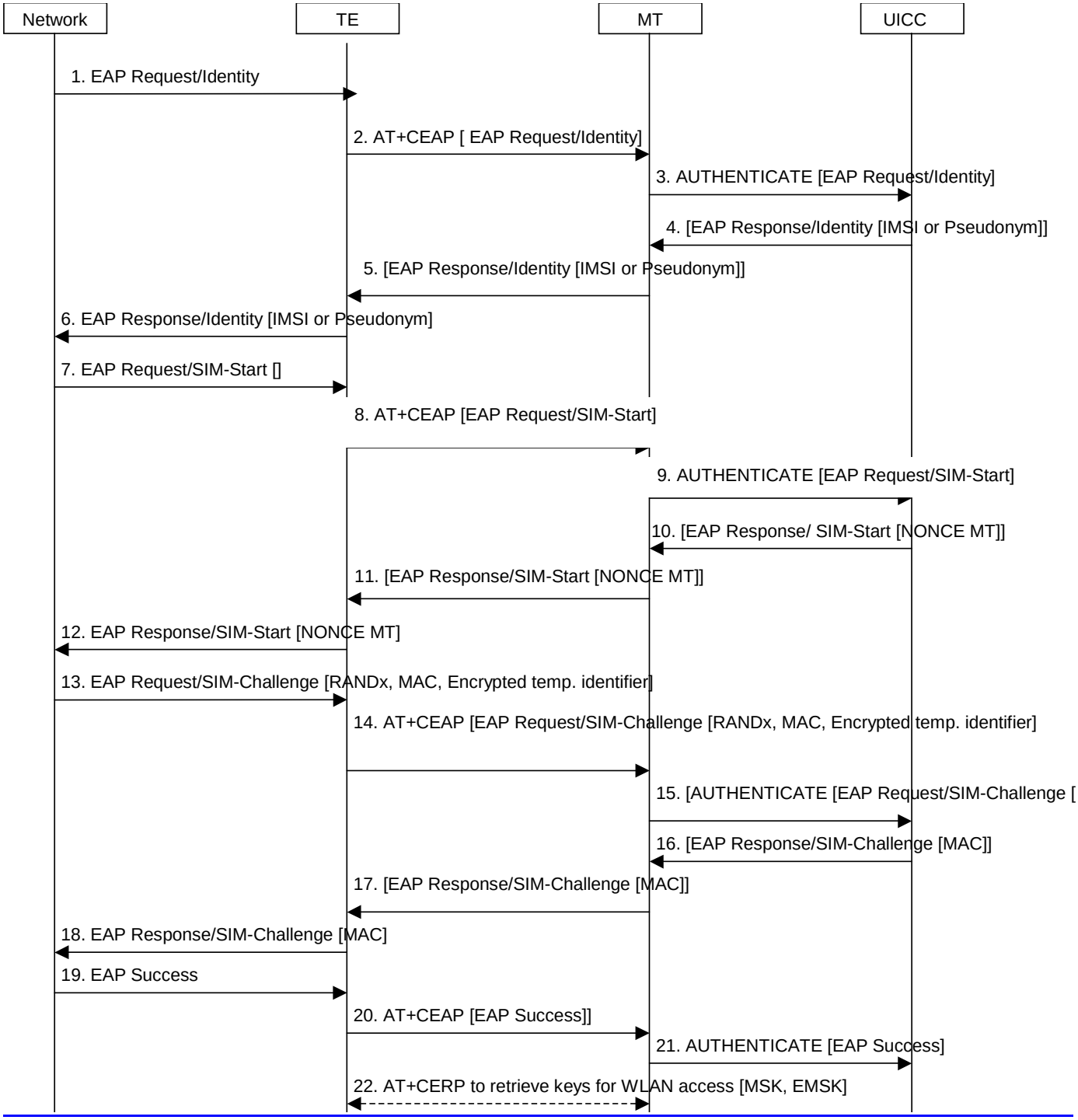


Figure 13: Full authentication with EAP-SIM

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~~sends the EAP packet received in message 1 ~~then sends this command~~ to the UICC application ~~USIM~~ using +CEAP~~GLA~~ AT command. The EAP request identity message is forwarded via the MT to the UICC application~~USIM~~. Prior to step 2, the TE shall open a communication session with the UICC application~~USIM~~, as indicated in TS 27.007 [38~~7xx~~], and shall select the appropriate DF, as indicated in TS 102.310 [39~~8yy~~].

3. The MT performs the received +CEAP~~GLA~~ AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [38~~7xx~~])

4. The UICC application ~~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 +CEAP~~GLA~~ AT command response data.

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

7. The network initiates the EAP SIM authentication process.

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

9. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [~~xx~~38]).

10. The UICC application ~~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~~CEAP 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.

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

15. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [38~~xx~~]).

16. The UICC application ~~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~~CEAP 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~~sends the EAP packet received in message 19 ~~then sends this command~~ to the UICC application ~~USIM~~ using +~~CGLA~~CEAP AT command.

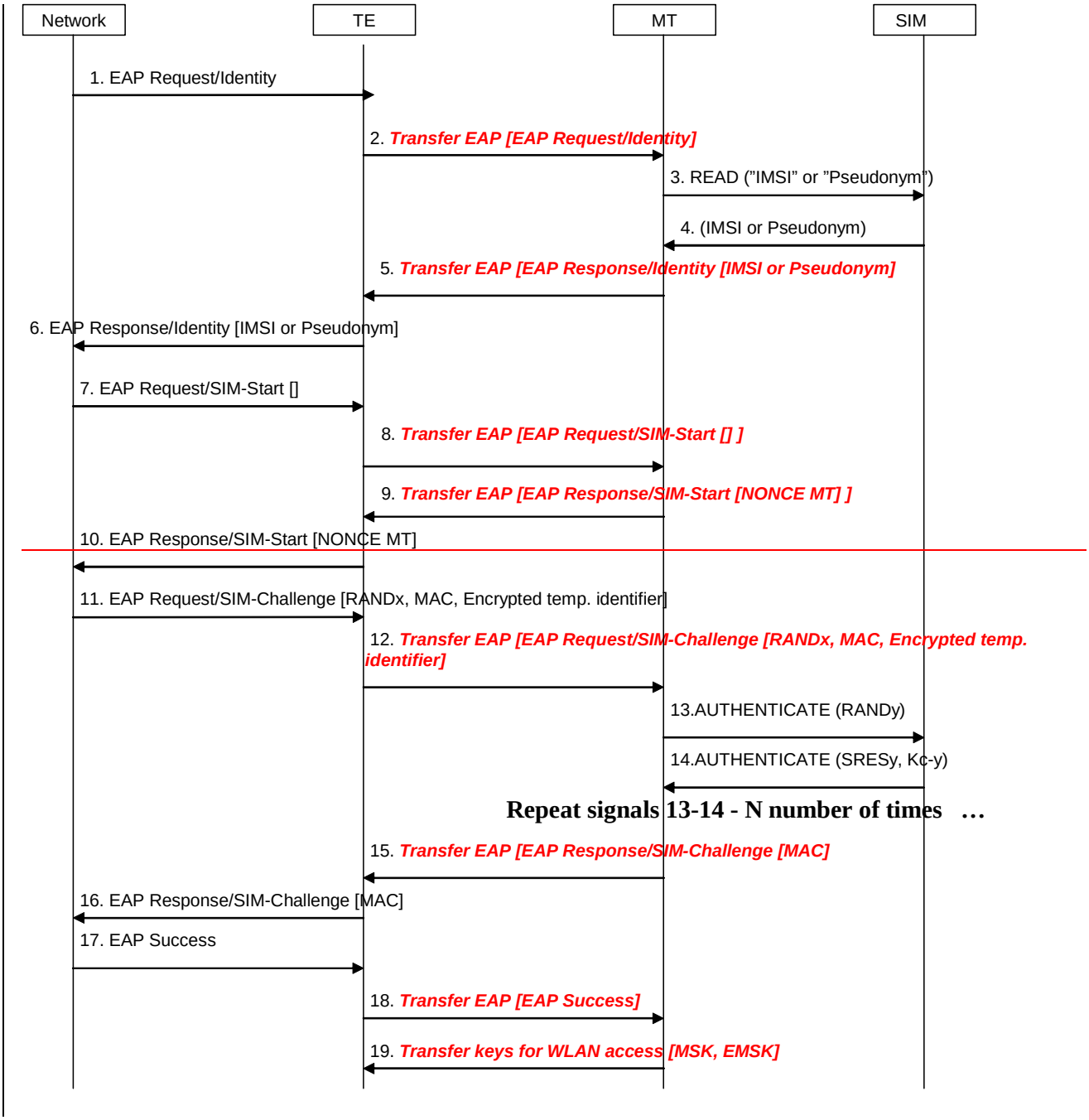
21. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [~~xx~~38]).

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~~CERP AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

6.7.2.2 Termination in the MT

~~The process is shown in figure 142, and it's very similar to EAP-AKA (from MT-TE interface point of view).~~

~~Editor's Note: AT command set for EAP termination in the MT is not yet defined.~~


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]

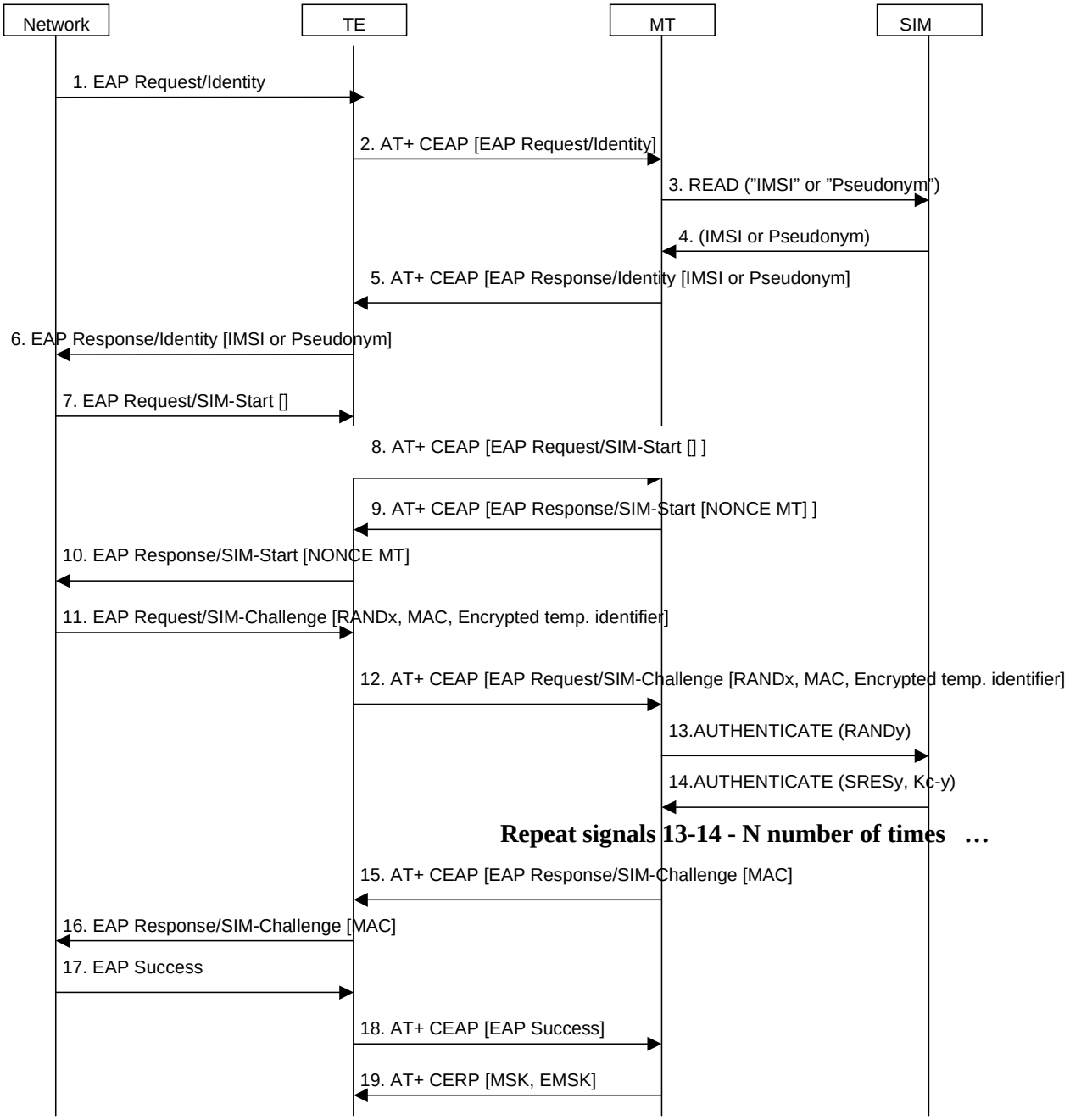


Figure 142: Full authentication with EAP SIM

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 TE sends the EAP packet received in message 1 to the MT using +CEAP AT command. ~~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, using the +CEAP AT command.
6. The TE sends the EAP response identity message to the network.
7. The network initiates the EAP SIM authentication process.

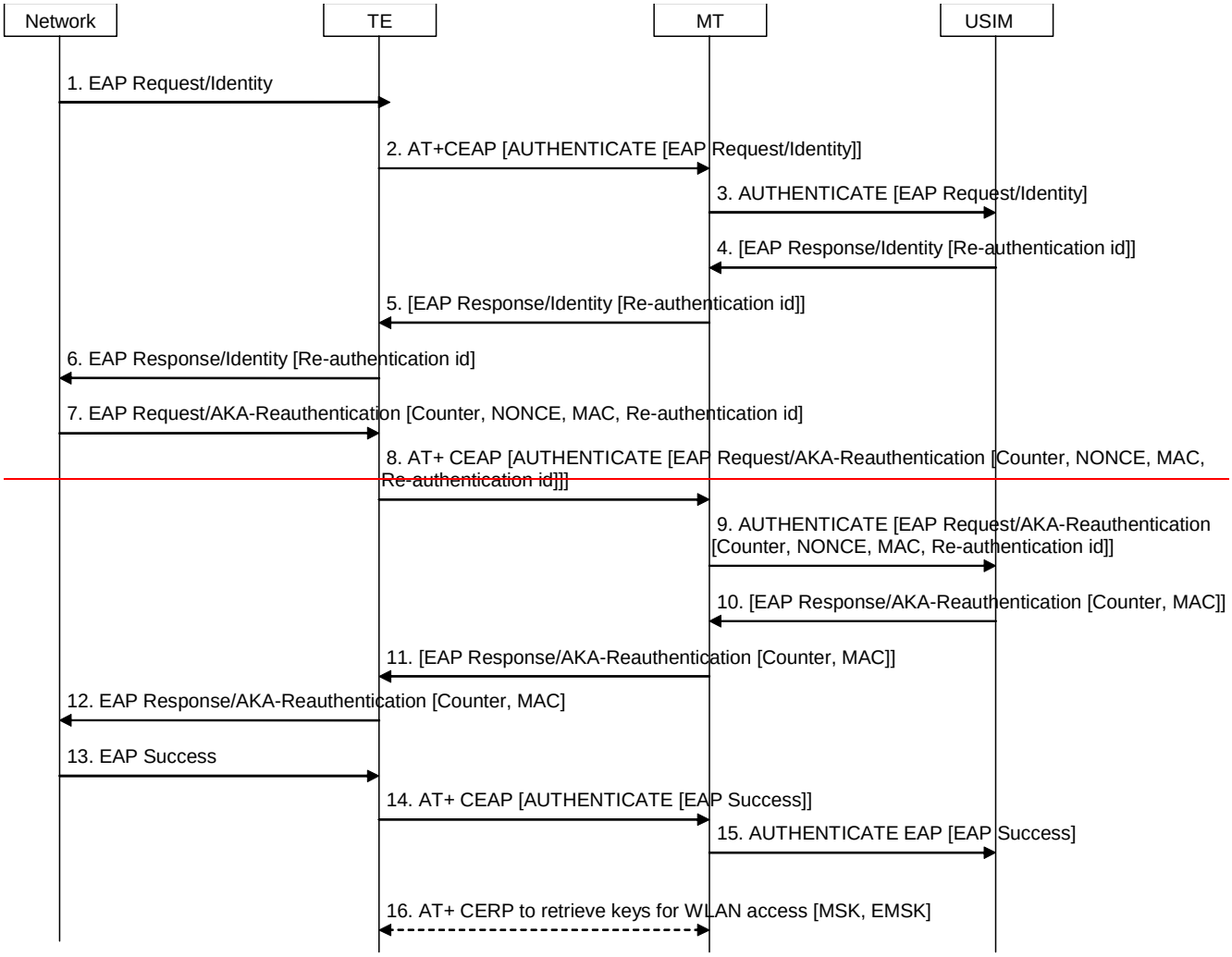
8. The TE forwards the EAP SIMstart request to the MT, using the +CEAP AT command.
9. The MT generates a NONCE and sends it to the TE, using the +CEAP AT command.
10. The TE forwards the NONCE to the network, which uses the NONCE to calculate the MAC.
11. The network sends an EAP SIM challenge request 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, using the +CEAP AT command.
13. The MT extracts the RAND and sends it to the SIM for key calculation, using the AUTHENTICATE command.
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) to the TE, using the +CEAP AT command.
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 TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.
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, using the +CERP AT command, which will use them for other security purposes, for example WLAN link layer security.

6.7.3 Fast re-authentication with EAP AKA

The procedures specified in this section 6.7.3 use the same UICC~~SIM~~ application as the preceding full authentication. So, there is no need to run the AT command +CUAD prior to the procedures specified in this section 6.7.3.

6.7.3.1 Termination in the UICC

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 UICC application ~~USIM~~ to the TE when the fast re-authentication process is finished. The process is shown in figure 15.


Network
TE
MT
USIM
1. EAP Request/Identity
2. AT+CEAP [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+ CEAP [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+ CEAP [AUTHENTICATE [EAP Success]]
15. AUTHENTICATE EAP [EAP Success]
16. AT+ CERP to retrieve keys for WLAN access [MSK, EMSK]

~~Figure 15: Fast re-authentication with EAP AKA~~

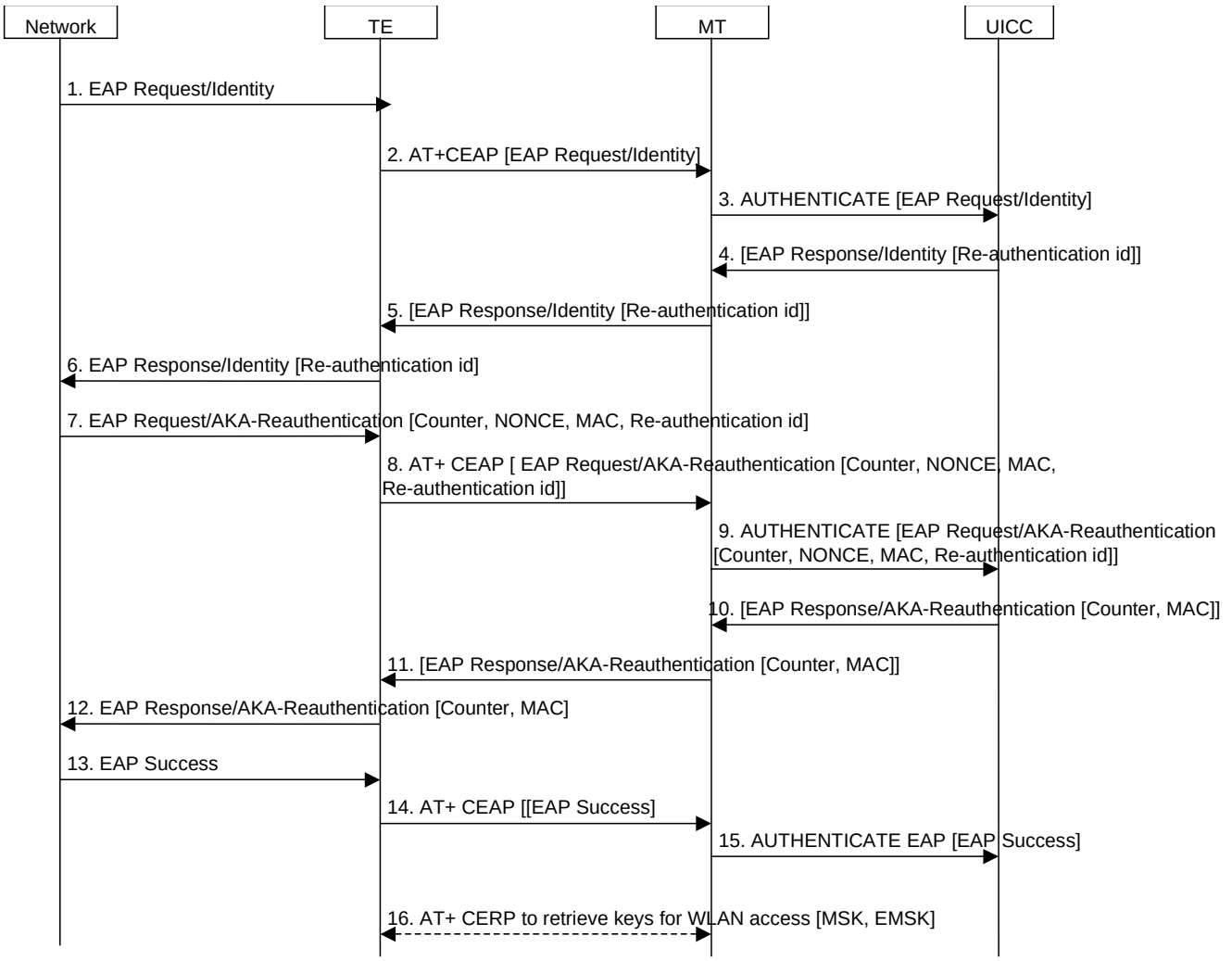


Figure 15: Fast re-authentication with EAP AKA

1. The network sends an EAP request identity message.
2. The TE ~~builds an EAP Authenticate command using~~sends the EAP packet received in message 1 ~~then sends this command~~ to the UICC application ~~USIM~~ using +~~CGLA~~CEAP AT command.
3. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM (~~see TS 27.007 [~~xx~~38]).
4. If the UICC application ~~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 UICC application ~~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~~CEAP 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~~sends the EAP packet received in message 7 ~~then sends this command~~ to the UICC application ~~USIM~~ via the ~~ME~~MT using +~~CGLA~~CEAP AT command.

9. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [~~xx~~38]).

10. The UICC application ~~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~~CEAP 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~~sends the EAP packet received in message 13 ~~then sends this command~~ to the UICC application ~~USIM~~ using +~~CGLA~~CEAP AT command.

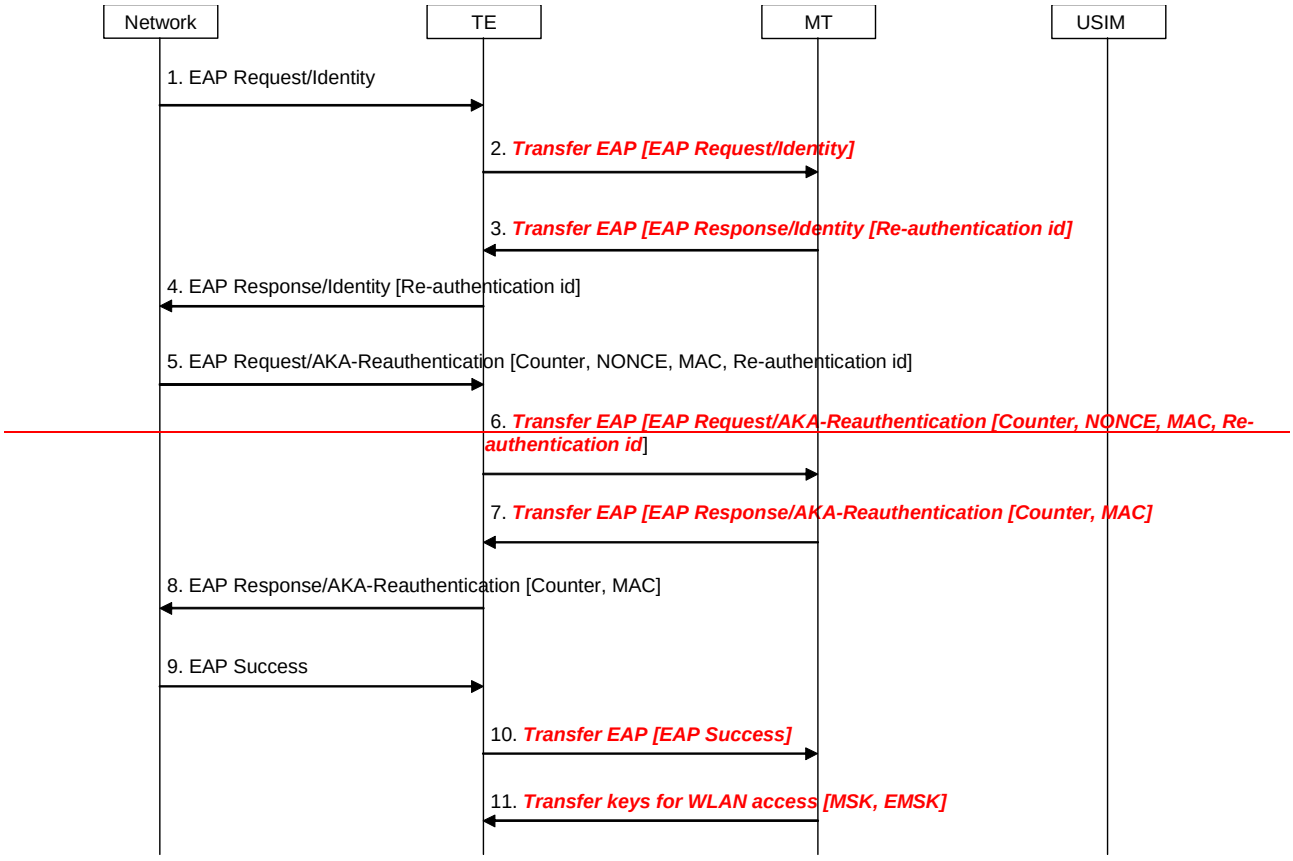
15. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [~~xx~~38]).

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~~CERP AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

6.7.3.2 Termination in the MT

~~Editor's Note: AT command set for EAP termination in the MT is not yet defined.~~

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 figure 16~~3~~.



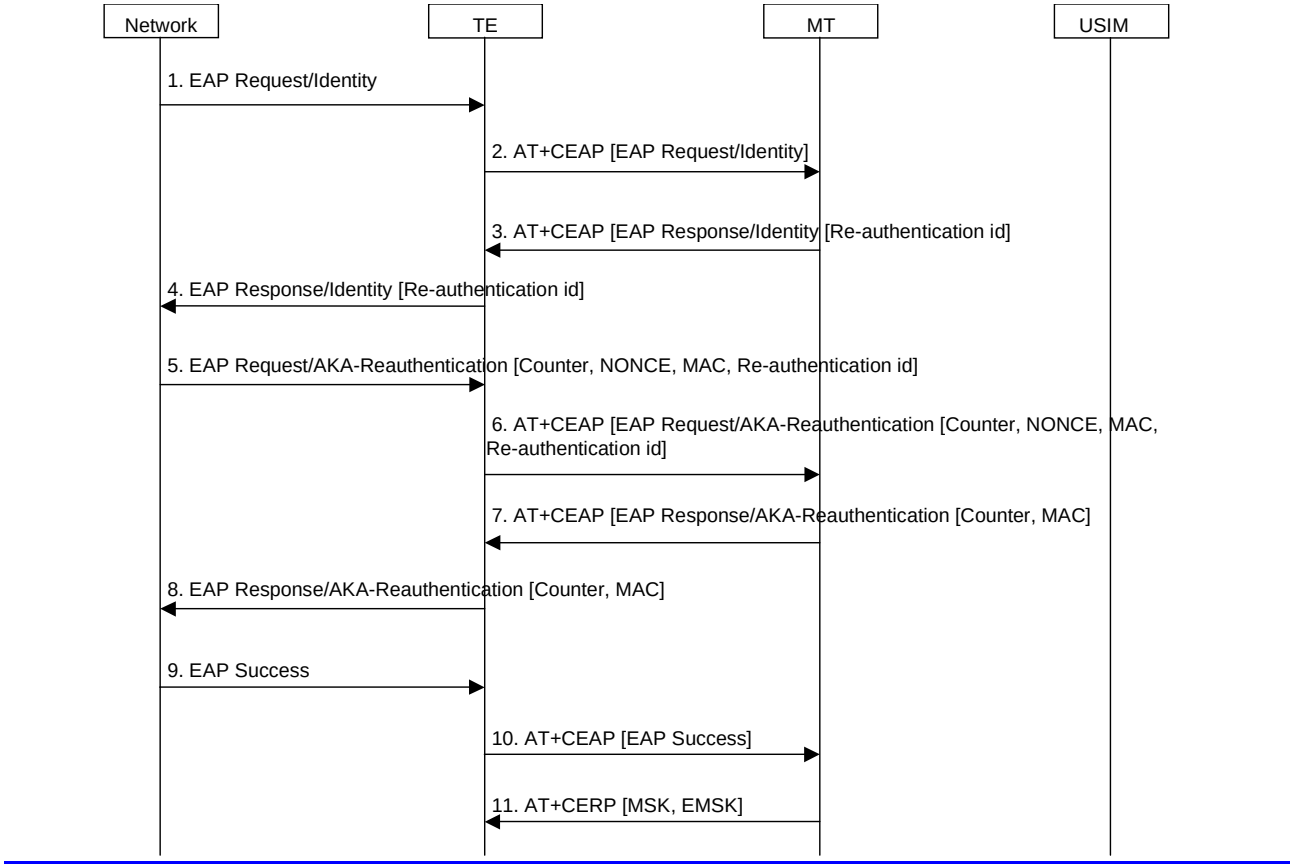


Figure 163: Fast re-authentication with EAP AKA

1. The network sends a EAP request identity message.
2. The TE sends the EAP packet received in message 1 to the MT using +CEAP AT command. ~~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.

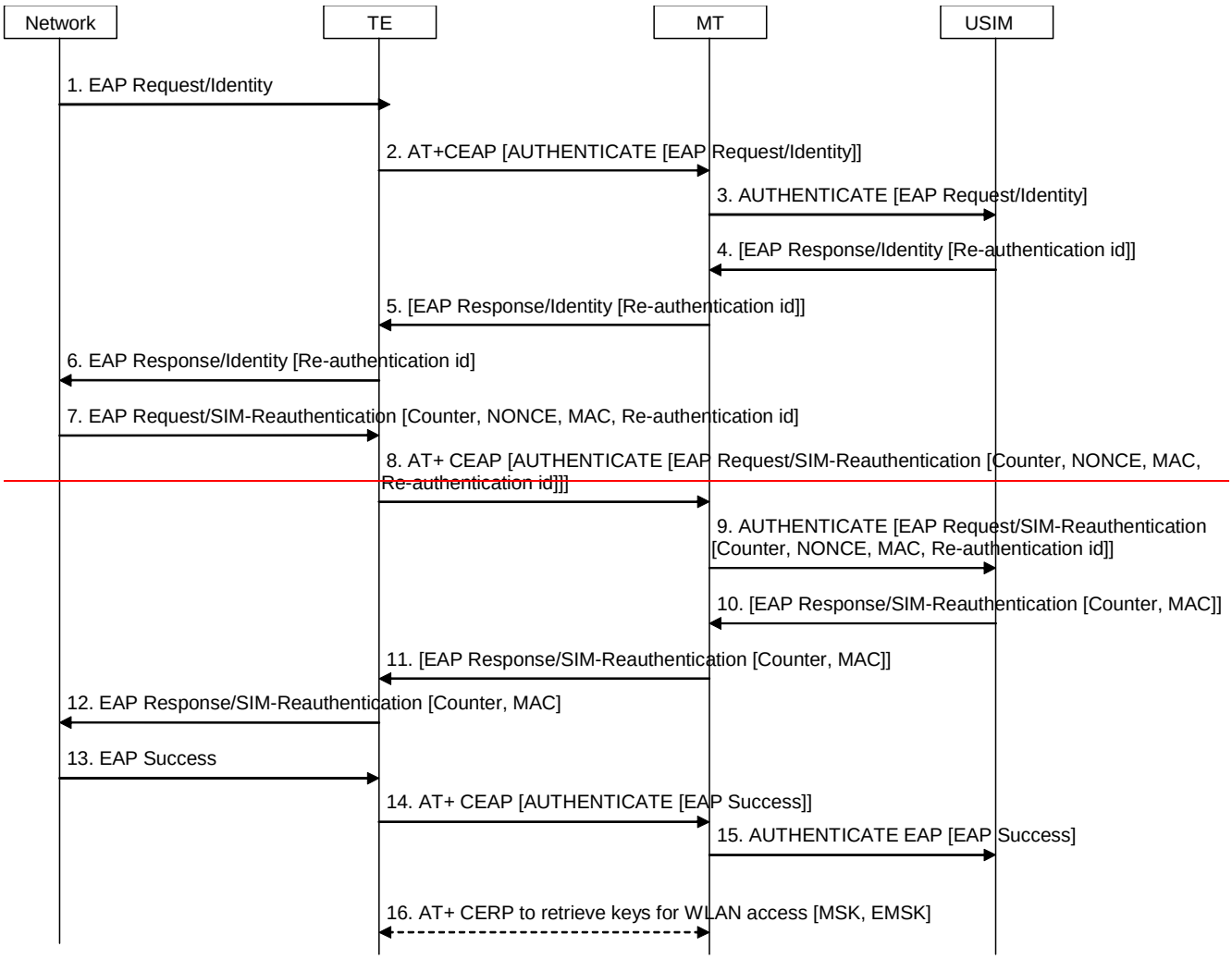
NOTE: The MT may need to access the USIM to check if there is a re-authentication id available. However, it is still to be decided whether the USIM will store the re-authentication identities.

4. The MT forwards the message to the network via the TE, using the +CEAP AT command.
5. The network sends the EAP AKA challenge with the needed parameters.
6. The TE transfers the message to the MT with the parameters, using the +CEAP AT command.
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 to the TE with the Counter received from the network, using the +CEAP AT command.
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 TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.
11. After receiving the success indication, the MT sends the new calculated MSK and EMSK and sends them to the TE, using the +CERP AT command.

6.7.4 Fast re-authentication with EAP SIM

6.7.4.1 Termination in the UICC

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 UICC application ~~USIM~~ to the TE when the fast re-authentication process is finished. The process is shown in figure 17.



~~Figure 17: Fast re-authentication with EAP SIM~~

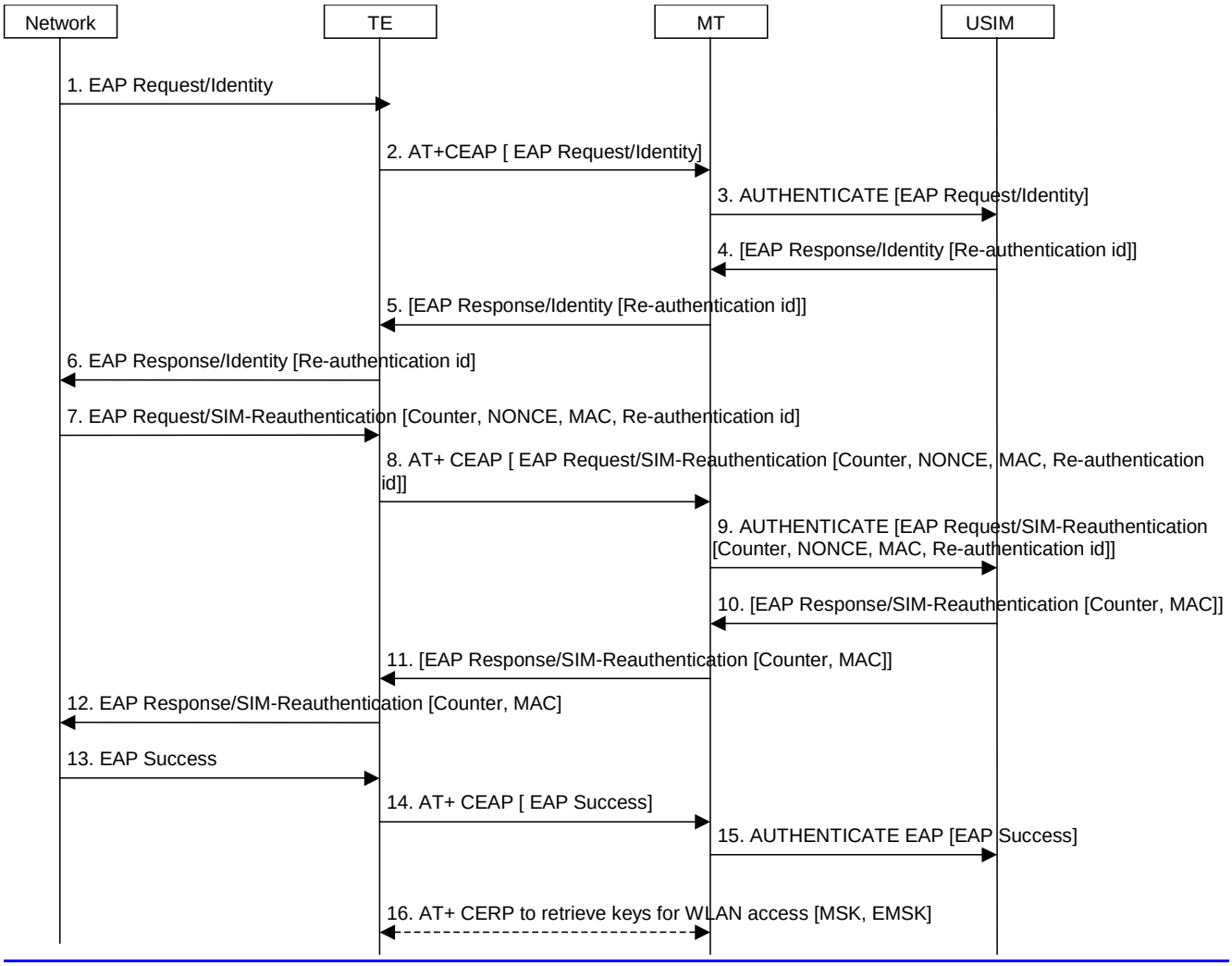


Figure 17: Fast re-authentication with EAP SIM

1. The network sends an EAP request identity message.
2. The TE ~~builds an EAP Authenticate command using~~sends the EAP packet received in message 1 ~~then sends this command~~ to the UICC application ~~USIM~~ using +~~CGLA~~CEAP AT command.
3. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [~~xx~~38]).
4. If the UICC application ~~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 UICC application ~~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~~CEAP 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~~sends the EAP packet received in message 7 ~~then sends this command~~ to the UICC application ~~USIM~~ via the ME using +~~CGLA~~CEAP AT command.

9. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command, as received in the AT command, to the USIM~~ (see TS 27.007 [~~xx~~38]).

10. The UICC application ~~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~~CEAP 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~~sends the EAP packet received in message 13 ~~then sends this command~~ to the UICC application ~~USIM~~ using +~~CGLA~~CEAP AT command.

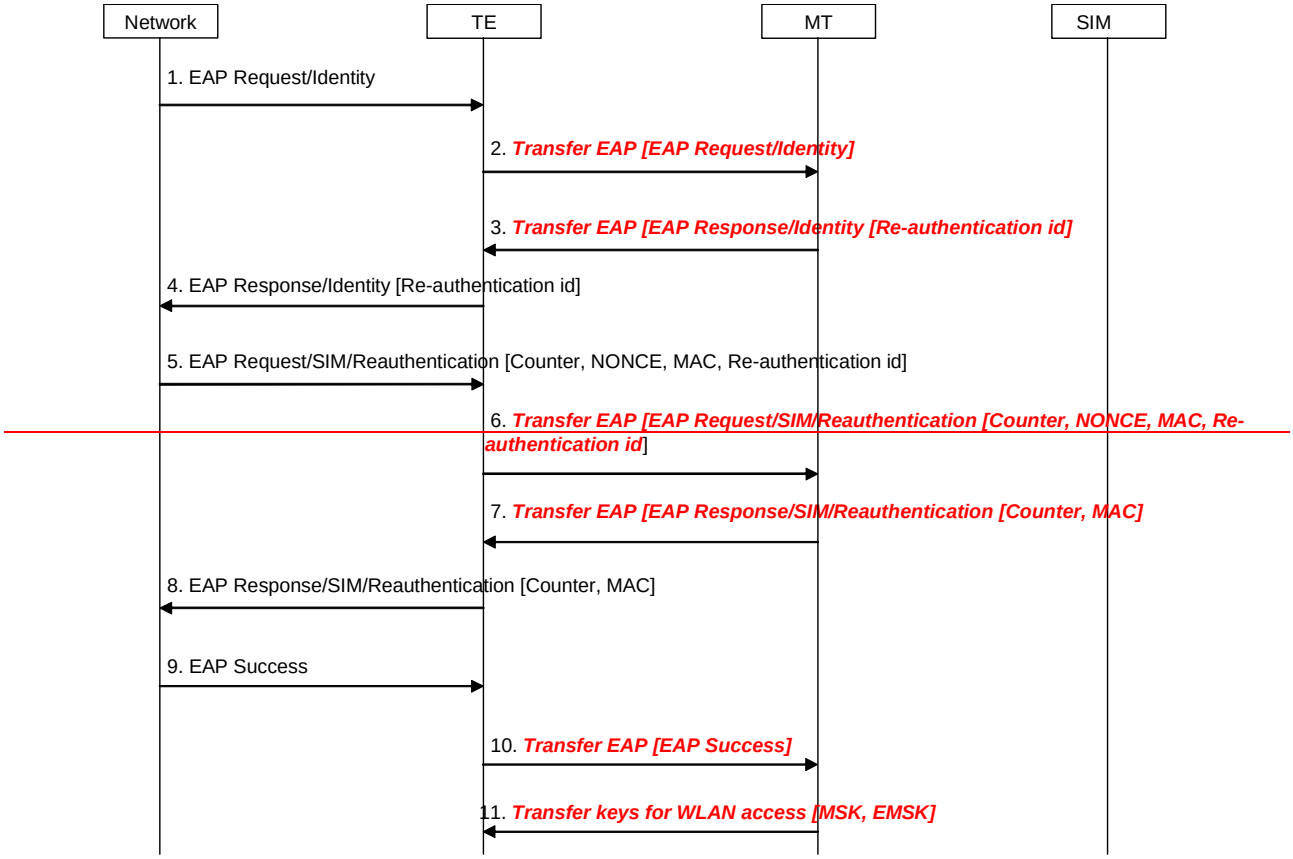
15. The MT performs the received +~~CGLA~~CEAP AT command ~~i.e. the MT sends the Authenticate command as it is to the USIM~~ (see TS 27.007 [38~~xx~~]).

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~~CERP AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

6.7.4.2 Termination in the MT

~~Editor's Note: AT command set for EAP termination in the MT is not yet defined.~~

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 figure 18~~4~~.


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]

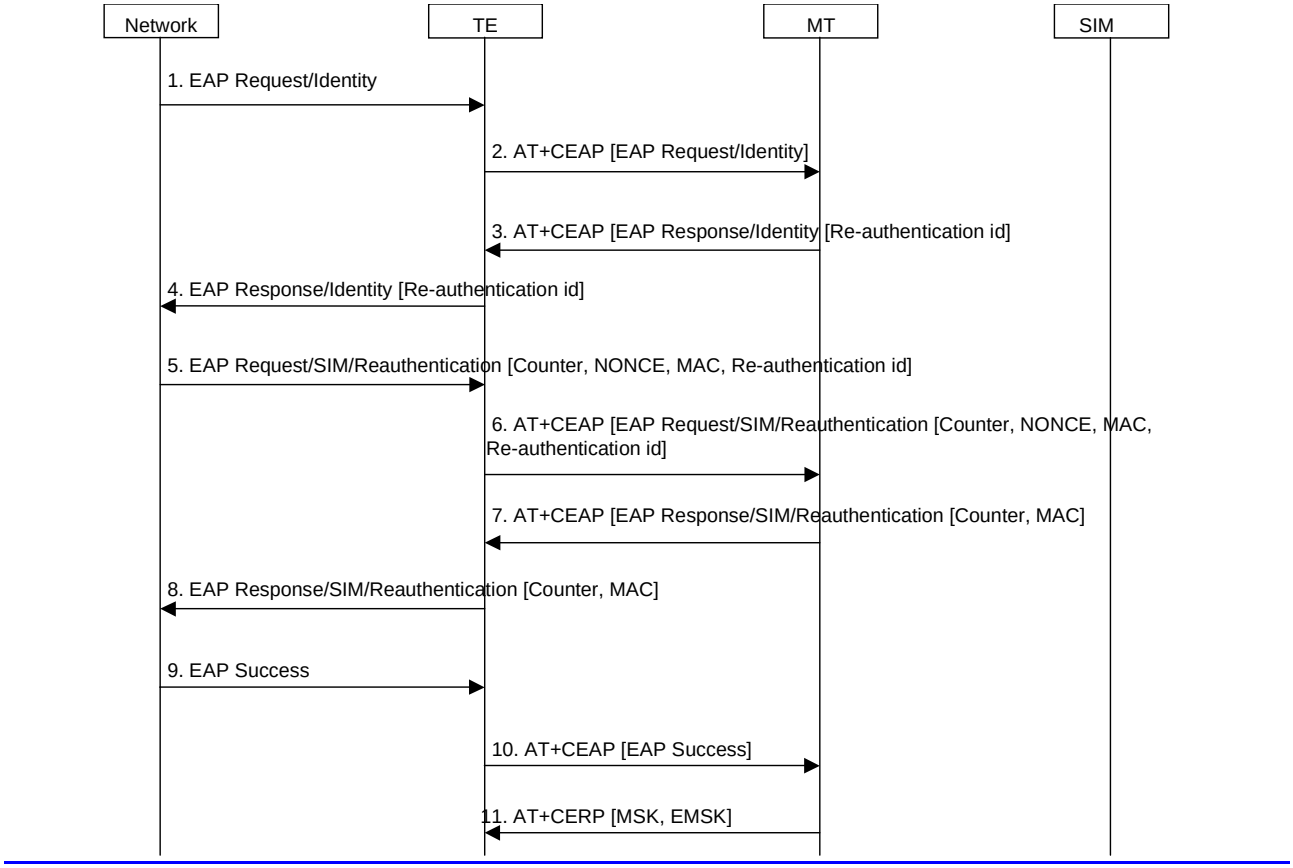


Figure 184: Fast re-authentication with EAP SIM

1. The network sends a EAP request identity message.
2. The TE sends the EAP packet received in message 1 to the MT using the +CEAP AT command. ~~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 to the TE with this fast re-authentication identity in the EAP response identity message, using the +CEAP AT command.

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 TE~~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, using the +CEAP AT command.
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 to the TE with the Counter received from the network, using the +CEAP AT command.
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 TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.
11. After receiving the success indication, the MT sends the new calculated MSK and EMSK and sends them to the TE, using the +CERP AT command.