International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3202.1

(05/2008)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Signalling and control requirements and protocols to support attachment in NGN environments

Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN

Recommendation ITU-T Q.3202.1

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	**Q.3200–Q.3249**
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for NGN networks	Q.3900–Q.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3202.1

Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN

Summary

In Recommendation ITU-T Q.3202.1, a couple of authentication protocols for heterogeneous access authentication are discussed. 3GPP has standardized the 3GPP system-based EAP-AKA for interworking 3GPP and WLAN networks. The WiMax or WLAN device requires an external UICC reader for applying the current EAP-AKA defined in 3GPP TS 33.234. This Recommendation proposes to apply the EAP-AKA protocol to non-3GPP network devices not equipped with UICC for interworking among 3GPP, WiMax, and WLAN in NGN.

Source

Recommendation ITU-T Q.3202.1 was approved on 22 May 2008 by ITU-T Study Group 11 (2005-2008) under Recommendation ITU-T A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T Q.3202.1

Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN

1 Scope

This Recommendation describes the authentication protocol based on the EAP-AKA for interworking 3GPP, WiMax [b-IEEE 802.16e], and WLAN [b-IEEE 802.11] access in NGN. 3GPP has standardized the 3GPP system-based EAP-AKA for interworking 3GPP and WLAN networks. The WiMax or WLAN device, however, requires an external UICC reader. Without UICC, the EAP-AKA mechanism loses its own advantages in security and portability aspects. This Recommendation proposes a modified version of the EAP-AKA protocol for extending its usage to existing WiMax/WLAN devices. In this Recommendation, two EAP-AKA full authentication protocols are described and proposed. Also, the fast re-authentication procedure of EAP-AKA is described.

1.1 Relationship

Work for this Recommendation is based upon the context of [ITU-T Q.3201]. This Recommendation complies with the EAP-based security signalling architecture for network attachment in [ITU-T Q.3201], and considers the compatibility with the functional architecture in [ITU-T Y.2012].

This Recommendation refers to [ETSI TS 133 234] for authentication protocol based on EAP-AKA with UICC and fast re-authentication procedure.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.3201] Recommendation ITU-T Q.3201 (2007), *EAP-based security signalling protocol architecture for network attachment*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN Release 1*.

[ETSI TS 133 102] ETSI TS 133 102 (2006), *Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102 version 7.1.0 Release 7)*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=25801>

[ETSI TS 133 234] ETSI TS 133 234 (2007), *Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234 version 7.5.0 Release 7)*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=27022>

3 Abbreviations

This Recommendation uses the following abbreviations:

AAA Authentication, Authorization and Accounting

ACR Access Control Router

AK Authentication Key

AKA Authentication and Key Agreement

AM-FE Access Management Functional Entity

AS Authentication Server

AV Authentication Vector

CK Confidentiality Key

DH Diffie-Hellman

EAP Extensible Authentication Protocol

EP Enforcement Point

GGSN Gateway GPRS Support Node

ID IDentity

IK Integrity Key

IMSI International Mobile Subscriber Identity

MAC Message Authentication Code

NACF Network Attachment Control Functions

RAS Radio Access Station

SGSN Serving GPRS Support Node

TAA-FE Transport Authentication and Authorization Functional Entity

TUP-FE Transport User Profile Functional Entity

UE User Equipment

UICC UMTS IC Card

USIM Universal Subscriber Identity Module

UTRAN UMTS Terrestrial Radio Access Network

VPLMN Visited Public Land Mobile Network

WAG Wireless Access Gateway

WiMax Worldwide Interoperability for Microwave Access

WLAN Wireless Local Area Network

4 Security Requirements for Authentication Interworking

- The EAP-AKA authentication protocol shall be applied easily to any mobile networks in NGN.
  - Mobile terminals equipped with UICC
  - Mobile terminals not equipped with UICC
- Authentication mechanisms in NGN shall include mutual authentication and key agreement.
- The key distribution and freshness for protecting signalling and user data on the wireless link shall be supported.

- Authentication protocols shall be secure against several attacks:
  - Man-in-the-middle attack (MITM)
  - Replay attack
  - Impersonation attack
  - Forgery attack
  - Dictionary attack
  - Eavesdropping
- A full re-authentication procedure shall be supported.
- A fast re-authentication procedure may be supported.

5 Network architecture for access authentication interworking in NGN

This clause describes the network model for access authentications interworking among the 3GPP, WiMax, and WLAN in NGN. There are two approaches. One approach is to apply WLAN authentication model based on the 3GPP system, defined in [ETSI TS 133 234], for heterogeneous access authentication. Figure 1 shows the 3GPP system-based authentication.

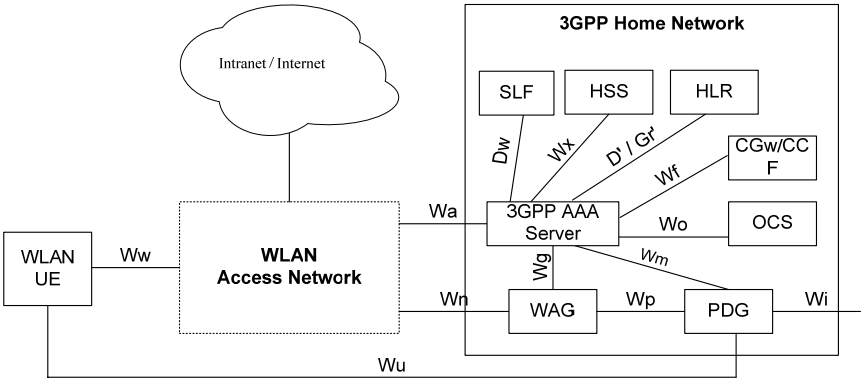

Figure 1 – 3GPP system-based authentication model

The other proposal is the authentication model, based on the function entities of NGN, as shown in Figure 2. The network architecture might be classified into four components of NGN: AR-FE, AM-FE, TAA-FE, and TUP-FE. This Recommendation describes signalling protocols for access authentication in this architecture. Also, the signalling protocols based on authentication model specified in [ITU-T Q.3201] are provided. Figures 3 and 4 show an integrated authentication model defined in [ITU-T Q.3201].

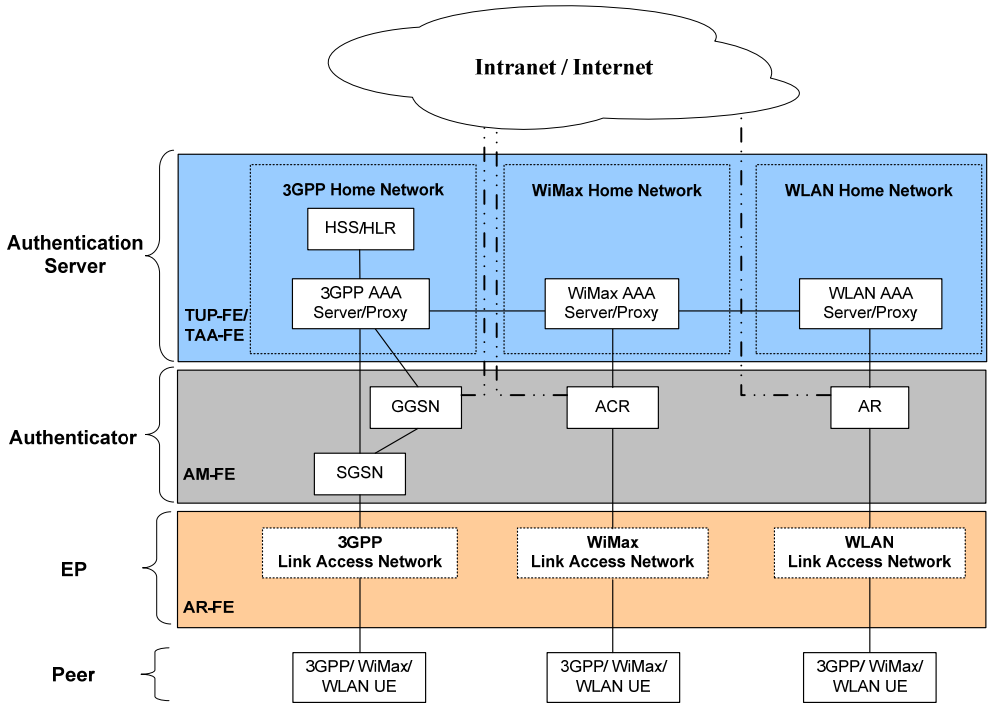

Figure 2 – An example authentication architecture for interworking among wireless access networks in NGN

Figure 3 shows an integrated authentication model, which is being controlled by an authenticator. The peer sends authentication information to the enforcement point, and the enforcement points forward it to the authenticator. This architecture helps the authenticator manage the authentication procedure.

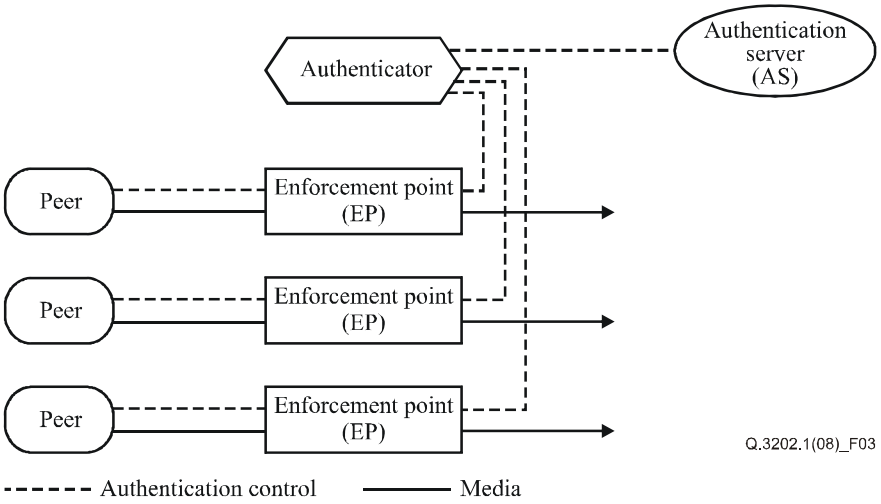

Figure 3 – Integrated authentication model

Figure 4 illustrates an integrated authentication model in NGN. It is assumed that the network attachment control function entities are the authenticator (AM-FE) and authentication server (TUP-FE/TAA-FE), and the AR-FE in access transport acts as the enforcement point. The AR-FE performs filtering data packet allowing only the authenticated packets. After successful authentication of the end-user function, the access transport allows the packets from the end-user function to be entered into the access network.

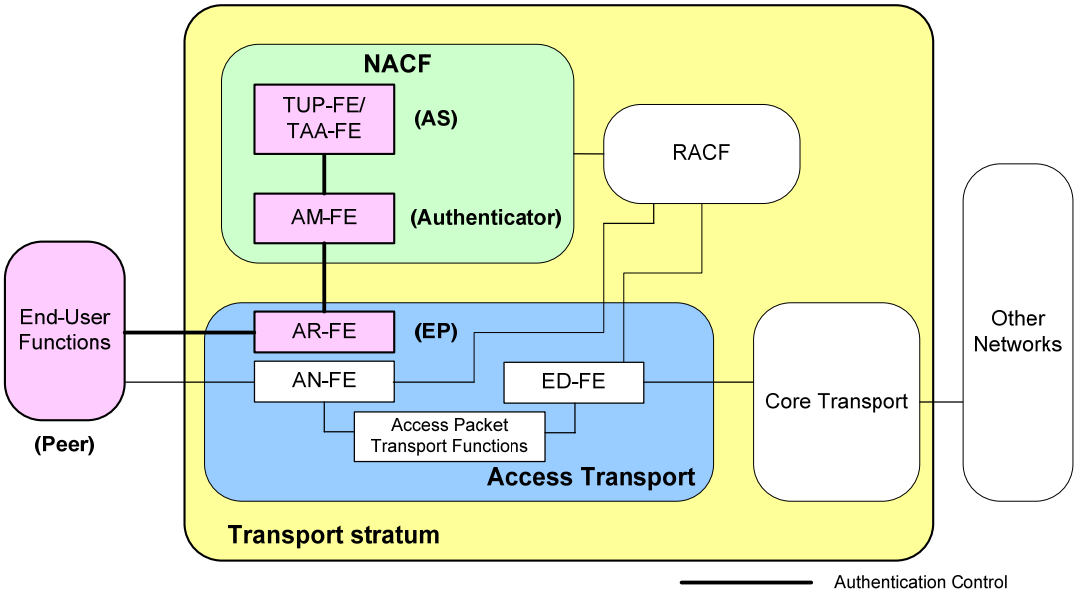

Figure 4 – An example of an integrated authentication model in NGN

6 Authentication protocols based on EAP-AKA for heterogeneous access authentication

The authentication protocols based on EAP-AKA for heterogeneous access authentication are shown in Appendix I. Appendix I describes how three authentication protocols based on EAP-AKA, two EAP-AKA authentication protocols for interworking authentication in wireless access (e.g., 3GPP, [b-IEEE 802.16e], and [b-IEEE 802.11]) and the fast re-authentication procedure of the EAP-AKA in NGN, could be used to provide authentication in heterogeneous access network. The existing EAP-AKA with UICC is basically used for access authentication mechanism in 3GPP, WiMax, and WLAN networks. This scheme requires that the WiMax or WLAN UE should be equipped with UICC card for access authentication. To solve this problem, this Recommendation proposes an access authentication scheme without UICC: EAP-AKA based on a password. The EAP-AKA based on a password provides access authentication for the UE without UICC. The UE equipped with the AKA algorithm uses Diffie-Hellman key instead of the long-term secret key stored in UICC.

7 Security considerations

Since the 3GPP system-based EAP-AKA uses a long-term key shared between the UICC and HSS/HLR, it can provide strong security and portability. Compared to the 3GPP system-based EAP-AKA, the proposed EAP-AKA based on non-UICC can also provide robust and enhanced security functions.

The dictionary attack in authentication protocol based on a password is the most critical attack. In the proposed protocol with non-UICC, it is impossible for an attacker to guess a legitimate password by obtaining public values during authentication session. The password in the authentication messages is protected against dictionary attack owing to the one-way hash function, random numbers, and discrete logarithm problem (DLP).

The perfect forward secrecy (PFS) and perfect backward secrecy (PBS) are very important security requirements, which mean that disclosure of a long-term key in the EAP-AKA should not reveal all the previous and upcoming communications. If an attacker gets a UICC, the attacker can disclose a long-term key by a physical access to the storage medium, which means that PFS and PBS are not provided. The EAP-AKA with non-UICC, however, provides PFS and PBS because the DH session

key is changed whenever the authentication procedure for generating a set of AVs is performed. In other words, it uses a short-term key.

The proposed EAP-AKA with non-UICC is secure against replay attack because DH private keys are changed every authentication procedure. Also, it can protect the UE and the TAA-FE against MITM attack using a password.

Appendix I

Example authentication in heterogeneous environments

(This appendix does not form an integral part of this Recommendation)

This appendix describes how two EAP-AKA authentication protocols and a fast re-authentication procedure could be used to provide authentication when heterogeneous accesses are used.

I.1 Example using EAP-AKA with UICC authentication mechanism

The EAP-AKA [b-IETF RFC 4187] authentication scheme for interworking between the 3GPP and WLAN is specified in [ETSI TS 133 234]. This clause shows that this mechanism is also used in the WiMax technology for interworking between the 3GPP and WLAN terminals. The complete operation is defined in [b-IETF RFC 4187].

Operational steps of the EAP-AKA with UICC:

1. The control channel between the UE and access network functions is established (out of the scope of this Recommendation).
2. The AR-FE notifies the AM-FE that the control channel is established between the UE and access network functions.
3. The AM-FE sends an EAP Request/Identity message to the UE.
4. The UE responds with an EAP Response/Identity including NAI based on a pseudonym or IMSI.

   The EAP message is routed towards the UE's AAA server based on the realm part of the NAI. The EAP message may be passed by one or several AAA proxies. The TAA-FE acts as an AAA server.
5. The communication between the AM-FE and TAA-FE may be achieved using the AAA protocol, such as Diameter [b-IETF RFC 3588] and [b-IETF RFC 4072] or Radius [b-IETF RFC 3579] and [b-IETF RFC 2865]. The AM-FE may act as an AAA client and the TAA-FE may act as an AAA server. The AM-FE generates a diameter AVP including the EAP payload and forwards the diameter message to the TAA-FE. Upon receiving the message, the TAA-FE retrieves the EAP Response/Identity message including the user identity, identifier of the access network, and VPLMN identity from the received diameter message.

   NOTE – This Recommendation omits AAA communication between the AM-FE and TAA-FE to simply description.
6. The TAA-FE identifies the subscriber, and then checks whether it has unused AV for the subscriber or not. If not, the TAA-FE retrieves a set of new AVs from the TUP-FE.
7. The TAA-FE sends an EAP Request/AKA-Identity again to the UE in order to request the subscriber identity. There exist some situations that intermediate nodes between the UE and the TAA-FE may have revised or replaced the user's identity received in the EAP Response/Identity message, as specified in [ETSI TS 133 234]. For the reason, this procedure may be performed. The service operator, however, can omit this new request if there exists the assurance that the user identity is not changed or modified by some reasons during EAP-AKA procedure.
8. The AM-FE sends the EAP Request/AKA-Identity to the AR-FE, and the AR-FE forwards the message to the UE.
9. The UE responds to the new request with the same identity. The AR-FE forwards the EAP Response/AKA-Identity including the same identity to the AM-FE.

10. The AM-FE sends the message to the TAA-FE. If the identity in the two messages of the EAP Response/Identity and EAP Response/AKA-Identity is the same, the TAA-FE will use the AV for authentication process. Otherwise, the TAA-FE shall repeat step 6 before step 11.
11. The TAA-FE checks whether it has the access network profile of the subscriber or not. If not, the TAA-FE retrieves the profile from the TUP-FE. The TAA-FE verifies whether or not the user is authorized to utilize the network service.
12. The TAA-FE derives new keying materials required by the EAP-AKA from IK and CK, see [ETSI TS 133 234]. Also, some additional keying materials may be generated for message confidentiality and/or integrity in the WiMax or WLAN environment.
13. The TAA-FE sends the EAP Request/AKA-Challenge that contains the RAND, AUTN, and MAC value to the AM-FE. The MAC is computed by using the new keying material derived from IK and CK. If two user identities, such as pseudonym and re-authentication identifier, are generated, they are also transferred securely to the AR-FE. The re-authentication identifier depends on whether the network operator allows the UE to perform re-authentication process in the access network or not. The TAA-FE may send a result indication to the UE. It also depends on the home operator's policies.
14. The AM-FE sends the EAP Request/AKA-Challenge message to the AR-FE, and the AR-FE forwards the message to the UE.
15. The UE performs the UMTS algorithm on the UICC. The UICC verifies the received AUTN to authenticate the network. If it is successful, the UICC computes RES, IK, and CK based on a long-term key. The UE derives new keying material from the new IK and CK, and then verifies the received MAC using the new derived keys. If the UE received a protected pseudonym and(or) re-authentication identity, it stores the received identity for future authentication.
16. The UE computes a new MAC value with the new derived key, and then sends the EAP Response/AKA-Challenge including the computed RES and the new MAC to the AR-FE. The UE may send a result indication to the TAA-FE if it received the result indication from the TAA-FE. It also depends on the home operator's policies. The AR-FE forwards the messages to the AM-FE.
17. The AM-FE forwards the EAP Response/AKA-Challenge message to the TAA-FE.
18. The TAA-FE verifies the received MAC, and then compares the XRES with the received RES.
19. If all validation is successful, the TAA-FE sends the EAP Request/AKA-Notification that notifies the success of the authentication to the UE. This notification can be protected by using a MAC.
20. The AM-FE sends the EAP message to the AR-FE, and it forwards the EAP message to the UE.
21. The UE sends the EAP Response/AKA-Notification to the AM-FE through the AR-FE.
22. The AM-FE sends the EAP Response/AKA-Notification to the TAA-FE.
23. The TAA-FE sends the EAP Success with keying material for providing message confidentiality and/or integrity in the WiMax or WLAN to the AM-FE.
24. The AM-FE sends the EAP Success to the AR-FE. The AR-FE stores the keying material. In future, the keying material is used to communicate with the UE.
25. The AR-FE informs the UE that its authentication and key distribution have been successful and complete.
26. The user channel is established between the UE and AN. The UE can access the network such as the 3GPP, WiMax, and WLAN.

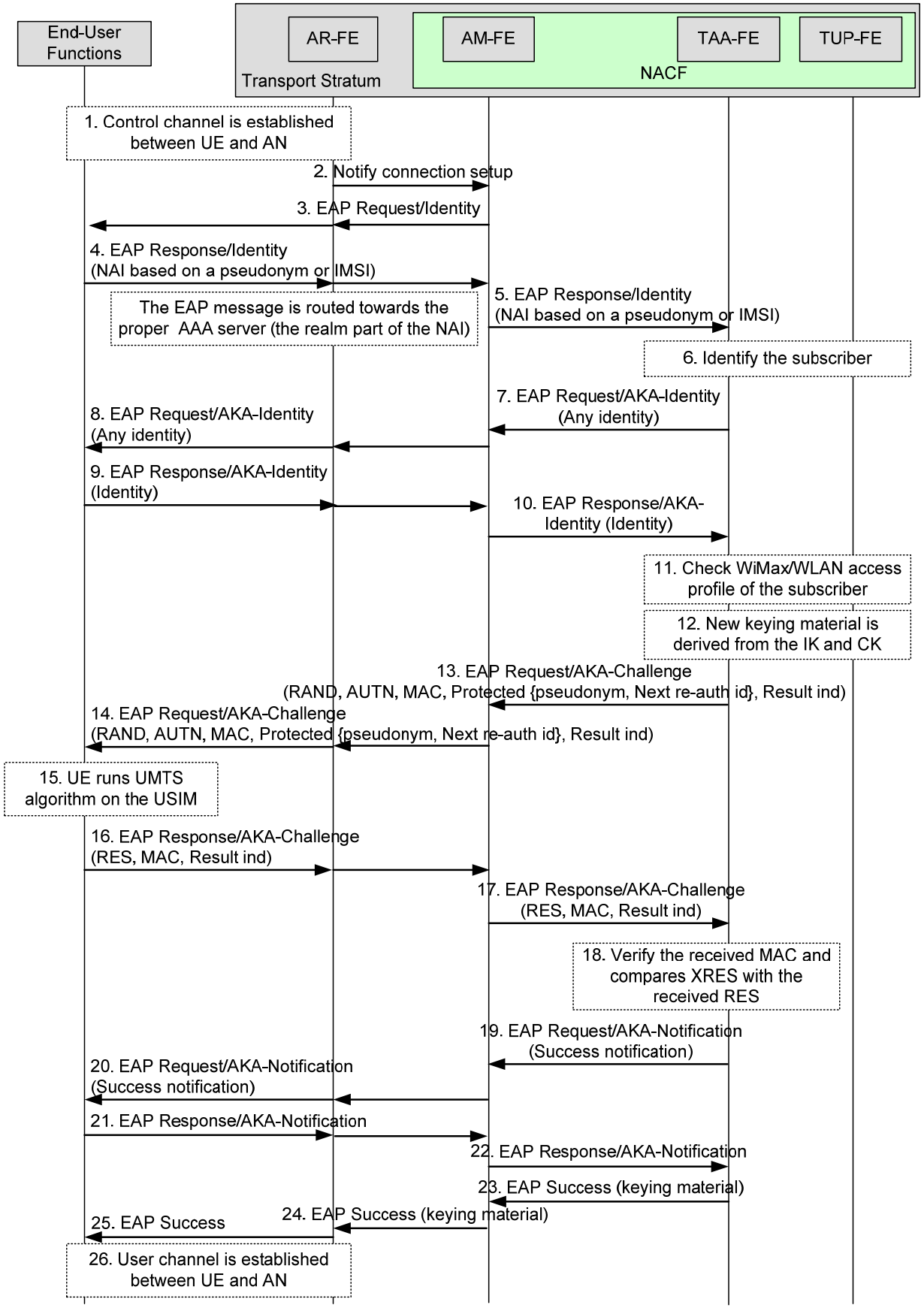

Figure I.1 – Authentication protocol based on EAP-AKA scheme with UICC in NGN

I.2 Example using EAP-AKA based on a password and the Diffie-Hellman algorithm

This clause proposes an access authentication protocol which uses a non-UICC authentication mechanism. Specifically, the example uses EAP-AKA based on a password and Diffie-Hellman (DH) key exchange algorithm among 3GPP, WiMax, and WLAN terminals. The proposed scheme can be used for legacy terminals with and without UICC. The legacy terminals only require an AKA algorithm based on a software module. Therefore, this authentication mechanism does not use a long-term secret key in UICC but a DH key generated through the authentication procedure. 3GPP AKA functions f1, f1*, f2, f3, f4, f5, and f5* used in this mechanism are the same as EAP-AKA with UICC.

Operational steps of the EAP-AKA with non-UICC:

1. The control channel between the UE and access network functions is established (out of the scope of this Recommendation).
2. The AR-FE notifies the AM-FE that the control channel is established between the UE and access network functions.
3. The AM-FE sends an EAP Request/Identity message to the UE.
4. The UE responds with an EAP Response/Identity including NAI based on a pseudonym or IMSI.

   The EAP message is routed towards the UE's AAA server based on the realm part of the NAI. The EAP message may be passed by one or several AAA proxies. The TAA-FE acts as an AAA server.
5. The communication between the AM-FE and TAA-FE may be achieved using the AAA protocol, such as Diameter [b-IETF RFC 3588] and [b-IETF RFC 4072] or Radius [b-IETF RFC 3579] and [b-IETF RFC 2865]. The AM-FE may act as an AAA client and the TAA-FE may act as an AAA server. The AM-FE generates a diameter AVP including the EAP payload and forwards the diameter message to the TAA-FE. Upon receiving the message, the TAA-FE retrieves the EAP Response/Identity message including the user identity, identifier of the access network, and VPLMN identity from the received diameter message.

   NOTE – This Recommendation omits AAA communication between the AM-FE and TAA-FE to simply description.
6. The TAA-FE identifies the subscriber, and then checks whether it has unused AVs for the subscriber or not. If not, the TAA-FE retrieves a set of new AVs from the TUP-FE. The new AV will be calculated after receiving the DH value of the UE (step 10).

   In the EAP-AKA with non-UICC, the TUP-FE should store user's password verifier *g^pwd*, where *pwd* is the user's password.
7. The TAA-FE sends an EAP Request/AKA-Identity again to the UE in order to request the subscriber identity. There exist some situations that intermediate nodes between the UE and the TAA-FE may have revised or replaced the user's identity received in the EAP Response/Identity message, as specified in [ETSI TS 133 234]. For the reason, this procedure may be performed. The service operator, however, can omit this new request if there exists assurance that the user identity is not changed or modified by some reasons during EAP-AKA procedure.
8. The AM-FE sends the EAP Request/AKA-Identity to the AR-FE, and it forwards the message to the UE.
9. The UE without UICC generates a DH value *g^(x+pwd)* mod *p*, where the *p* is a large prime number, the *g* is primitive root modular *p*, the *x* is a random number, the expression "^" is exponent operation, and the expression "mod" is modular operation. For a simple expression, this recommendation omits the expression "mod *p*" (e.g., not "*g^(x+pwd)* mod

p" but "*g*^(*x*+*pwd*)"). The UE also computes the value *H*(*g*^*pwd*, *g*^*x*||*Identity*), where *H*() is one-way hash function, such as SHA-1 and || is concatenation. The UE responds with the new request EAP Response/AKA-Identity including the computed values and the same identity. The AR-FE forwards the EAP Response/AKA-Identity to the AM-FE.

10. The AM-FE sends the message to the TAA-FE. If the identity in the two messages of the EAP Response/Identity and EAP Response/AKA-Identity is the same, the TAA-FE will use the AV for authentication process. Otherwise, the TAA-FE shall repeat step 6 before step 11.

11. The TAA-FE checks that it has the access network profile of the subscriber. If not, the TAA-FE retrieves the profile from the TUP-FE. The TAA-FE verifies whether or not the user is authorized to utilize the network service.

    The TUP-FE creates the AKA values based on the password and DH algorithm. The TUP-FE generates a value *g*^*x* by computing *g*^(*x*+*pwd*)/*g*^*pwd* and verifies the received hash value *H*(*g*^*pwd*, *g*^*x*||*Identity*). If it is successful, the TUP-FE generates a random value y and computes a DH value *g*^*y* and *g*^*xy*. Finally, the TUP-FE runs 3GPP AKA functions f1, f1*, f2, f3, f4, f5, and f5* with the DH session key *g*^(*xy*) to generate a new AV. The TUP-FE distributes the new AV to the TAA-FE.

12. The TAA-FE derives new keying materials required by the EAP-AKA from IK and CK, see [ETSI TS 133 234]. Also, some additional keying materials may be generated for message confidentiality and/or integrity in the WiMax or WLAN environment.

13. The TAA-FE sends the EAP Request/AKA-Challenge that contains the RAND, AUTN, and MAC value to the AM-FE. The MAC is computed by using the new keying material derived from IK and CK. If two user identities, such as pseudonym and re-authentication identifier, are generated, they are also transferred securely to the AR-FE. The re-authentication identifier depends on whether network operator allows the UE to perform re-authentication process in the access network or not. The TAA-FE may send a result indication to the UE. It also depends on the home operator's policies.

    In the EAP-AKA with non-UICC, the TAA-FE also sends the values *g*^(*y*+*pwd*) and *H*(*g*^*pwd*, *g*^*y*||*Identity*) to the UE.

14. The AM-FE sends the EAP Request/AKA-Challenge message to the AR-FE, and it forwards the message to the UE.

15. The UE retrieves a value *g*^*y* by computing *g*^(*y*+*pwd*)/*g*^*pwd* and verifies the received hash value *H*(*g*^*pwd*, *g*^*y*||*Identity*). If it is successful, the UE generates the DH session key *g*^(*xy*). The UE performs AKA algorithm to generate an AV using the DH session key instead of a long-term key. The UE verifies the received AUTN to authenticate the network. The UE derives new keying material from the new IK and CK, and then verifies the received MAC using the new derived keys. If the UE receives a protected pseudonym and(or) re-authentication identity, it stores the received identity for future authentication.

16. The UE computes a new MAC value with the new derived keys, and then sends the EAP Response/AKA-Challenge, including the computed RES and the new MAC to the AR-FE. The UE may send a result indication to the TAA-FE if it received the result indication from the TAA-FE. It also depends on the home operator's policies. The AR-FE forwards the message to the AM-FE.

17. The AM-FE sends the EAP Response/AKA-Challenge message to the TAA-FE server.

18. The TAA-FE verifies the received MAC, and then compares the XRES with the received RES.

19. If all validation is successful, the TAA-FE sends the EAP Request/AKA-Notification that notifies the success of authentication to the UE. This notification can be protected by using a MAC.

20. The AM-FE sends the EAP message to the AR-FE, and it forwards the EAP message to the UE.
21. The UE sends the EAP Response/AKA-Notification to the AM-FE through the AR-FE.
22. The AM-FE sends the EAP Response/AKA-Notification to the TAA-FE.
23. The TAA-FE sends the EAP Success with keying material for providing message confidentiality and/or integrity in the WiMax or WLAN to the AM-FE.
24. The AM-FE sends the EAP Success to the AR-FE. The AR-FE stores the keying material. In future, the keying material is used to communicate with the UE.
25. The AR-FE informs the UE that its authentication and key distribution have been successful and complete.
26. The user channel is established between the UE and AN. The UE can access the network such as the 3GPP, WiMax, and WLAN.

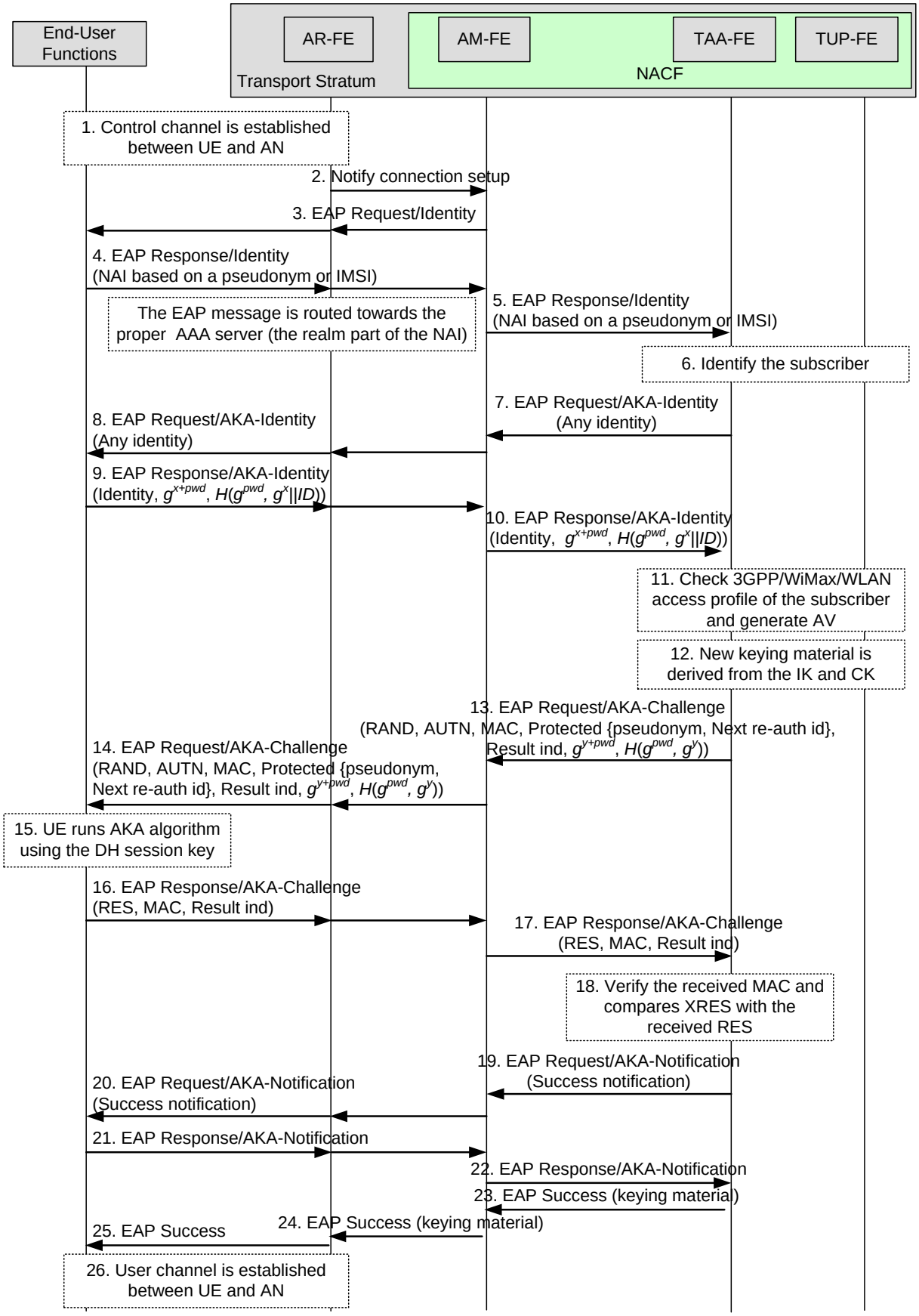

Figure I.2 – Authentication protocol based on EAP-AKA scheme with non-UICC in NGN

I.3 Example of fast re-authentication procedure

The fast re-authentication mechanism for interworking between the 3GPP and WLAN terminals is described in [ETSI TS 133 234]. This clause shows that this mechanism is also used in the EAP-AKA based on non-UICC. Since the fast re-authentication procedure is performed by reusing keys generated from previous authentication process, the fast re-authentication procedure of the two EAP-AKA protocols is the same. The complete operation is defined in [b-IETF RFC 4187]. This clause shows how the procedure could work in NGN.

Operational steps of the EAP-AKA fast re-authentication:

1. The AM-FE sends an EAP Request/Identity message to the UE.
2. The UE responds with an EAP Response/Identity message including re-auth. id that is previously obtained from the TAA-FE during a full EAP-AKA authentication procedure.
3. The AM-FE sends an EAP Response/Identity message to the TAA-FE.

NOTE – This Recommendation omits AAA communication between the AM-FE and TAA-FE to simply description.

4. Upon receiving the message, the TAA-FE sends EAP Request/AKA-Re-authentication message to the AM-FE. This message contains the Counter, the Nonce, the MAC, the protected re-authentication id for the next fast re-authentication procedure, and the Result indication to protect the success result message at the end of the process. If the TAA-FE cannot deliver a re-auth. id, the UE shall force a full EAP-AKA authentication procedure. The protection of the result message depends on the network operator's policies.
5. The AM-FE forwards EAP Request/AKA-Re-authentication message to the UE.
6. The UE checks that the Counter is fresh and the MAC value is correct, and then sends the EAP Response/AKA-Re-authentication message to the AM-FE. This message contains the same Counter value and a calculated MAC. If the UE receives the same result indication from the TAA-FE, it shall include the result indication in this message. Otherwise, the UE shall ignore this indication.
7. The AM-FE sends the EAP Response/AKA-Re-authentication message to the TAA-FE.
8. If the TAA-FE requested to use protected Result Indications in the previous steps, the TAA-FE verifies whether or not the received Counter value is the same value as it was sent before, and the MAC is correct. And then, it sends the EAP Request/AKA-Notification message to AM-FE. This message contains the protected MAC and an encrypted copy of the Counter.
9. The AM-FE forwards the EAP Request/AKA-Notification message to the UE.
10. The UE sends the EAP Response/AKA-Notification message to the AM-FE.
11. The AM-FE forwards the EAP Response/AKA-Notification message to the TAA-FE.
12. The TAA-FE sends an EAP Success message to the UE. If some additional keying materials were generated for protecting signalling and user data in access link, then the TAA-FE delivers the keying material embedded in the RADIUS or Diameter messages to the AR-FE. The AR-FE stores the keying material to be used in communication with the authenticated UE.
13. The AR-FE forwards the EAP Success message to the UE except the keying material.

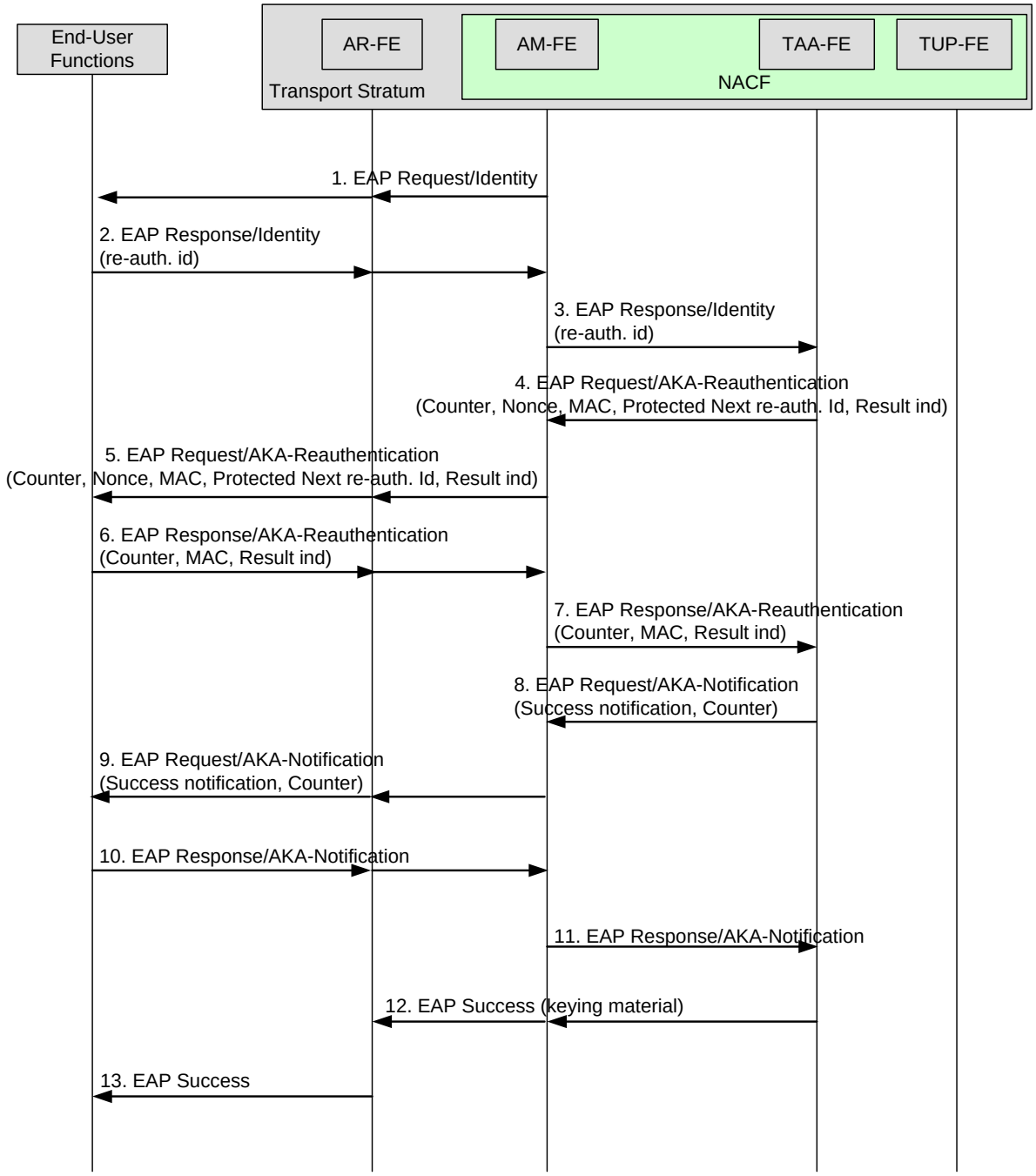

Figure I.3 – Fast re-authentication procedure of the EAP-AKA protocol in NGN

Bibliography

[b-IEEE 802.11] IEEE 802.11-2007, *IEEE Standard for information technology – Telecommunications and information exchange between systems – local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) Specifications*.

[b-IEEE 802.16e] IEEE 802.16e-2005 and 802.16/Cor1 Part 16: *Amendment for Physical and Medium Access Control layers for combined Fixed and Mobile Operation*.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

[b-IETF RFC 3579] IETF RFC 3579 (2003), *RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.

[b-IETF RFC 4072] IETF RFC 4072 (2005), *Diameter Extensible Authentication Protocol (EAP) Application*.

[b-IETF RFC 4187] IETF RFC 4187 (2006), *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009