3GPP TSG SA WG3 Security — S3#23 **S3-020354**
9 - 12 July 2002
Helsinki, Finland

3GPP TSG-SA WG2 meeting #25 **Tdoc S2-022022**
Naantali, Finland, 24th – 28th June 2002

Title: Liaison statement on 3GPP System to WLAN Inter working

Source: **SA2**

To: **SA3**

Cc: **-**

Response to: **None**

Contact Person:

Name: Farooq Bari
E-mail Address: Farooq.bari@attws.com

Attachments: TR 23.934 V 0.3.0

SA2 is currently working on 3GPP System to WLAN Inter working architecture (TR 23.934) and is sending the current version of this TR for SA3 review.

Action:
SA2 requests SA3 to review and comment on the security aspects as described in current version of the TR.

Date of Next SA WG 2 Meetings:

Title	Date	Location
SA2 #26	August 19 -23, 2002	Toronto, Canada

Technical Report

3GPP TR 23.934 V0.3.0 (2002-06)

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3GPP system to Wireless Local Area Network (WLAN) Interworking;
Functional and architectural definition
(Release 6)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Remove GSM logo from the cover page for pure 3rd Generation documents.

Select keywords from list provided in specs database.

Keywords

<keyword[, keyword]>

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Copyright Notification

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

1 Scope

Editor's note : Identify and analyse possible system architectures for allowing WLAN based radio networks to Interwork with 3GPP based systems.

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*.

3 Definitions, symbols and abbreviations

3.1 Definitions

3.2 Symbols

3.3 Abbreviations

4 WLAN Radio networks

Editor's notes : Provides a high-level description of WLAN technologies/standards.

4.1 WLAN Radio Technologies

There are many competing technologies that fit under the WLAN umbrella. This section attempts to describe the various attributes of the most popular of WLAN technologies, namely IEEE 802.11, Bluetooth, and HiperLan/2. Table 1 includes an indicative technology comparison.

Attribute	**802.11b**	**Bluetooth**	**802.11a**	**HiperLan/2**
Frequency	2.4 GHz	2.4 GHz	5 GHz	5 GHz
Physical Layer	Direct Sequence Spread Spectrum (DSSS)	Frequency Hopping Spread Spectrum (FHSS)	Orthogonal Frequency Division Multiplexing (OFDM)	OFDM
Channel Width	22 MHz	1MHz	22 MHz	22 MHz
Range	150 ft (indoors) 300 ft (outdoors)	30 ft (with 1mW)	100 ft (indoors) 200 ft(outdoors)	Expected to be same as 802.11a
Data Throughputs	1,2,6,11 Mbps	720 Kbps	6,9,12,18,36,54 Mbps (speed varies as distance from Access Point)	Same as 802.11a
MAC	CSMA/CA in Distributed Coordinated Function Mode (DCF) (optional) Polling Based in Point Coordination Function (PCF)	Time Division Duplex (TDD) with a Master/Slave Polling Mechanism	Same as 802.11b	TDMA with TDD
Miscellaneous	o High Speed Data Applications o Susceptible to interference from Bluetooth and other devices	o Wire Replacement; o Inexpensive o Low component count o Low Power	o Improve Spectral Efficiency over 802.11b	o Products not available yet

Table 1 WLAN Technology Comparison

4.2 WLAN Reference Model

For us to define the Interworking between WLAN and 3GPP systems, we should have network reference models for both WLAN and 3GPP networks. In 3GPP, we do have a network reference model for 3GPP. Unfortunately, there is no such network reference model available for WLAN networks. IEEE defined the physical, MAC and LLC layers in the 802.11 standards but not the network architecture. IETF has defined the layer 3 and above protocols, but not the network architecture. Each WLAN network is different, depending upon the operator's requirements and the environment where it is being used. However, to define the interworking, we must have a reference model we can work with.

The following is a reference model, which attempts to abstract the currently deployed WLAN networks. It shows only those elements of the WLAN network, which are relevant for the interworking with 3GPP. The reference model is shown in Figure 4.1.

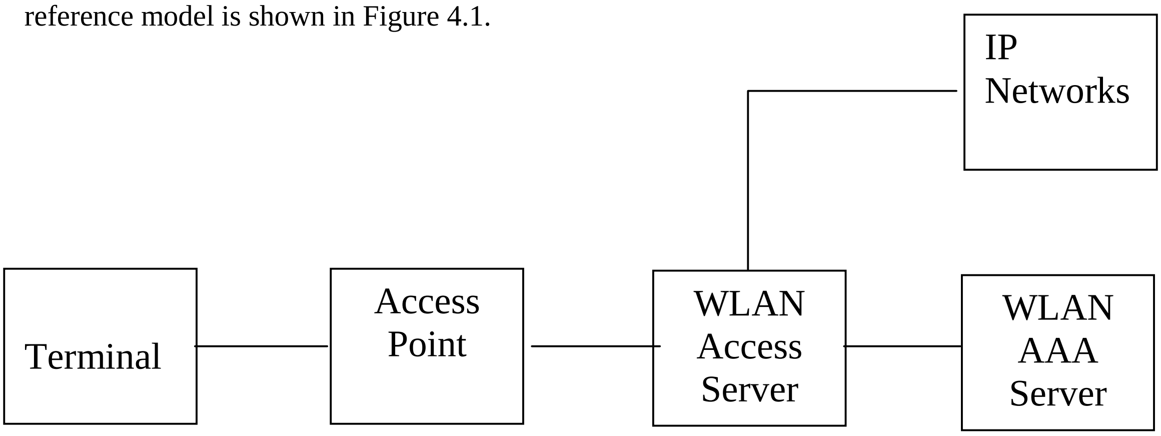


Figure 4.1: WLAN Network Reference Model

Terminal

This is the user equipment with a standard WLAN card, off the shelf, commercially available from multiple vendors. It could be, for example: a tabletop computer, a lap top computer or a hand held device.

Access Point

The Access Point is the WLAN equivalent of a Base Station as defined by IEEE or Hyperlan (or other WLAN) standards. Access Point is off the shelf, commercially available from multiple vendors.

WLAN Access Server

The WLAN Access Server provides the connectivity for the terminal with the rest of the network. It uses the services of the WLAN AAA server to authenticate the user. It uses the services of a DHCP server to assign an IP Address to the terminal. Based upon the results of Authentication, it may allow the user to access the network, access some limited local services or deny the access.

Though, the term WLAN Access Server is not a well-defined standard term in the industry, it's functionalities are based upon well defined open standards.

WLAN AAA Server

This is the Authorization, Authentication and Accounting server based upon well defined industry standards, widely used and available from multiple vendors. This term needs no further explanation.

5 High-level requirements

Editor's note : Provides the high-level functional requirements for the Interworking between WLAN and 3GPP system

5.1 Authentication Requirements

- Legacy WLAN terminals should be supported.
- Minimal impact on the user equipment, i.e. client software.
- The need for operators to administer and maintain end user SW should be minimized
- Existing UICC cards should be supported. The solution as such should not require any new changes to the UICC cards.
- Changes in the HSS/HLR/AuC should be minimized.
- The security data, i.e. long-term keys, which are stored on the UICCcard must not be sent from the card itself. Instead the interface to the UICC card should be of type challenge-response, i.e. a challenge is sent to the UICC card and a response is received in return.
- The user should have same security level for WLAN access as for 3GPP access.
- Mutual Authentication should be supported
- The selected Authentication solution should also allow for Authorisation
- Methods for key distribution to the WLAN access NW shall be supported
- Selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as 3GPP System authentication procedure
- Subsequent WLAN re-authentication shall not compromise the requirement for 3GPP System equivalent security
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks. In other words, a man in the middle shall not be able to learn the session key material.
- The WLAN technology specific connection between the WLAN UE and WLAN AN shall be able to utilise the generated keying material for protecting the integrity of an authenticated connection

- It shall be possible to store all long-term security credentials used for subscriber and network authentication in a tamper proof memory such as the UICC card.

5.2 Charging requirements

- The W-LAN access network shall be able to report the W-LAN access usage to the appropriate 3GPP system
- It shall be possible for the 3GPP system to command some operations on a specific ongoing W-LAN access session. This can be useful in the context of prepaid processing.
- It shall be possible for an operator to maintain a single prepaid account for W-LAN, PS, CS, and IMS per user.
- It shall be the role of the 3GPP system to process the W-LAN access resource usage information into 3GPP compatible format (CDR).

6 Architecture alternatives

Editor’s note : This chapter Identifies potential architectural alternatives for realising Interworking between WLAN and 3GPP systems. Each alternative should be treated in a specific chapter (alternative x handled in section 7.x)

For each alternative it

- Provides an architecture definition
- Describes the purpose (functionalities),
- Assesses its limitations
- Assesses possible impacts on 3GPP specifications and on non-3GPP standards/specifications.

An architecture alternative may take in several potential solutions for realising a particular functionality e.g. authentication.

6.1 Access Control and Charging Architecture

6.1.1 Reference Model

Editor's note : The term roaming is used here when referring to roaming between 3GPP networks. However, an intermediate aggregator or a chain of intermediate networks may possibly separate the user when accessing the WLAN from the 3GPP home network.

6.1.1.1 Non Roaming WLAN Inter-working Reference Model

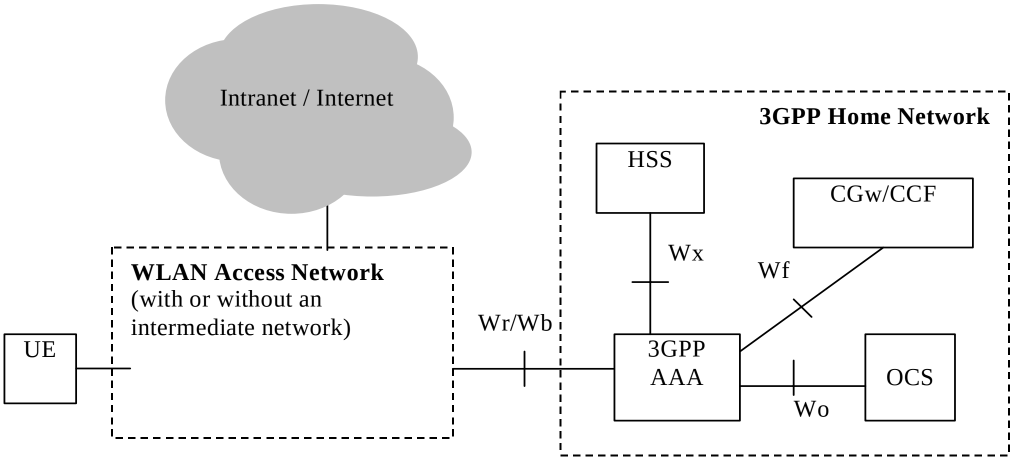


figure 6.1 Non Roaming Reference Model.

6.1.1.2 Roaming WLAN Inter-working Reference Model

6.1.1.2.1 Alternative 1

In this case, The visited network is responsible for access control and generating charging records. The Wx and Wo interfaces are inter-operator. The 3GPP network interfaces to other 3GPP networks via the Wx and Wo interfaces, and to non 3GPP networks via the Wr and Wb interfaces.

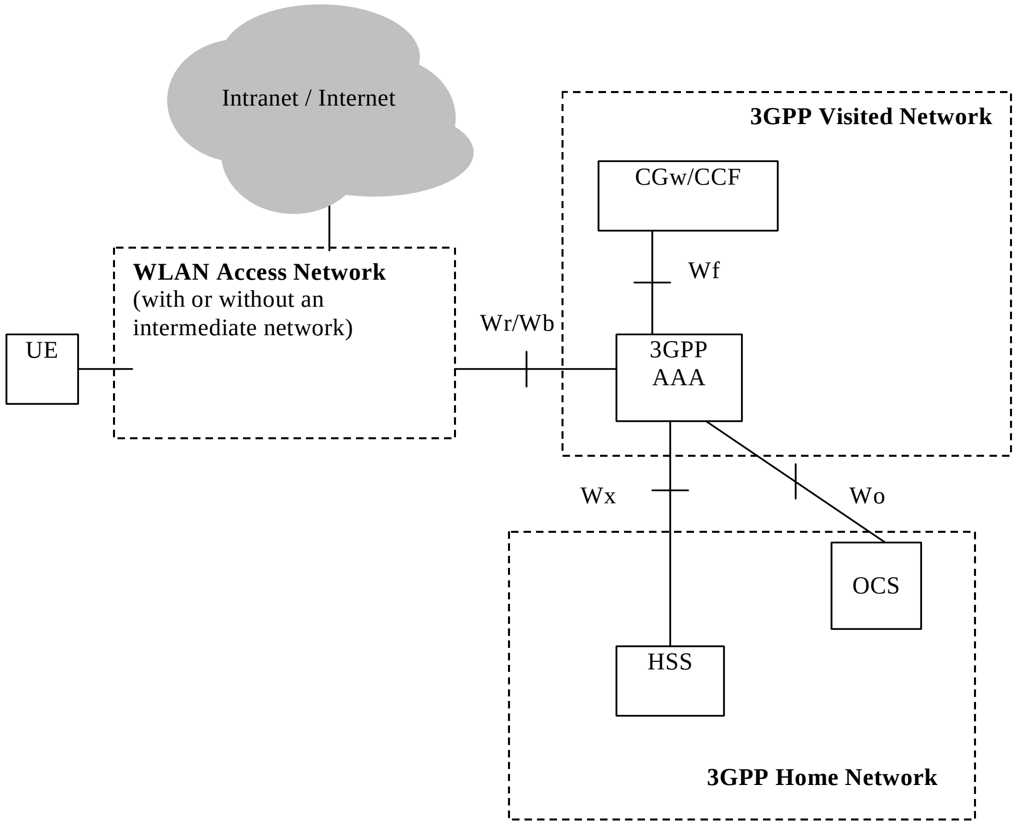


Figure 6.2 Roaming Reference Model.(Alternative 1)

6.1.1.2.2 Alternative 2

In this case, The home network is responsible for access control. Charging records can be generated in the visited and/or the home 3GPP networks.   The Wx and Wo interfaces are intra-operator. The 3GPP network interfaces to other 3GPP networks, WLANs, and intermediate networks via the Wr and Wb interfaces.

The 3GPP proxy AAA relays access control signalling and accounting information to the home 3GPP AAA server.

It can also issue charging records to the visited network CGw/CCF when required.

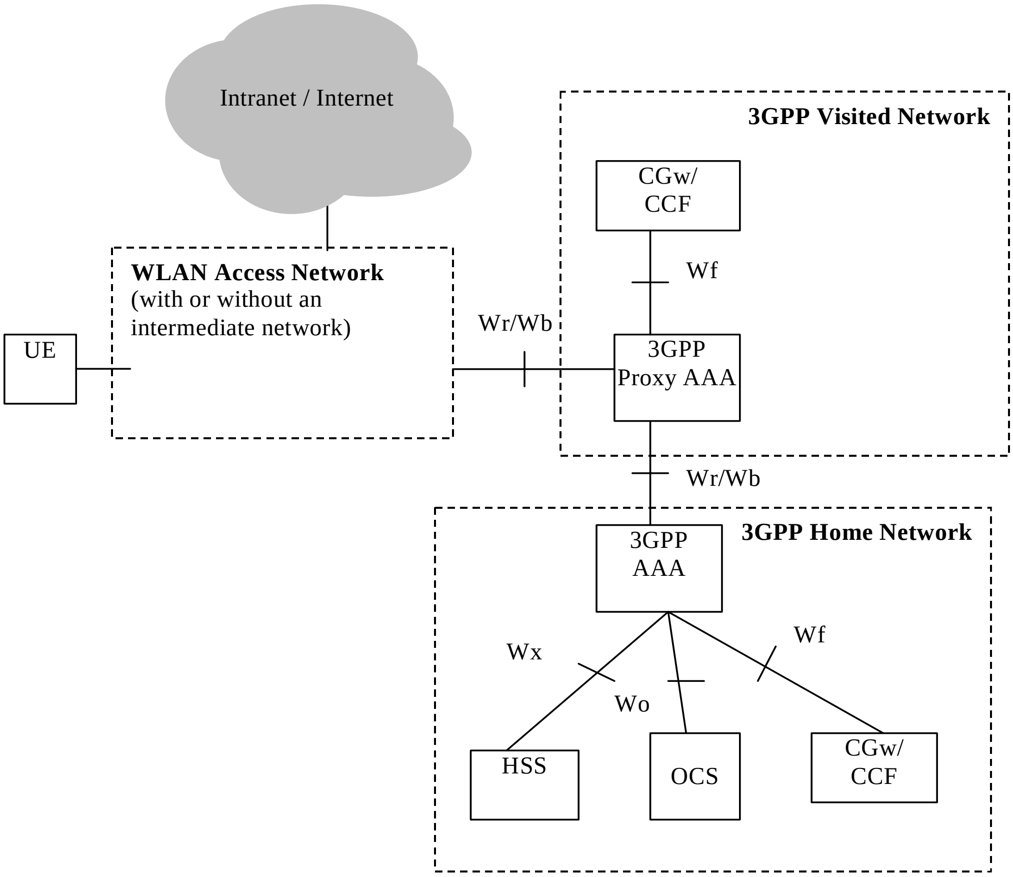


Figure 6.3 Roaming Reference Model.(Alternative 2)

6.1.1.3 Network elements

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

- the UE (potentially equipped with UICC card) utilised by a 3GPP subscriber to access the WLAN interworking service. The UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP System access. Some UE may be capable of simultaneous access to both WLAN and 3GPP systems. The UE may include terminal types whose configuration (e.g. interface to a UICC), operation and software environment are not under the exclusive control of the 3GPP system operator. As an example, a UE may be a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications.

- the AAA proxy represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server. These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.

The number of intermediate AAA proxies is not restricted by 3GPP specifications. The AAA proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA server or any other physical network node.

Note : the AAA proxy that resides in the 3GPP network is called a 3GPP AAA proxy.

- the 3GPP AAA server is located within the 3GPP network. The 3GPP AAA server :

  o retrieves authentication information and subscriber profile (including subscriber's authorisation information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network;

  o authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies.

  o communicates authorisation information to the WLAN potentially via AAA proxies.

  o registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorised 3GPP subscriber.

  o may act also as a AAA proxy (see above).

- the HLR/HSS located within the 3GPP subscriber's home network is the entity containing authentication and subscription data required for the 3GPP subscriber to access the WLAN interworking service.

6.1.2 Access Control

6.1.2.1 Principles

End to End Authentication : WLAN Authentication signalling is executed between WLAN UE and 3GPP AAA Server. This authentication signalling shall be independent on the WLAN technology utilised within WLAN Access network.. WLAN authentication signalling for 3GPP-WLAN interworking shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 2284.

Transporting Authentication signalling over WLAN Radio Interface : WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. These WLAN technology specific protocols shall be able to meet the security requirements set for WLAN Access control in 3GPP-WLAN interworking. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology. For IEEE 802.11 type of WLAN radio interfaces the WLAN radio interface shall conform to IEEE 802.11i standard.

Transporting Authentication signalling over Wr Reference Point : WLAN Authentication signalling shall be transported over *Wr* reference point by standard mechanisms, which are independent on the specific WLAN technology utilised within the WLAN Access network. The transport of Authentication signalling over Wr reference point shall be based on standard Diameter or RADIUS protocols.

6.1.2.2 Reference Points

6.1.2.2.1 Wr

The reference point Wr connects the WLAN access network, possibly via intermediate networks, to the 3GPP AAA Server. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and related information in a secure manner. The reference point has to accommodate also legacy WLAN access networks and thus should be DIAMETER or RADIUS-based.

The functionality of the reference point is to transport RADIUS/DIAMETER frames:

- Carrying data for authentication signalling between WLAN UE and 3GPP AAA Server
- Carrying data for authorization signalling between WLAN AN and 3GPP AAA server
- Carrying keying data for the purpose of radio interface integrity protection and encryption
- Used for purging a user from the WLAN access for immediate service termination

6.1.2.2.2 Wx

This reference point is located between 3GPP AAA Server and HSS/HLR. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HSS/HLR. The protocol crossing this reference point is either MAP or DIAMETER-based.

The functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HSS/HLR.
- Retrieval of WLAN access-related subscriber information (profile) from HSS/HLR
- Registration of the 3GPP AAA Server of an authorised WLAN user in the HSS/HLR.
- Indication of change of subscriber profile within HSS/HLR (e.g indication for the purpose of service termination).

6.1.3 Charging

6.1.3.1 Reference Points

6.1.3.1.1 Wb

The reference point Wb is located between WLAN access network and 3GPP network. The prime purpose of the protocols crossing this reference point is to transport charging-related information in a secure manner. The reference point has to accommodate also legacy WLAN access networks and thus should be DIAMETER or RADIUS-based.

The functionality of the reference point is to transport RADIUS/DIAMETER frames with:

- Charging signalling per each WLAN user

To minimize the requirements put on the WLAN Access Network and to protect the confidentiality of the subscribers charging status the fact whether a user is offline or online charged by his 3GPP subscription provider shall be transparent for the WLAN AN and thus for the Wb reference point. However for online charged users the interval to deliver accounting information from WLAN AN over Wb reference point may typically be set to a smaller value than for offline charged users.

6.1.3.1.2 Wo

Reference point Wo is used by a 3GPP AAA server to communicate with 3GPP Online Charging System (OCS). The prime purpose of the protocol(s) crossing this reference point is to transport online charging related information so as to perform credit control for the prepaid subscriber.

The protocol(s) crossing this interface shall be DIAMETER-based.

The functionality of the reference point is to transport:

- Online charging data

Wo reference point should be similar to Ro interface currently used in 3GPP OCS.

6.1.3.1.3 Wf

The reference point Wf is located between 3GPP AAA Server and 3GPP Charging Gateway Function (CGF)/Charging Collection Function (CCF). The prime purpose of the protocols crossing this reference point is to transport/forward charging information towards 3GPP operator’s Charging Gateway/Charging collection function.

The information forwarded to Charging Gateway/Charging collection function is typically used for:

- Generating bills for offline charged subscribers by the subscribers’ home operator
- Calculation of inter-operator clearing charging from all roaming users. This inter operator clearing is used to settle the payments between visited and home network operator and/or between home/visited network and WLAN.

The protocol(s) crossing this interface is DIAMETER-based.

The functionality of the reference point is to transport:

- WLAN access-related charging data per each WLAN user

7 Procedures

7.1 Authentication methods

Editor’s note : the purpose of this section is to list a certain number of proposals with regards to authentication methods and to provide the corresponding identified message flows. It is understood that this will need review of SA3.

7.1.1 USIM based AuthenticationUSIM based authentication is a proven solution that satisfies the authentication requirements from section 5.1. However, requiring USIM based authentication does not automatically mean that the USIM needs to be included in the WLAN card, for example the WLAN device can be linked with a UE supporting a USIM via, for example Bluetooth, Irda, USB or serial cable.

7.1.1.1 EAP/AKA Procedure

USIM based authentication may be based on existing AKA method. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP. EAP/AKA authentication mechanism is described in Internet Draft draft-arkko-pppext-eap-aka. The current version is 03 (draft-arkko-pppext-eap-aka-03.txt). The following procedure is based on EAP/AKA authentication mechanism:

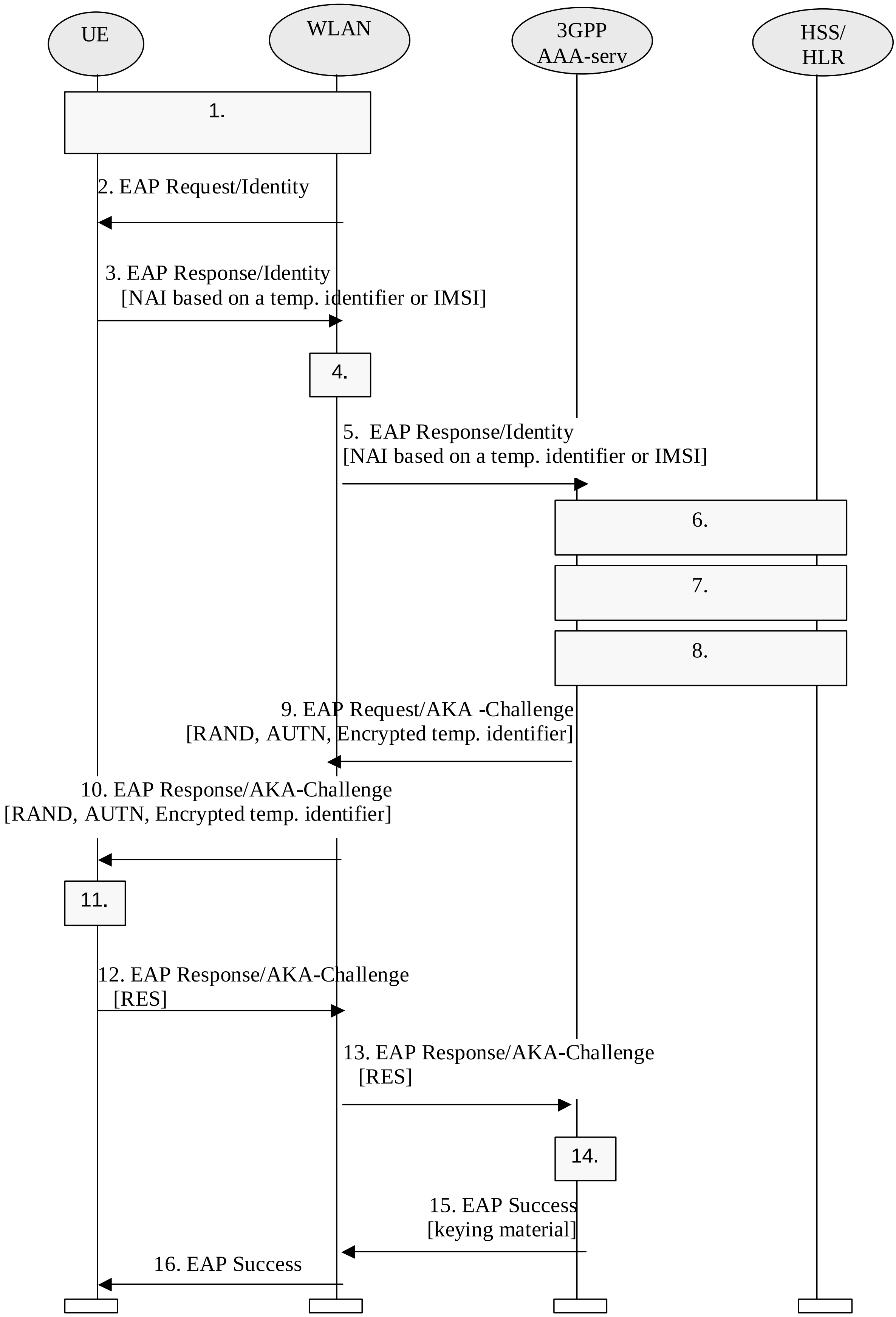

UE
WLAN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
4.
5. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
6.
7.
8.
9. EAP Request/AKA -Challenge [RAND, AUTN, Encrypted temp. identifier]
10. EAP Response/AKA-Challenge [RAND, AUTN, Encrypted temp. identifier]
11.
12. EAP Response/AKA-Challenge [RES]
13. EAP Response/AKA-Challenge [RES]
14.
15. EAP Success [keying material]
16. EAP Success

Figure 7.1 Authentication based on EAP AKA scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a Wireless LAN technology specific procedure (out of scope for 3GPP).

2. The WLAN sends an EAP Request/Identity to the UE.

EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The UE starts EAP AKA authentication procedure by sending an EAP Response/Identity message. The UE sends its identity complying to Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a temporary identifier (pseudonym) allocated to UE in previous authentication or, in the case of first authentication, the IMSI.

Note : generating an identity conforming to NAI format from IMSI is defined in EAP/AKA draft (draft-arkko-pppext-eap-aka-03.txt).

4. The 3GPP AAA Server is chosen based on the NAI.

Note : diameter/radius proxy chaining and/or diameter referral can be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity.

6. 3GPP AAA Server checks that it has an authentication vector available (RAND, AUTN, XRES, IK, CK) for the subscriber from previous authentication. If not, a set of authentication quintuplets is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

7. 3GPP AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS/HLR. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.

Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14. (This will be specified as part of the Wx interface.)

8. New keying material is derived from IK and CK. The extra keying material is required in order to pass the encrypted and integrity protected temporary identifier to the UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.

A new pseudonym is chosen and encrypted.

9. 3GPP AAA Server sends RAND, AUTN, and encrypted temporary identifier to WLAN in EAP Request/AKA-Challenge message.

10. The WLAN sends the EAP Request/AKA-Challenge message to the UE

11. UE runs UMTS algorithm on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure (not shown in this example). If AUTN is correct, the USIM computes RES, IK and CK.

UE derives required additional keying material from IK and CK. UE decrypts pseudonym and saves it to be used on next authentication.

12. UE sends EAP Response/AKA-Challenge containing calculated RES to WLAN

13. WLAN sends the EAP Response/AKA-Challenge packet to 3GPP AAA Server

14. 3GPP AAA Server compares XRES and the received RES.

15. If the comparison in step 14 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated UE.

16. WLAN informs the UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the UE and the WLAN share session key material.

Note 1: The 3GPP AAA Server that is referred to in this diagram is the one that actually realises the authentication. If AAA Proxies are used between the WLAN Access Network and the AAA Server, they are not referred to in this diagram.

Note 2: Temporary identifier generation and storage is FFS.

7.1.2 GSM SIM based authentication

GSM SIM based authentication is useful for GSM subscribers that do not have a UICC card with a USIM application. SIM based authentication, with enhancements for network authentication, satisfies the authentication requirements from section 5.1.

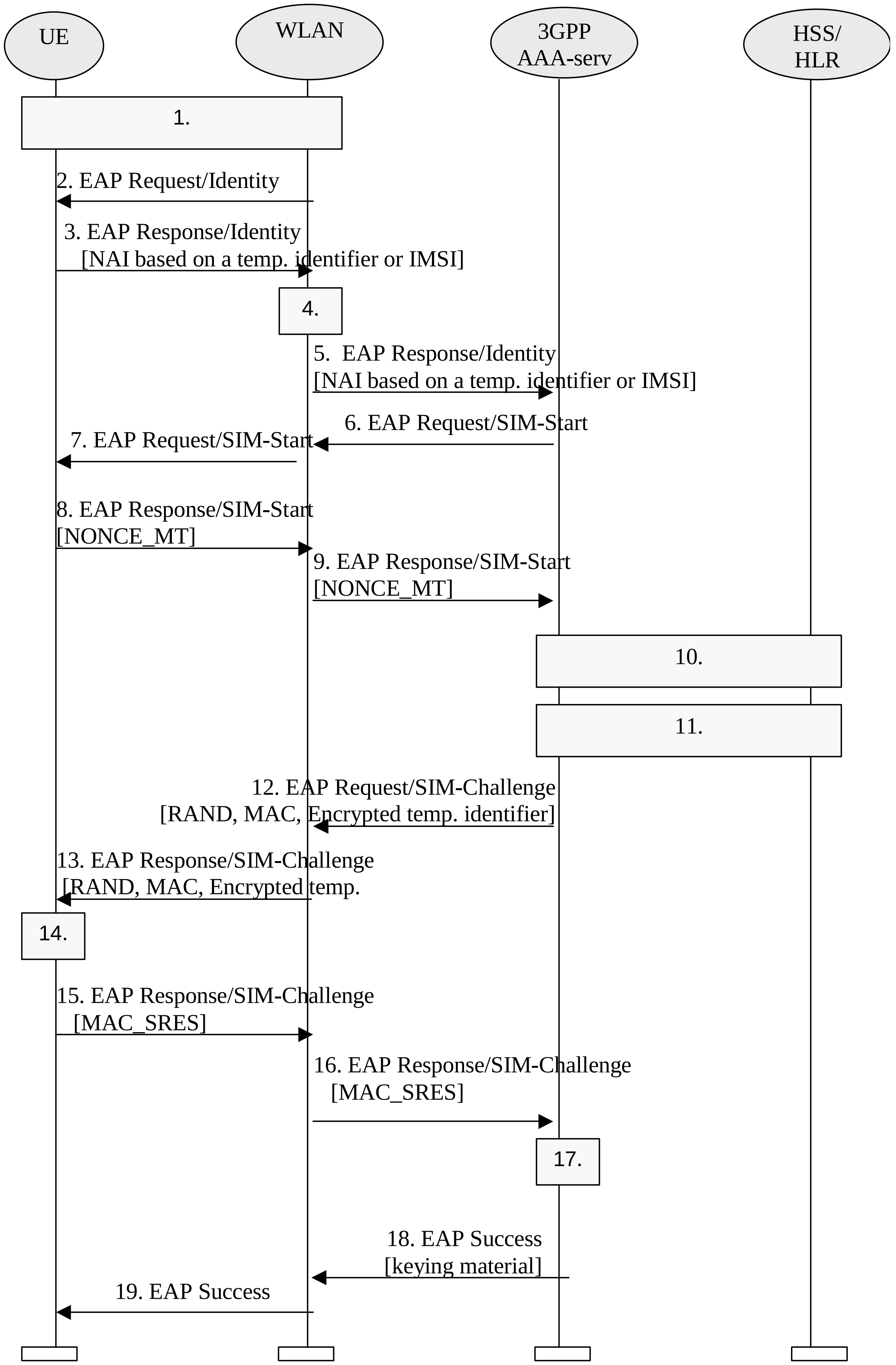
However, requiring SIM based authentication does not automatically mean that the SIM needs to be included in the WLAN card, for example the WLAN device can be linked with a UE supporting a SIM via, for example Bluetooth, Irda, USB or serial cable.

7.1.2.1 EAP SIM procedure

SIM based authentication shall be based on existing GSM AKA method but shall include enhancements for network authentication. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP.

EAP SIM authentication mechanism is described in Internet Draft draft-haverinen-pppext-eapsim. The current version is 04 (draft-haverinen-pppext-eap-sim-04.txt).

The following procedure is based on EAP SIM authentication mechanism:


UE
WLAN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
4.
5. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
6. EAP Request/SIM-Start
7. EAP Request/SIM-Start
8. EAP Response/SIM-Start [NONCE_MT]
9. EAP Response/SIM-Start [NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Encrypted temp. identifier]
13. EAP Response/SIM-Challenge [RAND, MAC, Encrypted temp.
14.
15. EAP Response/SIM-Challenge [MAC_SRES]
16. EAP Response/SIM-Challenge [MAC_SRES]
17.
18. EAP Success [keying material]
19. EAP Success

7.2 Authentication based on EAP SIM scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a Wireless LAN technology specific procedure (out of scope for 3GPP).

2. The WLAN sends an EAP Request/Identity to the UE.

EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The UE starts EAP SIM authentication procedure by sending an EAP Response/Identity message. The UE sends its identity complying to Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a temporary identifier (pseudonym) allocated to UE in previous authentication or, in the case of first authentication, the IMSI.

Note : generating an identity conforming to NAI format from IMSI is defined in EAP/SIM (draft-haverinen-pppext-eap-sim-04.txt).

4. The 3GPP AAA Server is chosen based on the NAI.

Note : diameter/radius proxy chaining and/or diameter referral can be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity.

6. The 3GPP AAA Server guesses, based on the NAI, that the subscriber is a GSM user; hence it sends the EAP Request/SIM-Start packet to WLAN.

7. WLAN sends the EAP Request/SIM-Start packet to UE

8. The UE chooses a fresh random number NONCE_MT. The random number is used in network authentication.

The UE sends the EAP Response/SIM-Start packet, containing NONCE_MT, to WLAN

9. WLAN sends the EAP Response/SIM-Start packet to 3GPP AAA Server

10. 3GPP AAA Server checks that it has N (usually two or three) available authentication triplets (RAND, SRES, Kc) for the subscriber from previous authentication. Several triplets are required in order to generate longer session keys. If N triplets are not available, a set of authentication triplets is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

Although this step is presented after step 9 in this examples, it could be performed at some other point, for example after step 5, however before step 12. (This will be specified as part of the Wx interface.)

11. 3GPP AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS/HLR. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.

Although this step is presented after step 10 in this example, it could performed at some other point, however before step 18. (This will be the specified as part of the Wx interface.)

12. New keying material is derived from NONCE_MT and N Kc keys. The extra keying material is required in order to calculate a network authentication value and to pass the encrypted and integrity protected temporary identifier to the UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.

A message authentication code (MAC) is calculated over the RAND challenges using a newly derived key. This MAC is used as a network authentication value.

A new temporary identifier is chosen and encrypted.

3GPP AAA Server sends RAND, MAC, and encrypted temporary identifier to WLAN in EAP Request/SIM-Challenge message.

13. The WLAN sends the EAP Request/SIM-Challenge message to the UE

14. UE runs the GSM A3/A8 algorithms N times, once for each received RAND.

This computing gives N SRES and Kc values.

The UE derives additional keying material from N Kc keys and NONCE_MT.

The UE calculates its copy of the network authentication MAC and checks that it is equal with the received MAC. If the MAC is incorrect, the network authentication has failed and the UE cancels the authentication (not shown in this example). The UE continues the authentication exchange only if the MAC is correct.

UE decrypts pseudonym and saves it to be used on next authentication.

UE calculates a combined response value MAC_SRES from the N SRES responses.

15. UE sends EAP Response/SIM-Challenge containing calculated MAC_SRES to WLAN

16. WLAN sends the EAP Response/SIM-Challenge packet to 3GPP AAA Server

17. 3GPP AAA Server compares its copy of the MAC_SRES with the received MAC_SRES.

18. If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated UE.

19. WLAN informs the UE about the successful authentication with the EAP Success message. Now the EAP SIM exchange has been successfully completed, and the UE and the WLAN share session key material.

Note 1: The 3GPP AAA Server that is referred to in this diagram is the one that actually realises the authentication. If AAA Proxies are used between the WLAN Access Network and the AAA Server, they are not referred to in this diagram.

Note 2: Temporary identifier generation and storage is FFS.

Note 3 : the derivation of the value of N is for further study

8 Conclusion

Editor's note : Concludes on which architecture alternative(s) can be specified and how specific functionality can be realised.

ANNEX A : Refererence Points Signalling Flows

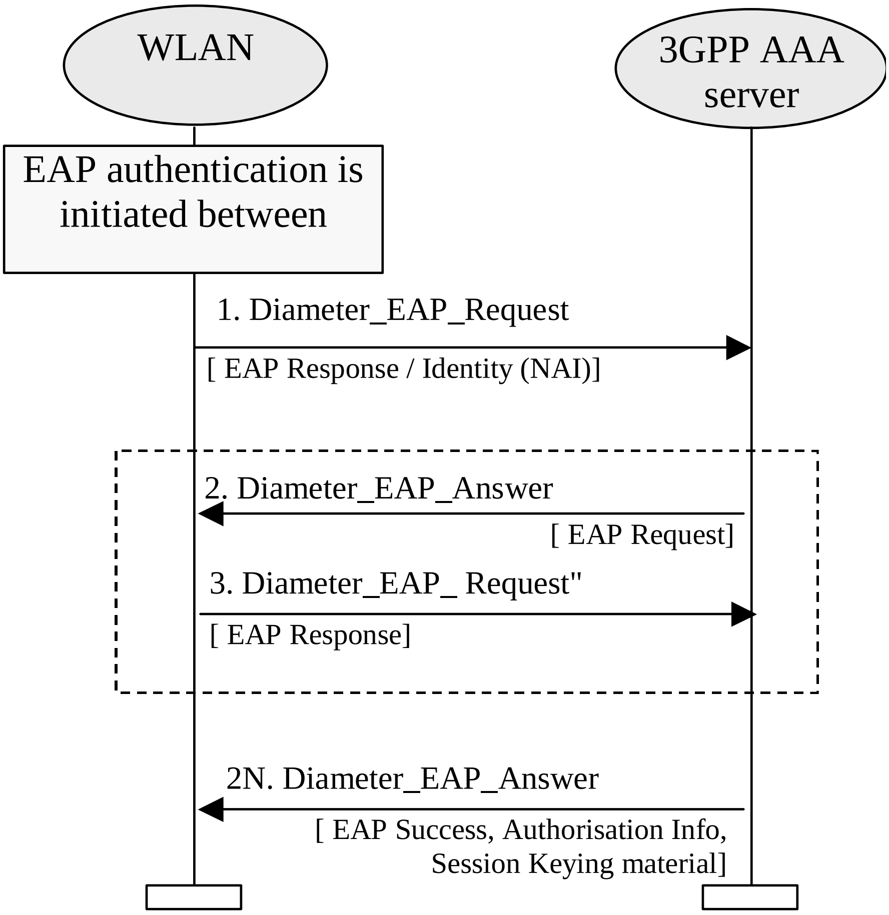
A.1 Signalling Sequences examples for Wr Reference Point

A.1.1 Authentication, Authorisation and Session Key delivery

The purpose of this signalling sequence is to carry UE - 3GPP AAA Server authentication signalling over the Wr reference point. As a result of a successful authentication, authorisation information and session keying material for the autenticated session is delivered from the 3GPP AAA Server to the WLAN.

This Wr signalling sequence is initiated by the WLAN when authentication of a UE is needed. This can take place when a new UE accesses WLAN, when a UE switches between WLAN APs or when a periodic re-authentication is performed.

The signalling sequence shown is based on Diameter. For signalling to WLANs using RADIUS the conversion defined in Diameter specification shall be used.



1. The WLAN initiates authentication procedure towards 3GPP network by sending Diameter_EAP_Request message to 3GPP AAA Server. This Diameter message carries encapsulated EAP Response/Identity message to 3GPP AAA Server. Message also carries a Session-ID used to identify the session within the WLAN.

2. 3GPP AAA Server performs the authentication procedure based on information retrieved from HSS/HLR. 3GPP AAA Server sends message Diameter_EAP_Answer to WLAN. This message carries encapsulated EAP Request message. The content of the EAP Request message is dependent on the EAP type being used. WLAN conveys the EAP Request message to the UE.

3. UE responds to WLAN by a EAP Response message. WLAN encapsulates it into Diameter_EAP_Request message and sends it to 3GPP AAA Server. The contents of the EAP Response message is dependent on the EAP type being used.

The number of roundtrip Diameter signalling exchanges similar to the signal pair 2 and 3 is dependent e.g. on the EAP type being used.

2N. When 3GPP AAA server has successfully authenticated the 3GPP subscriber, the 3GPP AAA Server sends final Diameter_EAP_Answer message carrying encapsulated EAP Success message to WLAN. WLAN forwards the EAP Success message to the UE.

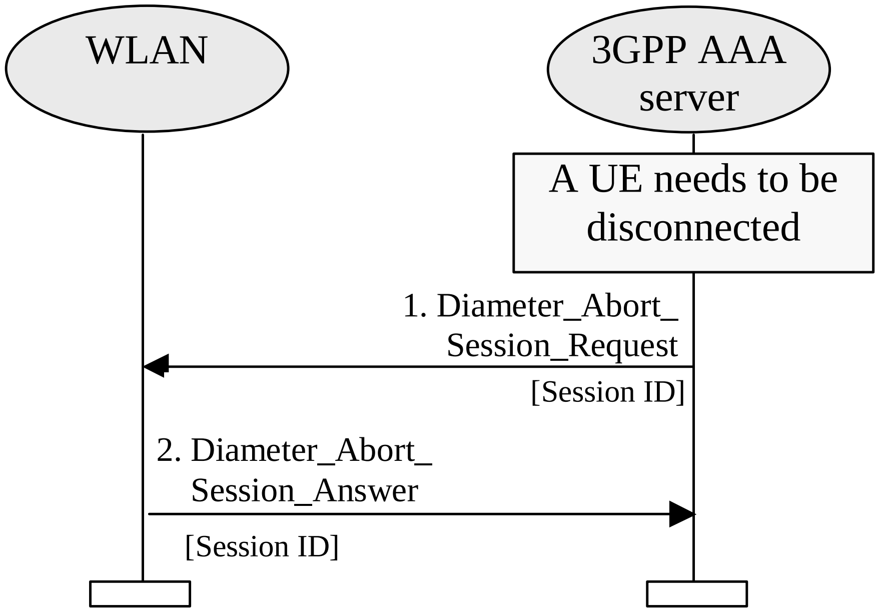
This Diameter_EAP_Answer message also carries the authorisation information (e.g. NAS Filter Rule or Tunneling attributes) for the authenticated session. Message also carries the keying material from 3GPP AAA Server to WLAN to be used for the authenticated session by WLAN.

A.1.2 Immediate purging of a user from the WLAN access

The purpose of this signalling sequence is to indicate to the WLAN that a specific UE shall be disconnected from accessing the WLAN interworking service.

This signalling sequence is initiated by the 3GPP AAA Server when a UE needs to be disconnected from accessing WLAN interworking service. For example, a UE used by a 3GPP subscriber may need to be disconnected when the 3GPP subscriber's subscription is canceled or when the 3GPP subscribers online charging account expires.

The signalling sequence shown is based on Diameter. For signalling to WLANs using RADIUS the conversion defined in Diameter specification shall be used.


WLAN
3GPP AAA server
A UE needs to be disconnected
1. Diameter_Abort_ Session_Request
[Session ID]
2. Diameter_Abort_ Session_Answer
[Session ID]

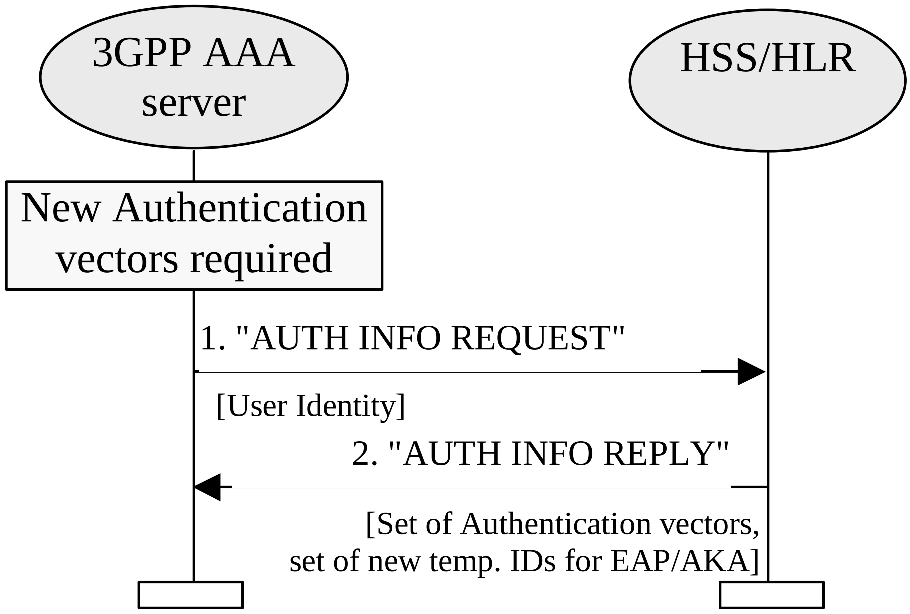
1. When 3GPP AAA Server needs to disconnect (e.g. after receiving an external trigger) a 3GPP subscriber from the WLAN access service, the 3GPP AAA Server sends a Diameter_Abort_Session_Request to WLAN . This message contains the Session ID by which the session is identified within WLAN.

2. WLAN responds by Diameter_Abort_Session_Answer as defined in Diameter.

A.2 Signalling Sequences examples for Wx Reference Point

A.2.1 Authentication Information Retrieval

This signalling sequence is initiated by a 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS/HLR.


3GPP AAA server
HSS/HLR
New Authentication vectors required
1. "AUTH INFO REQUEST"
[User Identity]
2. "AUTH INFO REPLY"
[Set of Authentication vectors, set of new temp. IDs for EAP/AKA]

1. 3GPP AAA server detects that it requires new authentication vectors for a given 3GPP subscriber. This can happen for example, when a new 3GPP subscriber has accessed 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server.

   3GPP AAA server sends "AUTH INFO REQUEST" message to the HSS/HLR requesting a set of authentication vectors. In the message the subscriber is identified by a unique identifier which is used as the username part of the NAI identity.

   In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the pseudonym (associated with the IMSI) allocated in a previous authentication or, in case of the very first authentication, the IMSI.

Note : For USIM authentication (EAP/AKA) it is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server, i.e. whether IMSI or Temporary identifier Is used as user identity over Wx.

2. HSS/HLR replies by a "AUTH INFO REPLY" message containing the requested authentication vectors.

   For USIM authentication (EAP/AKA) HSS/HLR has also allocated a new set of pseudonyms for the subscriber to be given to the subscriber in each subsequent authentication.

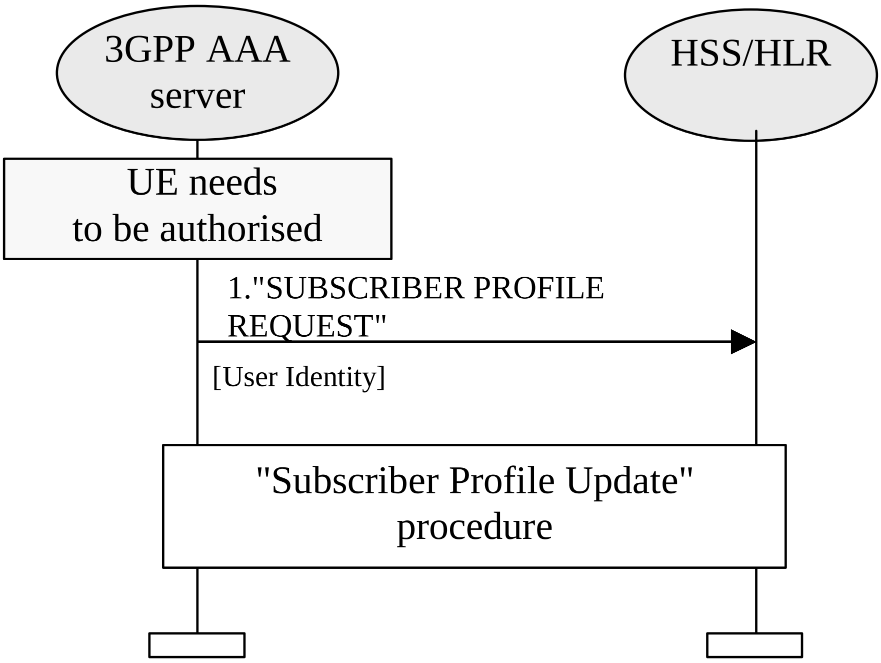
Note: It is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server

In case of UMTS AKA authentication, each authentication vector consists of RAND, XRES, AUTN, CK, and IK.

3GPP AAA Server stores the authentication vectors and pseudonyms to be used in future authentication procedures for the subscriber.

A.2.2 Subscriber Profile Retrieval

This signalling sequence is initiated by a 3GPP AAA Server when a new subscriber has accessed the 3GPP AAA server and the subscription profile information of that subscriber is not available in the 3GPP AAA server. This signalling sequence can also be used if for some reason the subscription profile of a subscriber is lost. Subscription profile contains e.g. authorisation information.


3GPP AAA server
HSS/HLR
UE needs to be authorised
1."SUBSCRIBER PROFILE REQUEST"
[User Identity]
"Subscriber Profile Update" procedure

1. 3GPP AAA server detects that it requires the subscription profile for a given 3GPP subcriber. For example. this can happen when a new subscriber has accessed the 3GPP AAA Server for authentication.

   3GPP AAA server sends "SUBSCRIBER PROFILE REQUEST" message to the HSS/HLR requesting the subscriber's profile to be downloaded to the 3GPP AAA server. In the message the subscriber is identified by a unique identifier which is used as the username part of the NAI identity.

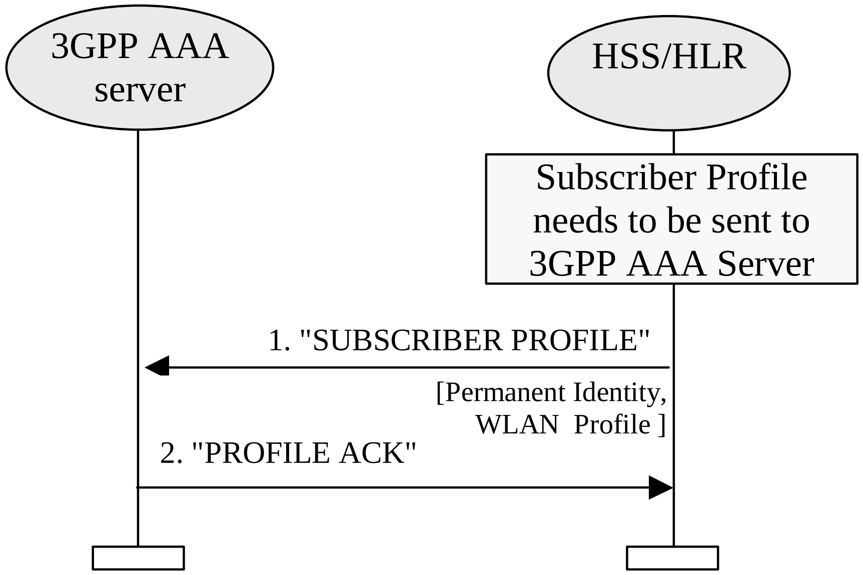
   In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the pseudonym (associated with the IMSI) allocated in the previous authentication or, in case of the very first authentication, the IMSI.

Note : it is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server, i.e. whether IMSI or Temporary identifier Is used as user identity over Wx.

2. At reception of "SUBSCRIBER PROFILE REQUEST" message, the HSS/HLR initiates a Subscriber Profile Update procedure towards the 3GPP AAA Server. The Subscriber Profile Update procedure is explained in the following subchapter.

A.2.3 Subscriber Profile Update

This signalling sequence is initiated by the HSS/HLR when subscriber profile needs to be sent to a 3GPP AAA server. This can be due to an explicit request from the 3GPP AAA Server or due to a modification or cancellation of subscription in the HSS/HLR.


3GPP AAA server
HSS/HLR
Subscriber Profile needs to be sent to 3GPP AAA Server
1. "SUBSCRIBER PROFILE"
[Permanent Identity, WLAN Profile]
2. "PROFILE ACK"

1. HSS/HLR initiates the signalling when a subscriber profile needs to be sent to a 3GPP AAA server. This can be due to an explicit request from the 3GPP AAA Server or due to a modification or cancellation of subscription in the HSS/HLR.

   HSS/HLR sends "SUBSCRIBER PROFILE" message to 3GPP AAA Server. For example. this message includes
   - Users permanent unique identifier. In case of USIM authentication (EAP/AKA) the utilised

     unique identifier shall be the IMSI,
   - service authorisation information,

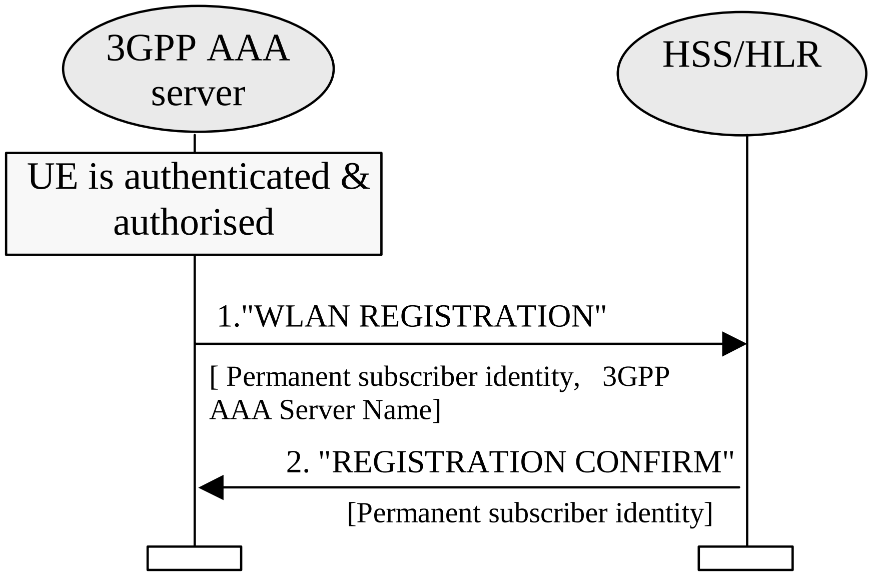
   - charging mechanism (offline / online),
   - in case of online charging. the DNS name of the subscribers online charging system

   3GPP AAA Server stores the subscriber profile information.

2. 3GPP AAA Server acknowledges the reception of the subscriber profile information by sending "PROFILE ACK" message to the HSS/HLR.

A.2.4 WLAN Registration

This signalling sequence is initiated by the 3GPP AAA Server when a new subscriber has been authenticated and authorised by the 3GPP AAA server. The purpose of this procedure is to register the current 3GPP AAA Server address in the HSS/HLR.


3GPP AAA server
HSS/HLR
UE is authenticated & authorised
1."WLAN REGISTRATION"
[Permanent subscriber identity, 3GPP AAA Server Name]
2. "REGISTRATION CONFIRM"
[Permanent subscriber identity]

1. 3GPP AAA server initiates the signalling when a new 3GPP subscriber has been authenticated and authorised by the 3GPP AAA server. 3GPP AAA server sends WLAN REGISTRATION message to the HSS/HLR. This message contains the address/name of the 3GPP AAA Server and the permanent subscriber identifier. In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the IMSI.

2. HSS/HLR confirms the reception of the WLAN REGISTRATION message by REGISTRATION CONFIRM message.

Annex B: Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
26.04.02	SA2#24				Upgraded to version 0.1.0 on the basis of the contributions S2-021446, S2-021447, S2-021449, S2-021450		V0.1.0
26.06.02	SA2#25				Upgraded to version 0.2.0 on the basis of S2-021793, 796, 798, 799, 800, 801, 802.	V0.1.0	V0.2.0
27.06.02	SA2#25				Upgraded to version 0.3.0 on the basis of S2-021933, 934, 970, 971, 972, 973.	V0.2.0	V0.3.0