3GPP TSG- SA WG3 SECURITY Meeting #34
Acapulco, Mexico, July 6-9 2004

Tdoc ⌘S3-040610

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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 authentication procedure for WLAN UE split
Source:	⌘	Huawei
Work item code:	⌘	WLAN-3G interworking security
Date:	⌘	08/07/2004
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:	⌘	The current TS describes the authentication procedures for WLAN UE split interworking. Some steps in the procedure are unnecessary and should be avoided to save resource on the MT. In particular, after the TE receives the EAP success message , the TE does not inform the MT . This means that the MT generates the MSK/EMSK and sends these keys to the TE without any indication from the TE. However, if there is an authentication failure, it is unnecessary that the MT generates these keys.
Summary of change:	⌘	Add a message between the TE and MT to indicate the authentication result to the MT.
Consequences if not approved:	⌘	MT will do unnecessary work in the authentication failure case

Clauses affected:	⌘	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:	⌘	

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:

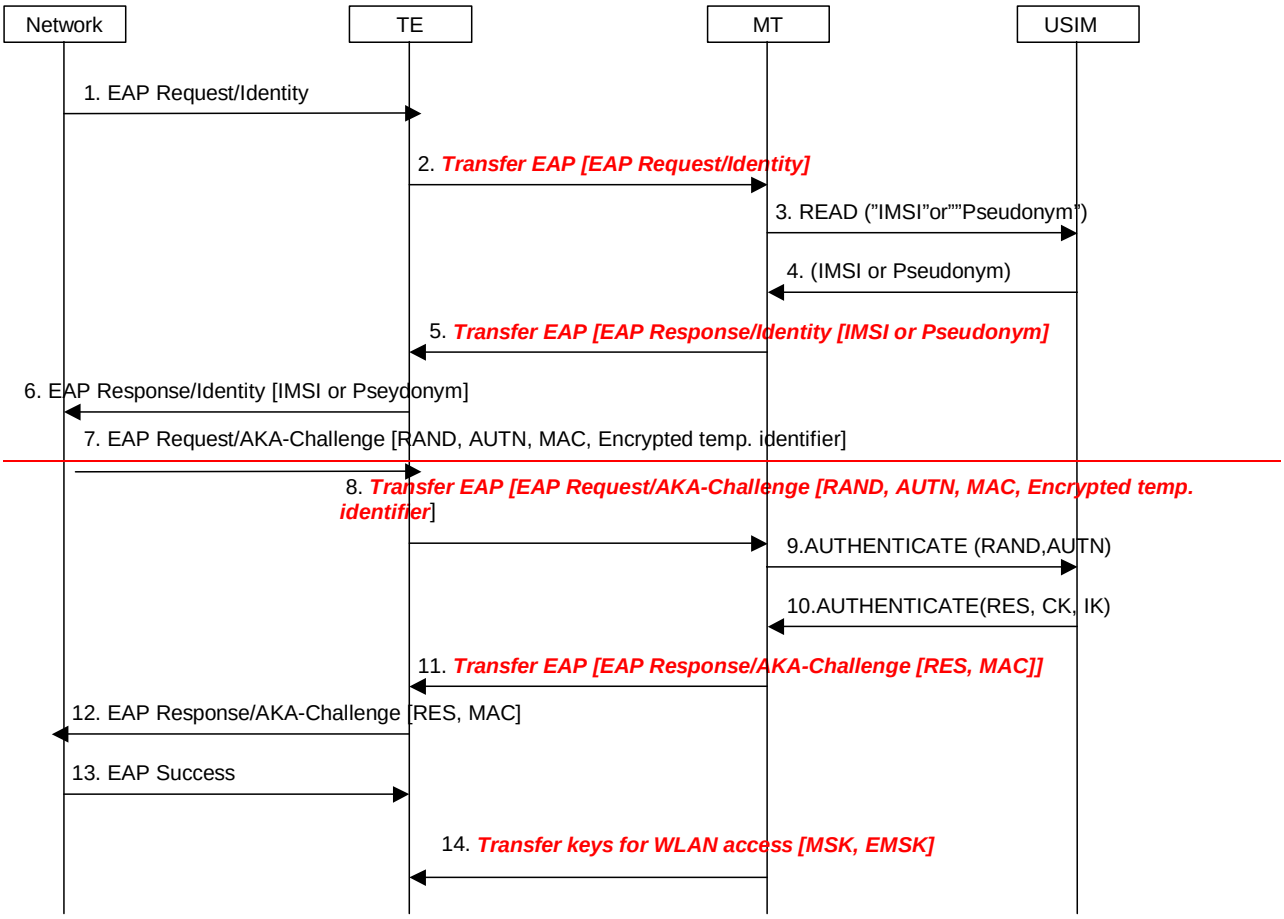
1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

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.

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 keys for WLAN access [MSK, EMSK]

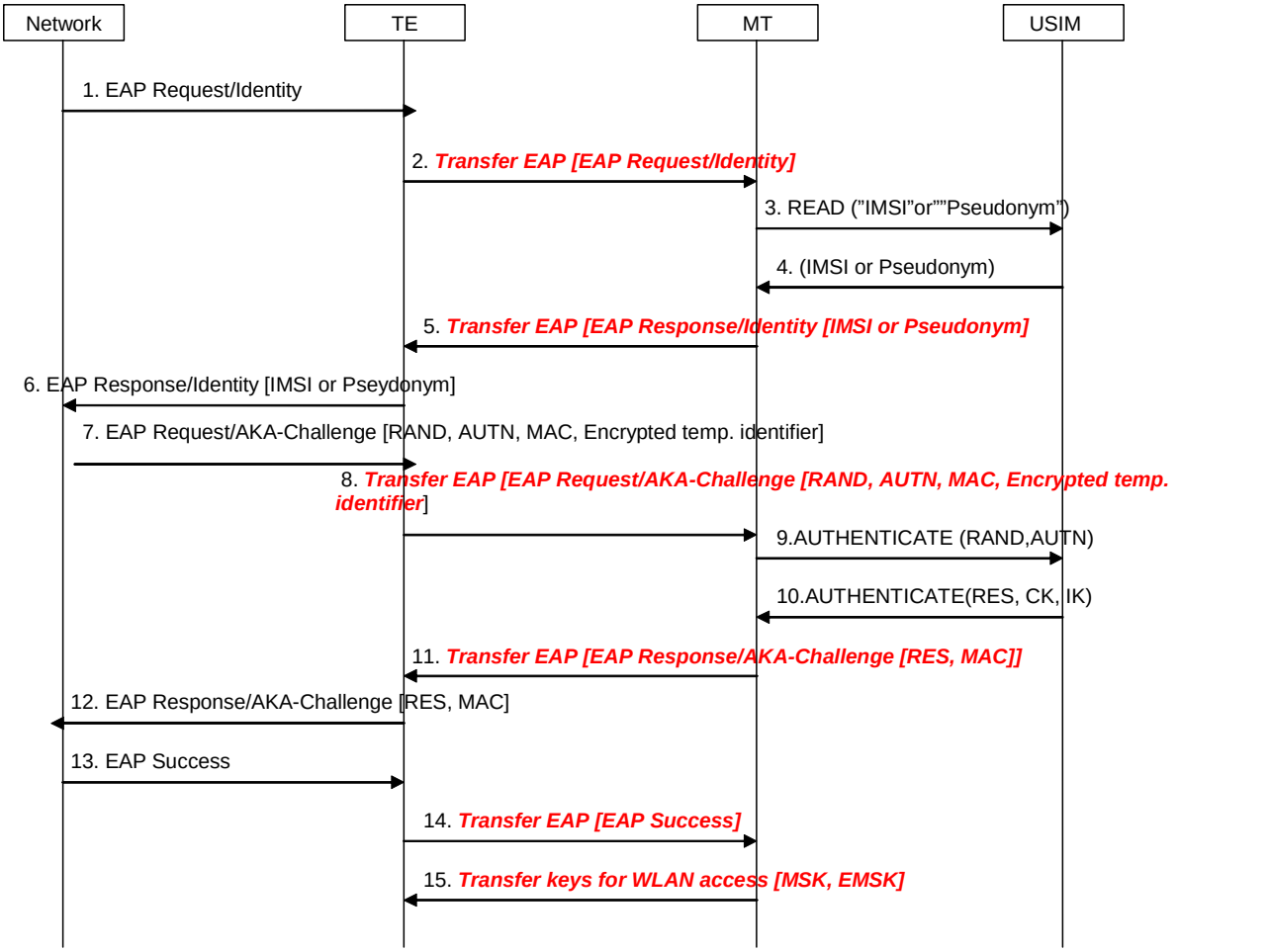

Network
TE
MT
USIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. READ (”IMSI”or””Pseudonym”)
4. (IMSI or Pseudonym)
5. Transfer EAP [EAP Response/Identity [IMSI or Pseudonym]
6. EAP Response/Identity [IMSI or Pseydonym]
7. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. 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]

Figure 11: Full authentication with EAP AKA

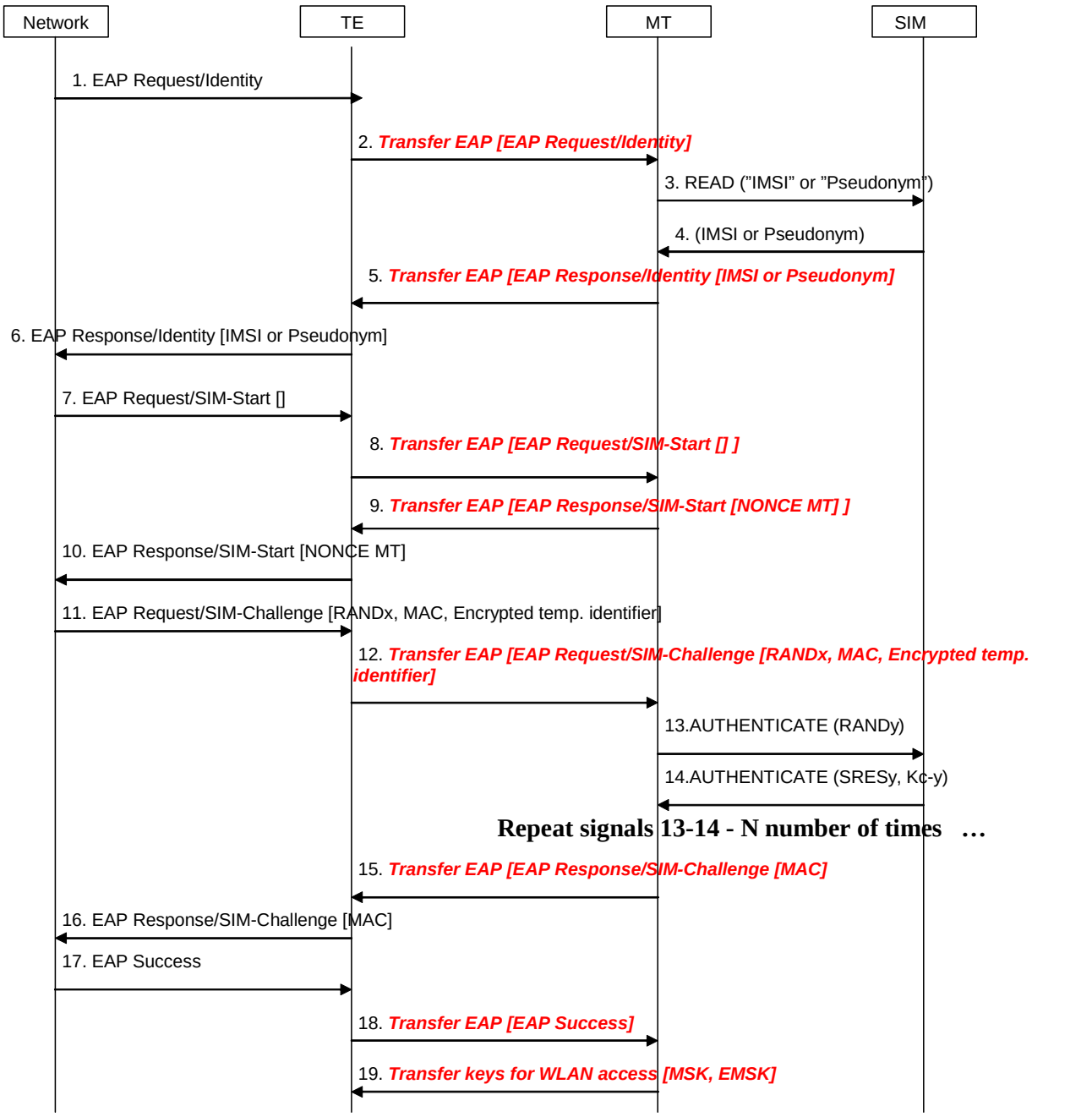
1. The network sends a EAP request identity (either a IMSI or a pseudonym) message to the TE (the device providing WLAN access) in order to initiate the procedure.
2. The EAP request identity message is forwarded via the Bluetooth interface to the MT.
3. If the MT does not have the identity available, 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 TE forwards the EAP success to the MT as a success indication.

~~14~~15. After receiving the success indication, ~~T~~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 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]

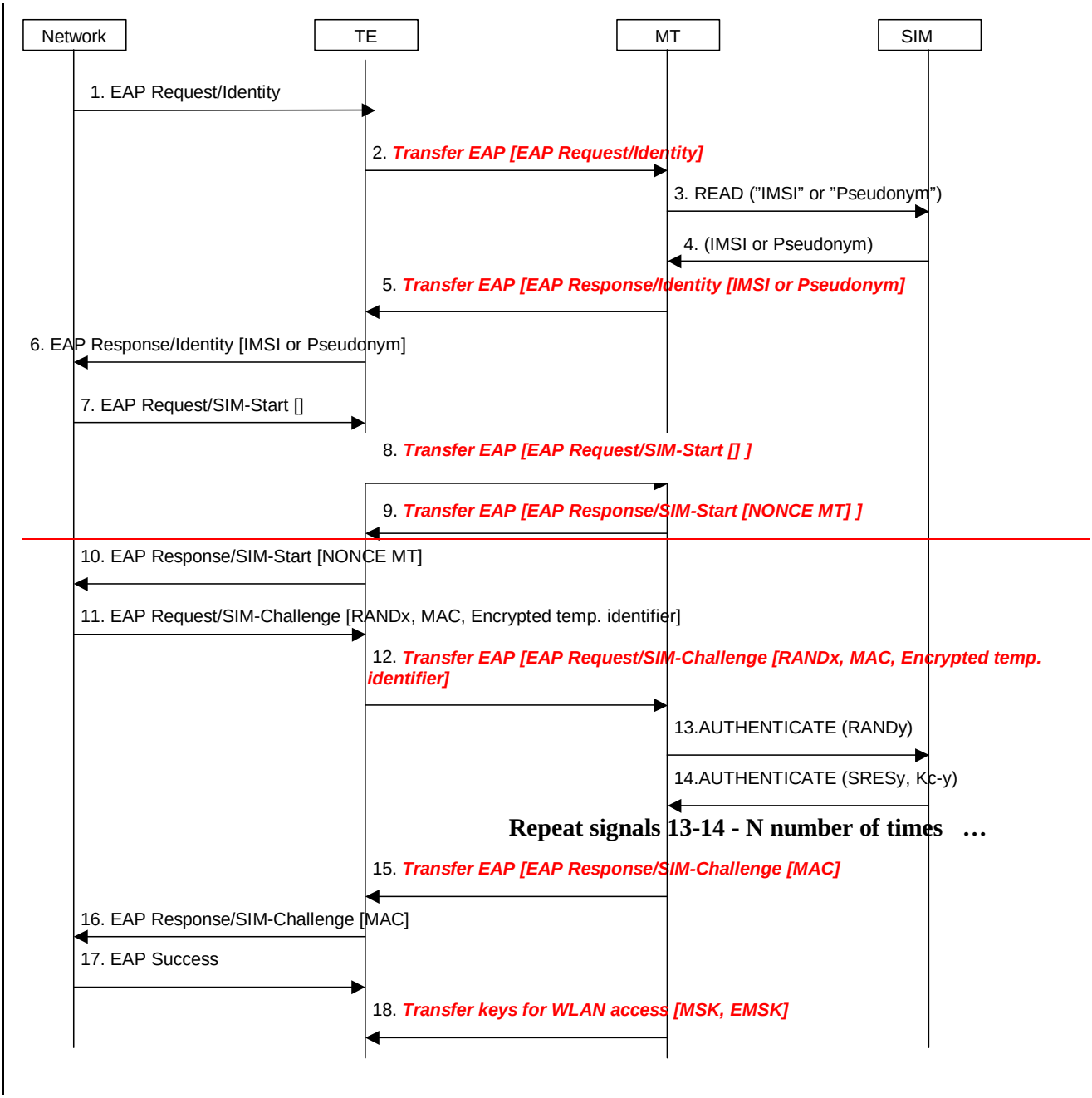


Figure 12: Full authentication with EAP SIM

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

~~18~~19. After receiving the success indication, ~~T~~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 figure 13.

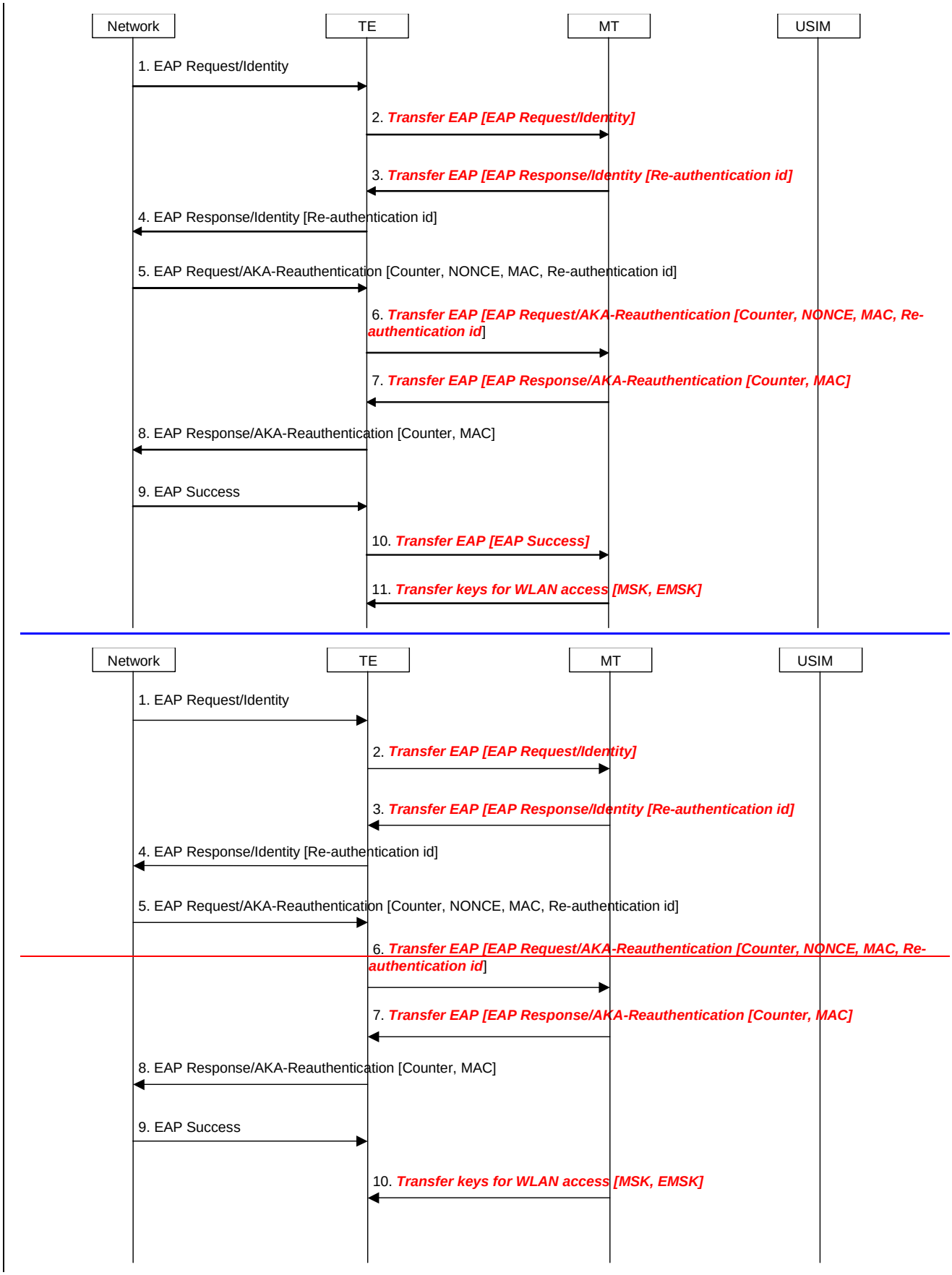


Figure 13: Fast re-authentication with EAP AKA

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.

~~10~~11. After receiving the success indication, ~~T~~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 figure 14.

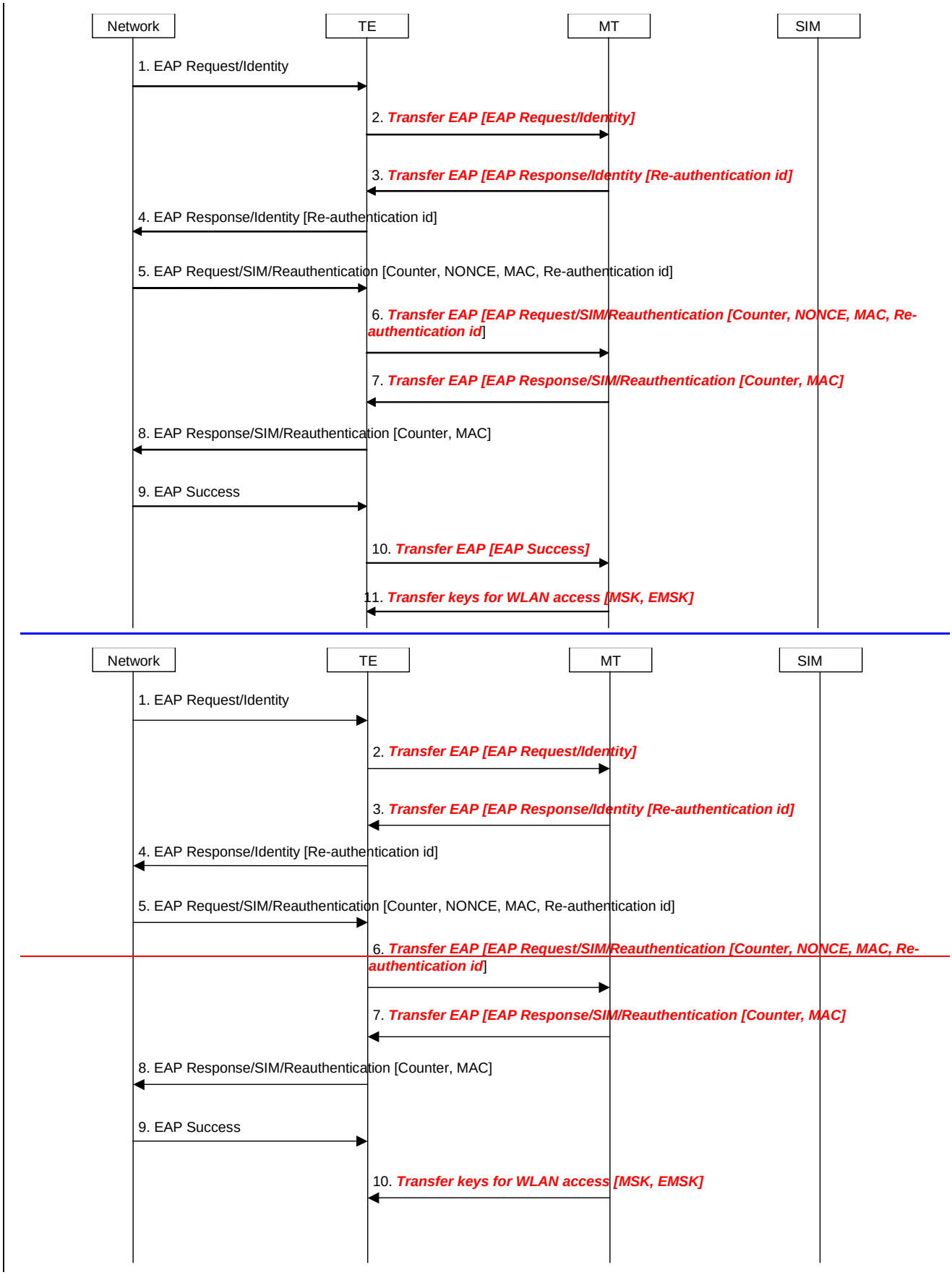


Figure 14: Fast re-authentication with EAP SIM

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

~~10~~11. After receiving the success indication, ~~T~~the MT sends the new calculated MSK and EMSK and sends them to the TE.