3GPP TSG SA WG3 Security — S3#26 **S3-020596**
19- 22 November 2002
Oxford, UK

3GPP TSG-SA WG2 meeting #27 **Tdoc S2-023122**
Beijing, China, 14th – 18th October 2002

Title: **LS on: "3GPP System – WLAN Interworking"**
Source: **SA2**
To: **SA3**
Cc:
Response to:
Contact Person:

Name: **Nicolas MARTIQUET (Orange)**
Tel. Number: **+33.1.45.29.51.69**
E-mail Address: Nicolas.martiquet@rd.francetelecom.com

Attachments: TS 23.234 v1.1.0 (s2-022989)

---

1. Overall Description

SA2 advanced its study of 3GPP - WLAN Interworking. According to the new Work Item Description (sp-020542), scenarios 2 and 3 are now addressed in TS 23.234 (attached to this LS) and concern Release 6, whereas scenarios 4 and 5 are addressed in TR 23.934 and concern Release 7.

2. Security issues

During Beijing meeting, the SA2 WLAN group identified the following security issues:

- In TS 23.234 v1.1.0, SA2 removed all the security requirements, considering that they were already addressed in SA3 specifications. SA3 is required to ensure that these requirements are present in his specification;
- WLAN authentication necessitates the use of a temporary identifier, which needs to be stored somewhere in the terminal; however in pre-R6 implementations, it is not possible to store it within pre-R6 (U)SIMs. SA2 wonders if it raises security issues;
- How often (if ever) is it acceptable to send the IMSI in the clear ?
- How to keep the AAA Server stateless by e.g. including the IMSI encrypted within pseudonym ?
- SA3 is also asked to study the possibility of generating temporary identifiers by cryptographic derivation from the IMSI (the working assumption in SA2 is that temporary identifiers are allocated and stored in the AAA Server);
- Is it acceptable security-wise that the network can request the IMSI from the UE at any time?

2. Actions:

To SA3 group

ACTION:

SA2 asks SA3 group to continue updating us about progress in this area, and to provide answers to the issues addressed in section 2 of this Liaison.

3. Next SA2 Meeting:

Meeting	Date	Location	Host
SA2#28	**11-15 Nov 2002**	**Bangkok, THAILAND**	**Japanese Friends**

3GPP TS 23.234 V1.~~0~~1.0 (2002-~~09~~10)

Technical Specification

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

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

Contents

Foreword

This Technical Specification 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

This document specifies the 3GPP WLAN subsystem. The 3GPP WLAN subsystem is assumed to provide bearer services for connecting a 3GPP subscriber via WLAN to IP based services compatible with those offered via PS domain.

2 References

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

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

[1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] RFC2284: ” PPP Extensible Authentication Protocol (EAP)”

[4] RFC 2486: “The Network Access Identifier”

3 Definitions, symbols and abbreviations

3.1 Definitions

TBD.

3.2 Symbols

For the purposes of the present document the following symbols apply:

Wb	Interface between WLAN Access Network and 3GPP AAA
Wf	Interface between a CGw/CCF and 3GPP AAA
Wo	Interface between 3GPP AAA and OCS
Wr	Interface between WLAN Access Network and 3GPP AAA
Wx	Interface between HSS and 3GPP AAA

3.3 Abbreviations

CCF Charging Collection Function

CGw Charging Gateway

OCS Online Charging System

PDA Personal Digital Assistant

WLAN Wireless Local Area Network

4 WLAN Radio networks

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

4.1 WLAN Networks Interworking with 3GPP

Figure 4.1 illustrates WLAN networks from the point of view of 3GPP interworking. The Authentication, Authorization and Accounting (AAA) server is a Diameter or Radius server. The WLAN includes WLAN access points and may include other devices such as routers or intermediate AAA elements. The User Equipment (UE) includes all equipment that is in possession of the end user, such as a computer, WLAN radio interface adapter etc.

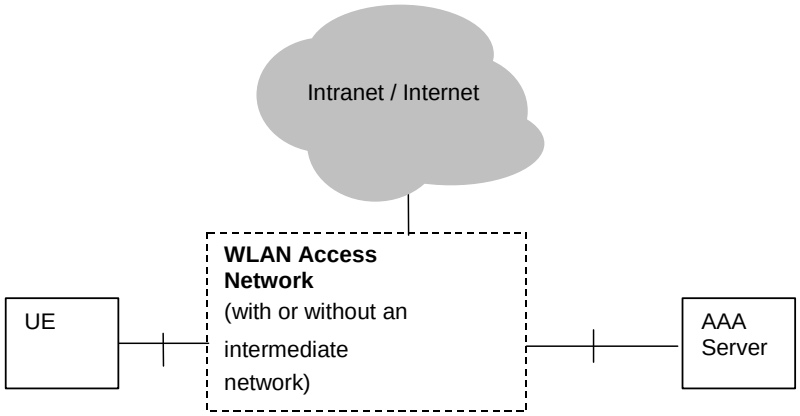


Figure 4.1: Simplified WLAN Network Model

- As 3GPP-WLAN interworking concentrates on the interfaces between 3GPP elements and the interface between the 3GPP system and the WLAN, the internal operation of the WLAN is out of 3GPP-WLAN interworking scope.

For IEEE 802.11 Wireless LANs, the authentication and security functionality between UE and WLAN is specified in the IEEE 802.11i standard.

[Editor's note; IEEE 802.11i is work in progress at the time of writing.]

5 High-level Requirements and Principles

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

It is necessary to provide WLAN interconnection between WLAN Networks and pre-R6 3GPP Networks. Hence it is required that this TS is compatible with R99 Networks and onward.

5.1 Access Control Requirements

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. security reasons.
- Minimal impact on the user equipment, i.e. client software.
- Minimal impact on existing WLAN networks.
- The need for operators to administer and maintain end user SW shouldall be minimized
- Existing ~~UICC cards should~~SIM and USIM shall be supported. ~~The solution as such should not require any new changes to the UICC cards.~~
- R6 USIM may include new functionality if seemed necessary e.g. in order to improve privacy.
- Changes in the HSS/HLR/AuC shall~~ould~~ 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
- The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber
- Authorization shall occur upon the success of the authentication procedure
- It shall be possible to indicate to the user of the results of authorization requests.
- It shall be possible to indicate to the user any conditions for use of an authorised service.
- Results of authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- The authorization mechanism shall be able to inform the user and WLAN immediately of any change in service provision.
- Policy control applies to the services authorized for the user
- ~~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 Access Control Principles

End to End Authentication : WLAN Authentication signalling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and enabling the access to the WLAN and 3GPP network. 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, ETSI HIPERLAN2 shall be conform with TS 101 761, 101 493 , Draft TS [H2-3G interworking].

Transporting Authentication signalling between WLAN and 3GPP network : WLAN Authentication signalling shall be transported **between WLAN and 3GPP network** by standard mechanisms, which are independent on the specific WLAN technology utilised within the WLAN Access network. The transport of Authentication signalling **between WLAN and 3GPP network** shall be based on standard Diameter or RADIUS protocols.

Service Selection

The end to end signalling shall include means for delivering encrypted service selection information from the UE to the 3GPP AAA server. The service selection information may contain APN and External Protocol Configuration Options as they are defined in 3GPP TS 24.008. Before admitting the user to access WLAN, 3GPP AAA server shall verify users subscription to the indicated APN against the WLAN subscriber profile retrieved from HSS.

5.3 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.

5.3.1 General Requirements

Authentication shall rely on (U)SIM based authentication mechanisms.

5.3.2 USIM based Authentication

USIM 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. An example of USIM-based authentication procedure, EAP/AKA, is found in Annex A.

5.3.3 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. An example of SIM-based authentication procedure, EAP/SIM, is found in Annex A.

5.3.4 WLAN specific SIM and USIM functions

It shall be possible to use the existing unmodified USIM for WLAN EAP-AKA and SIM for EAP-SIM respectively. For these SIMs and pre-release 6 USIMs the temporary ID shall be stored in the WLAN UE (outside the SIM/USIM).

The R6 USIM shall be able to store the temporary ID in order to minimize the need to send the permanent IMSI based identifier.

5.3.5 Re-authentication

On some networks, EAP authentication may be performed frequently. For such cases, EAP SIM and EAP AKA include an optional re-authentication procedure. Re-authentication causes less load on the network and is faster to execute than the full SIM/USIM authentication procedure. Re-authentication is optional to implement for both the WLAN UE and 3GPP AAA server. On each EAP authentication, either one of the entities may also fall back on full authentication if they do not want to use re-authentication. Re-authentication is based on the keys derived on the preceding full authentication.

On re-authentication, the UE protects against replays with an unsigned 16-bit counter. The server includes an encrypted server nonce (NONCE_S) in the re-authentication request. The Message Authentication Code attribute in the client's response is calculated over NONCE_S to provide a challenge/response authentication scheme. The NONCE_S also contributes to the new session keys.

Because one of the objectives of the re-authentication procedure is to reduce load on the network, the re-authentication procedure does not require the 3GPP AAA server to contact a reliable database. Therefore, the re-authentication procedure makes use of separate re-authentication user identities. Pseudonyms and the permanent IMSI-based identity are reserved for full authentication only. The network does not need to store re-authentication identities as carefully as pseudonyms. If a re-authentication identity is lost and the network does not recognize it, the 3GPP AAA server can fall back on full authentication.

If the 3GPP server supports re-authentication, it may communicate an encrypted re-authentication identity for next re-authentication to the WLAN UE during full authentication. If the client wants to use re-authentication, it uses this re-authentication identity on next authentication.

5.4 User Identity

The network authentication procedure are based on the use of EAP method, as described in clause 7, where User Identity field carries the user identity composed by the Public User Identity and a Home Network Domain Name. For user identity protection a Temporary Identity can be used.

5.4.1 Home network domain name

The home network domain name shall be in the form of an Internet domain name as specified in RFC 1035.

The UE shall derive the home network domain name from the IMSI as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC with "."; and
2. reverse the order of the MCC and MNC. Append to the result: "WLAN.3gppnetwork.org"

An example of a home network domain name is:

EXAMPLE: IMSI in use: 234150999999999;

- where;
- MCC: 234;
- MNC: 15;
- MSIN: 0999999999; and
- home domain name: 15.234.WLAN.3gppnetwork.org.

NOTE: Other mechanisms to retrieve a realm e.g. by having a realm configured in a R6 USIM are FFS.

5.4.2 User identity

FFS

5.4.3. Allocation of temporary identifier

The use of a temporary identifier is necessary to replace the IMSI in radio transmissions as it protects the user against tracing from unauthorized access networks.

As a working assumption, it is considered in this version of the TS that temporary identifiers are allocated and stored in the 3GPP AAA Server.

5.45 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).

5.65 Charging Principles

5.65.1 Offline Charging

WLAN offline charging includes mechanisms for collection and forwarding information about occurred WLAN access resource usage.

5.65.2 Online Charging

Online charging includes mechanism to get online permission from online charging system to allow an online charged subscriber to access WLAN.

5.7 Network Selection Principles

If the WLAN radio technology allows for features enabling radio access network sharing or provider selection these shall be reused for network selection in 3GPP-WLAN interworking.

5.7.1 Case of IEEE 802.11 WLANs

In the case of IEEE 802.11 WLANs, the WLAN network name is provided in WLAN beacon signal in so called SSID (Service Set ID) information element. There is also the possibility for a UE to actively solicit support for specific SSIDs by sending a probe request message and receive a reply if the access point does support the solicited SSID. [IEEE 802.11-01/659r0]

Once confirmed the availability of one of the preferred SSIDs either in beacon or in a probe response message, WLAN UE performs association with the particular access point using the selected preferred SSID.

WLAN acting in 3GPP reference model as a DIAMETER client for transport of authentication exchanges carried in EAP, shalluse the used SSID as information that determines the first hop routing of DIAMETER frames, according to 3GPP reference model this implies selection of 3GPP AAA proxy. In this way the user can select either his/her home operator or its preferred roaming partner's 3GPP AAA proxy. 3GPP AAA Proxy then makes further AAA routing decision based on the NAI it has received.

To enable the PLMN Selection functionality for automatic processing SSID format would have to be standardized. SSID is 0-32 octets large (see IEEE 802.11-1999).

5.7.2 Case of HiperLan/2 WLANs

FFS

5.7.3 Case of Bluetooth WLANs

FFS

6 Interworking Architecture

6.1 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 Non Roaming WLAN Inter-working Reference Model

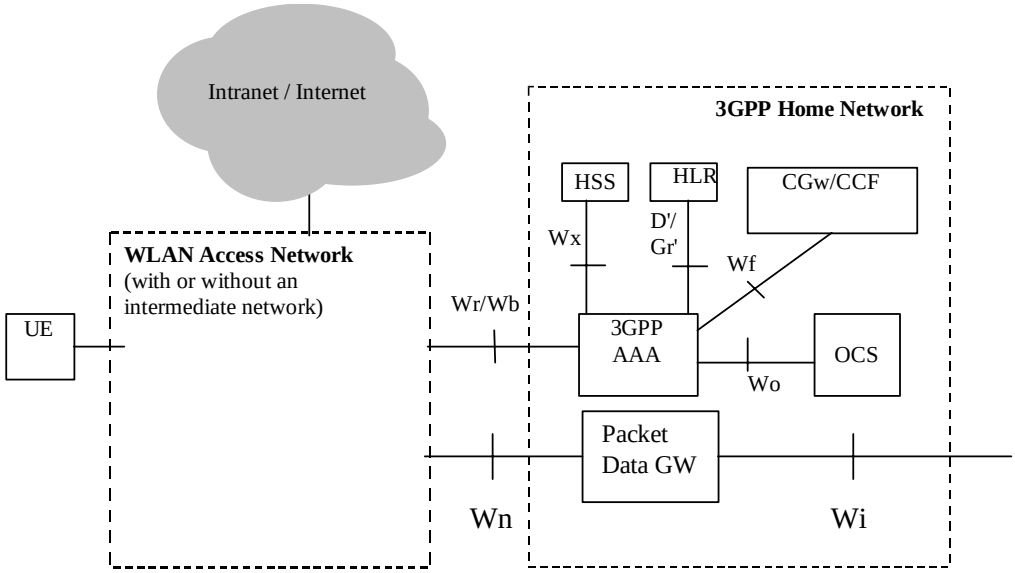


figure 6.1 Non Roaming Reference Model.

6.1.2 Roaming WLAN Inter-working Reference Model

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.

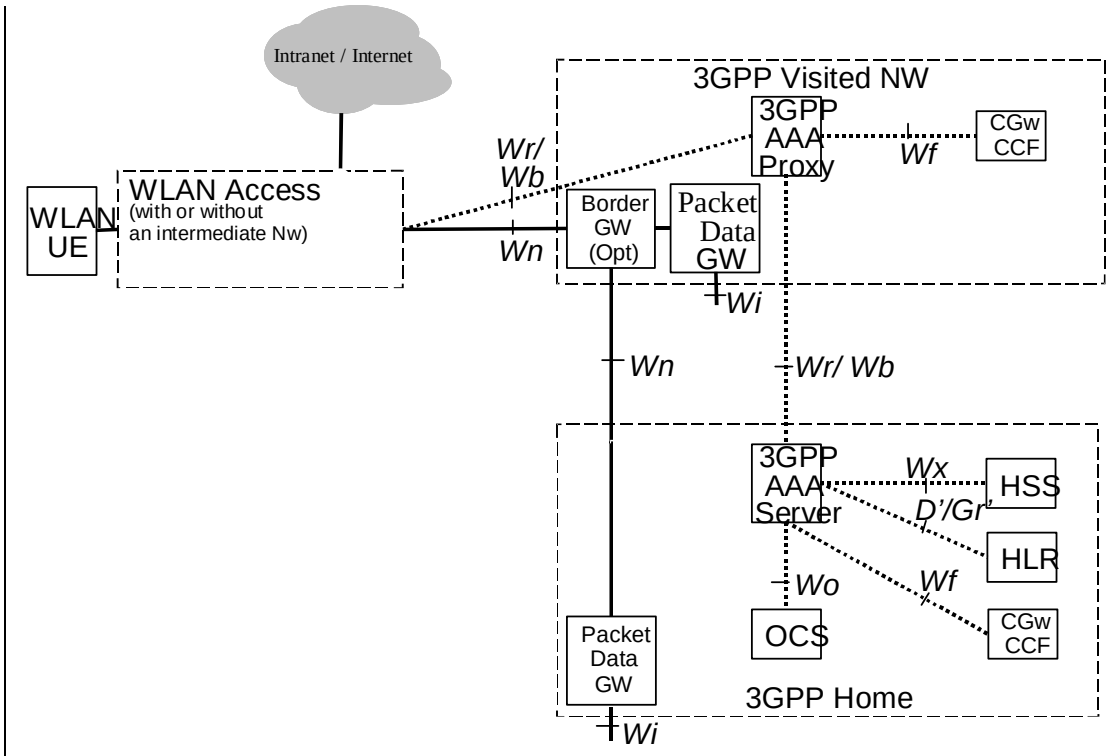


Figure 6.3 Roaming Reference Model.

6.2 Network elements

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

- the UE (equipped with (U)ICC card including (U)SIM) 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 (U)ICC), operation and software environment are not under the exclusive control of the 3GPP system operator, such as a laptop computer or PDA with a WLAN card, (U)ICC card reader and suitable software applications.

- the 3GPP proxy AAA represents a Diameter proxying and filtering functionthat resides in the visited 3GPP network. The 3GPP proxy AAA functions include.:

- Relay the AAA information between WLAN and the 3GPP AAA Server.
- Enforce policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Report charging/accounting information to local CCF/CGw for roaming users
- Service termination (O&M initiated termination from visited NW operator)
- Receives authorization information (Subscriber information)
- Forwarding authorization information to WLAN
- Rejection of authorization according to local policy

The 3GPP proxy AAA functionality can reside in a separate physical network node, it may reside in the 3GPP AAA server or any other physical network node.

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

  - retrieves authentication information and subscriber profile (including subscriber's authorisation information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network;
  - authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies.
  - communicates authorisation information to the WLAN potentially via AAA proxies.
  - registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorised 3GPP subscriber.
  - may act also as a AAA proxy (see above).

Editor's note : Clarification on the caching functionality is for further study

- 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.

- The Border Gateway is an optional gateway via which the data between WLAN and Packet Data Gateway can be routed.

- The Packet Data Gateway is a node via which packet data networks are connected to 3GPP interworking WLAN. The location of Packet Data Gateway may be different for each specific service accessed WLAN. For some WLAN connections no Packet Data Gateway is used, for some accessed services Packet Data Gateway may be in home network and for some accessed services it may locate in visited Nw.

6.3Reference Points

6.3.1 Wr

6.3.1.1 General description

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.

6.3.1.2 Functionality

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

6.3.1.3 Protocols

Wr reference shall be based on IETF Diameter Base protocol. EAP authentication shall be transported over *Wr* reference point by Diameter Extensible Authentication Protocol (EAP) Application.,

[Editors note: Diameter base protocol is work in progress in IETF [draft-ietf-aaa-diameter-12.txt]]

[Editors note: Diameter Extensible Authentication Protocol (EAP) Application is work in progress in IETF [draft-ietf-aaa-eap-00.txt]]

To support legacy logical nodes outside of 3GPP scope and which terminate or proxy the Wr reference point signalling and not supporting Diameter protocol, a signalling conversion between RADIUS and Diameter may be performed. This conversion is not specified by 3GPP.

6.3.2 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).

6.3.3 D'/Gr'

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

The functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HLR.

D'/Gr' include a subset of D/Gr Reference Point.

6.3.~~3~~4 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.

6.3.5~~4~~ 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.

6.3.~~5~~6 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

6.3.7 Wn

Reference point *Wn* indicates the reference point for transporting tunneled WLAN user data towards 3GPP system. Routing of *Wn* reference point is service specific. For accessing home network services the *Wn* may be routed directly between WLAN and Home 3GPP Network or forced to go via Border Gateway functionality within the Visited Network.

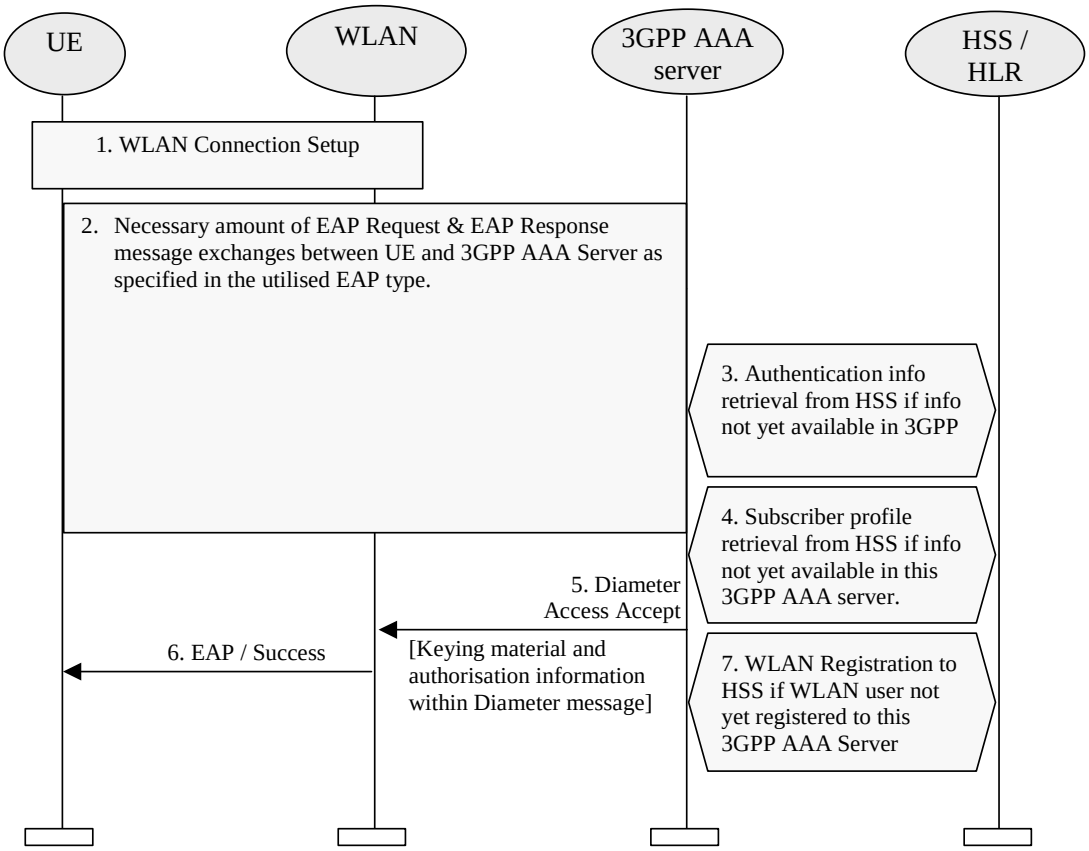
6.3.8 Wi

This is the reference point between Packet Data GW and a packet data network. The packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services.

Wi reference point is similar to the *Gi* reference point provided by the PS domain.

7 Procedures

7.1 Authentication and Authorisation



1. WLAN connection is established with a Wireless LAN technology specific procedure (out of scope for 3GPP).

2. The EAP authentication procedure is initiated in WLAN technology specific way.

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

All EAP packets are transported over the Wr reference point encapsulated within Diameter messages as specified in Diameter EAP application .

[Editors note: Diameter Extensible Authentication Protocol (EAP) Application is work in progress in IETF [draft-ietf-aaa-eap-00.txt]]

A number of EAP Request EAP Response message exhanges is executed between 3GPP AAA Server and UE. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.

3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in 3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised.

4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.

[Editors note: The execution order of steps 5 and 6 as well as further division of these steps to several substeps is ffs.]

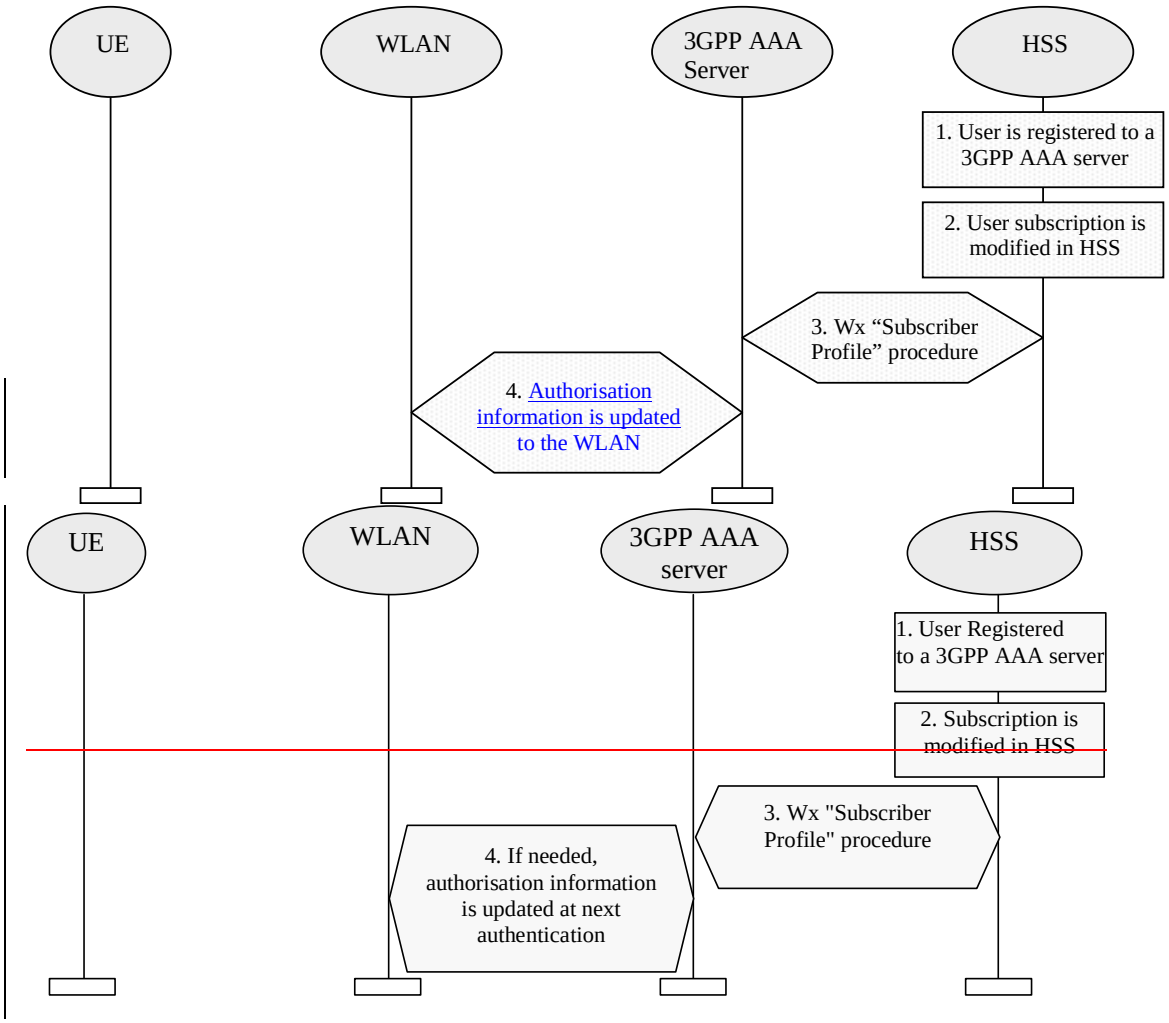
5 If the EAP authentication was successful, then 3GPP AAA Server sends Diameter Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success messge, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunneling attributes) to the WLAN.

WLAN stores the keying material and authorisation information to be used in communication with the authenticated UE.

6 WLAN informs the UE about the successful authentication with the EAP Success message.

7 3GPP AAA server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already regiostered to this 3GPP AAA Server.

7.2 Subscriber Profile Update



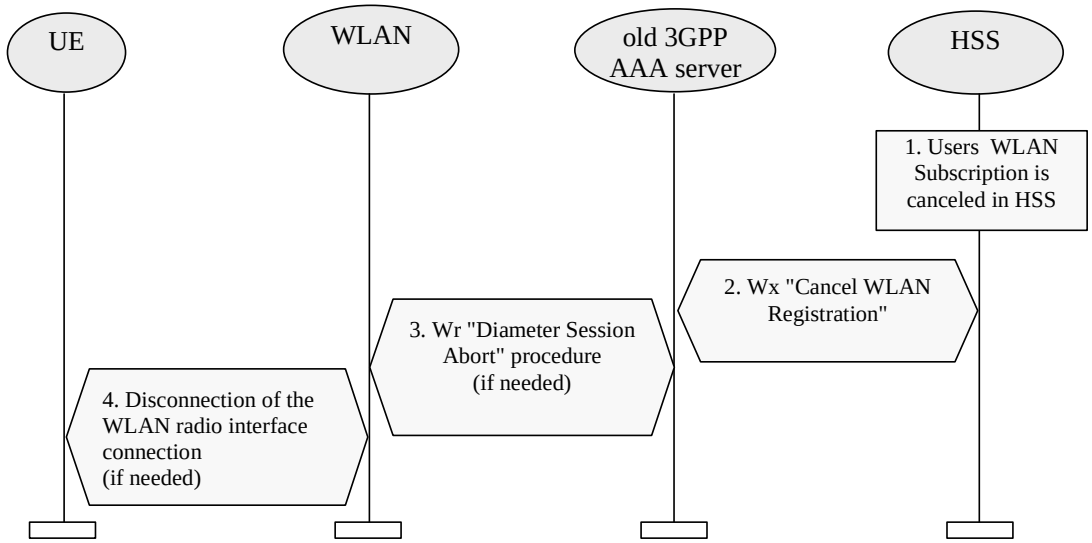
1. User is registered to a 3GPP AAA server

2. Subscribers subscription is modified inthe HSS e.g. via O&M.

3. HSS updates the profile information stored in the registered 3GPP AAA server by Wx reference point procedure "Subscriber Profile".

4. The authorisation information of the associated connection is updated to WLAN as necessary.~~If changed, the authorisation information of the associated connection is updated to WLAN at the next EAP authentication between UE and 3GPP AAA Server.~~

7.3 Canceling WLAN Registration



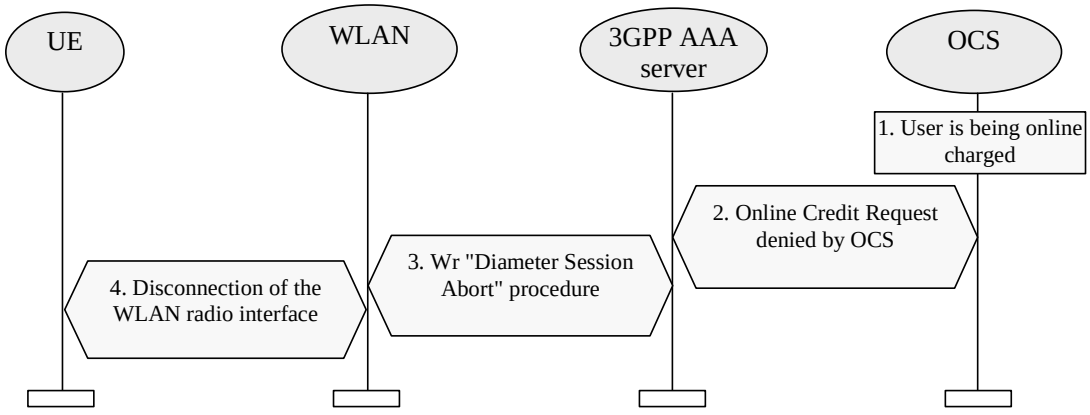
1. The 3GPP subscribers WLAN subscription is canceled in HSS.

2. HSS cancels subscribers WLAN registration in the 3GPP AAA Server by Wx reference point procedure "Cancel WLAN Registration". In the messages subscriber is identified by his permanent identity.

3. If the subscribers connection still exists, Wr reference point procedure "Diameter Session Abort" procedure is executed towards WLAN.

4. If the radio connection still exists, WLAN disconnects the radio interface connection by WLAN technology specific mechanisms.

7.4 Disconnecting a Subscriber by Online Charging System



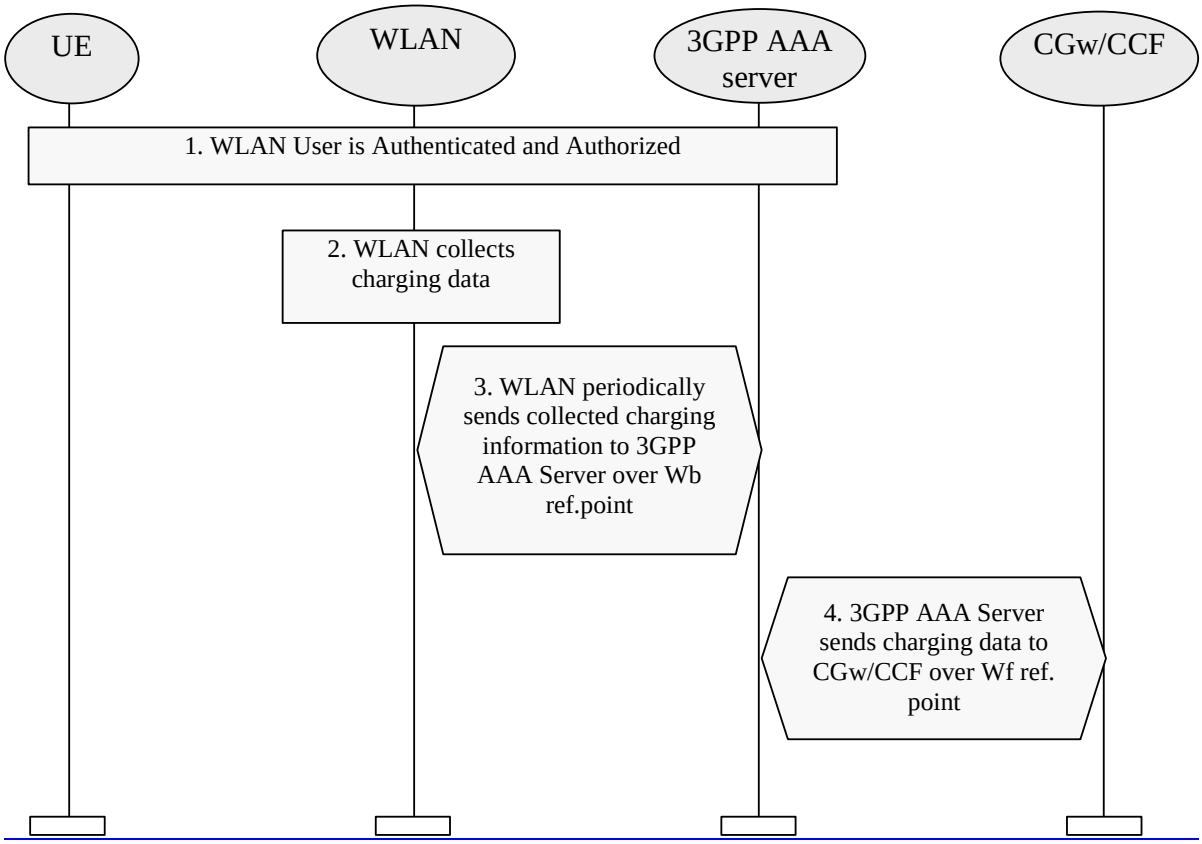
1. A subscriber is being online charged by 3GPP AAA server.

2. OCS (online Charging System) denies credit request from the 3GPP AAA server for WLAN access. The possibly already retrieved online credit runs out.

3. To disconnect the subscribers connection, *Wr* reference point procedure "Diameter Session Abort" procedure is executed towards WLAN.

4. WLAN disconnects the radio interface connection by WLAN technology specific mechanisms

7.5 Charging offline charged subscribers



1. WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA server. Part of the profile is information that the user is to be offline charged.

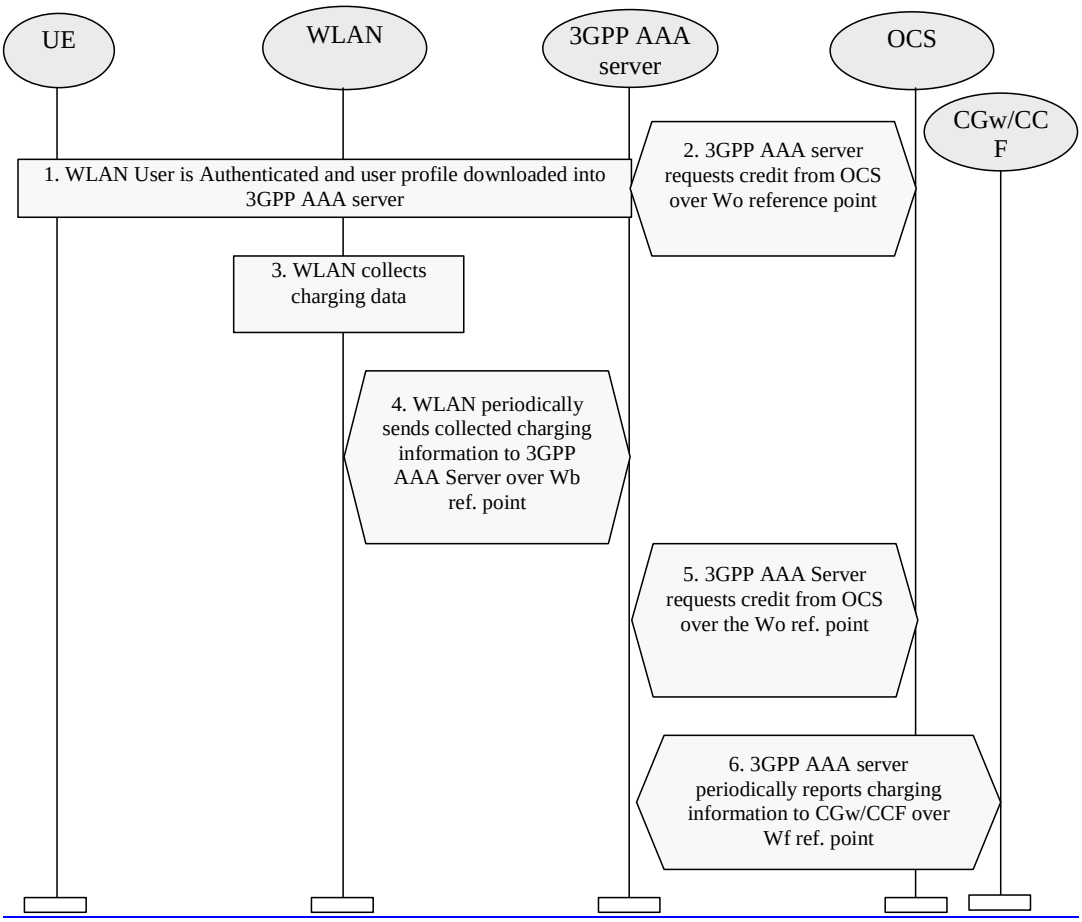
2. WLAN access network collects charging data related to access or services locally consumed.

3. WLAN access network periodically forwards collected charging information to the 3GPP AAA server over Wb reference point.

4. 3GPP AAA server forwards charging information to the CGw/CCF over the Wf reference point.

Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local CGw/CCF over Wf reference point.

7.6 Charging online charged subscribers



1. WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA server. Part of the profile is information that the user is to be online charged.

2. 3GPP AAA server obtains online charging credit from the OCS.

3. WLAN access network collects charging information.

4. WLAN access network periodically forwards collected charging information to the 3GPP AAA server over Wb reference point. WLAN access network does not request charging credit as the fact whether a user is online of offline charged is transparent for it.

5. If the credit is to be exceeded, 3GPP AAA server requests further credit from OCS over the Wo reference point.

6. 3GPP AAA server periodically reports to usage of resources to the CGw/CCF over Wf reference point. The purpose of this reporting is to enable inter-operator clearing.

Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local CGw/CCF over Wf reference point.

Annex A (informative): Refererence Points Signalling Flows

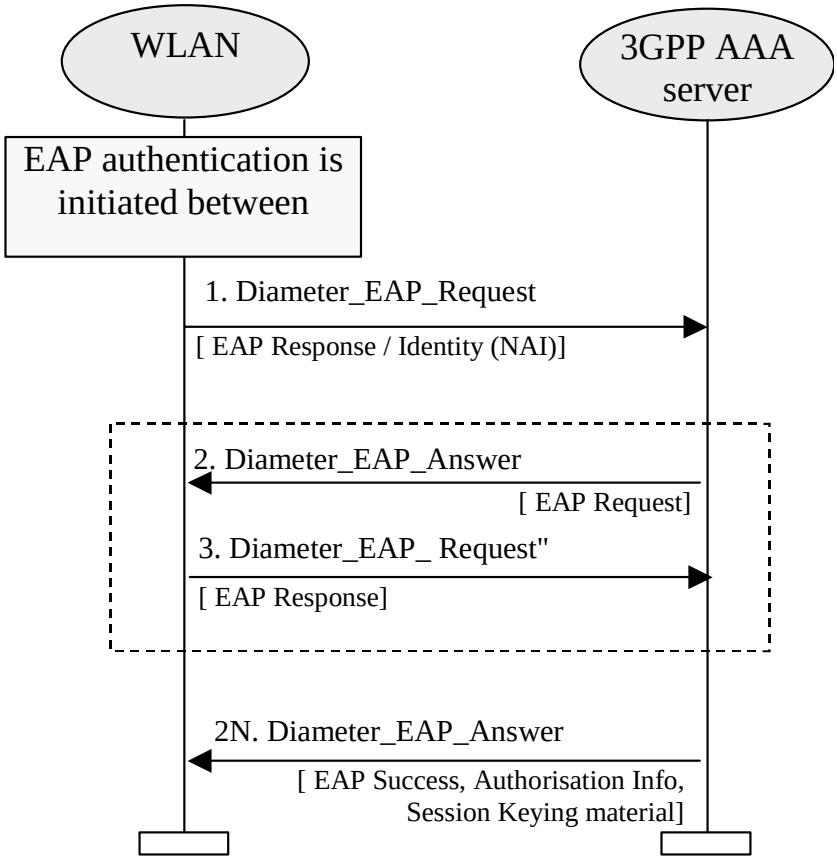
A.1 Signalling Sequences examples for Wr Reference Point

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.

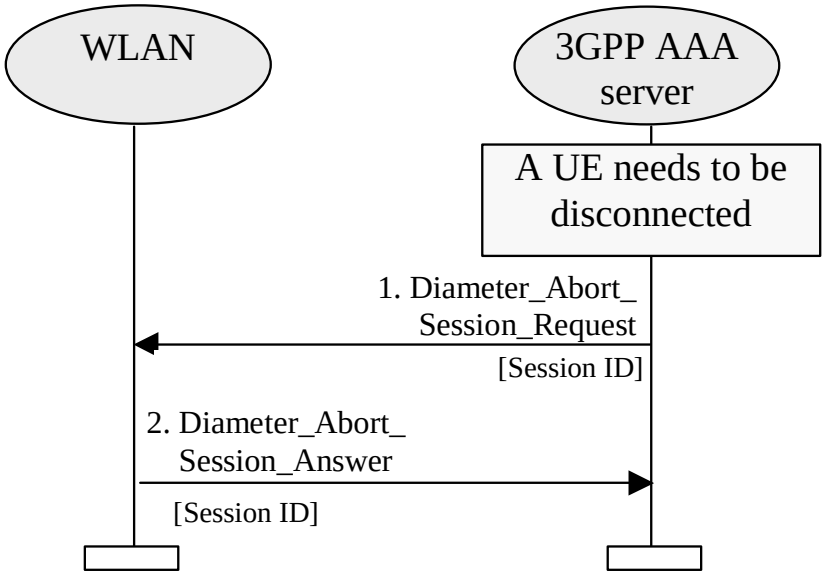
This Diameter_EAP_Answer message also carries the authorisation information (e.g. NAS Filter Rule or Tunneling attributes) for the authenticated session. Message also carries the keying material from 3GPP AAA Server to WLAN to be used for the authenticated session by WLAN.

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.



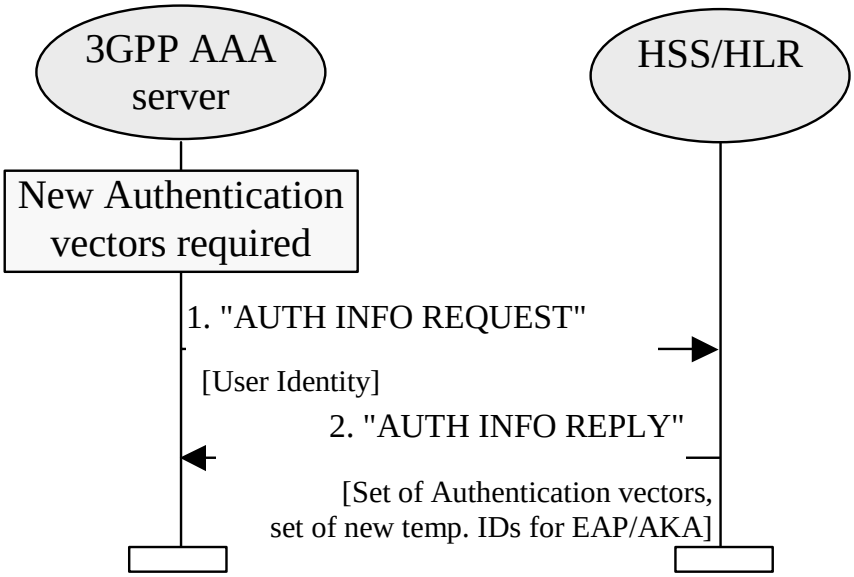
1. When 3GPP AAA Server needs to disconnect (e.g. after receiving an external trigger) a 3GPP subscriber from the WLAN access service, the 3GPP AAA Server sends a Diameter_Abort_Session_Request to WLAN . This message contains the Session ID by which the session is identified within WLAN.

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.



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.

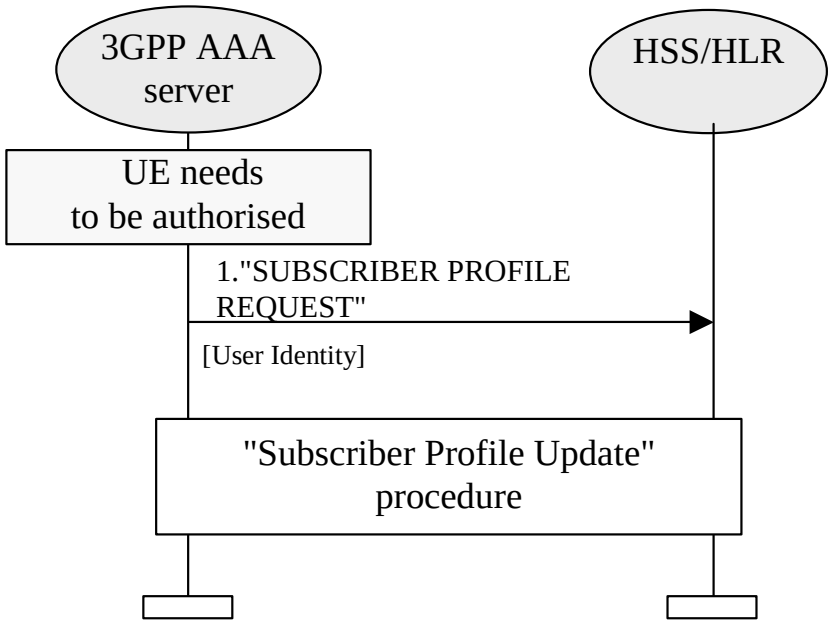
Note: It is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server

   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.



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.

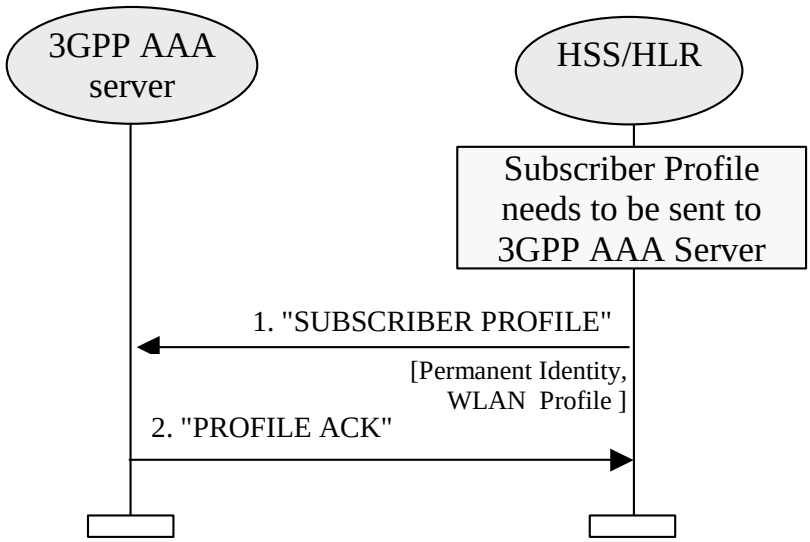
   In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the pseudonym (associated with the IMSI) allocated in the previous authentication or, in case of the very first authentication, the IMSI.

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.



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,

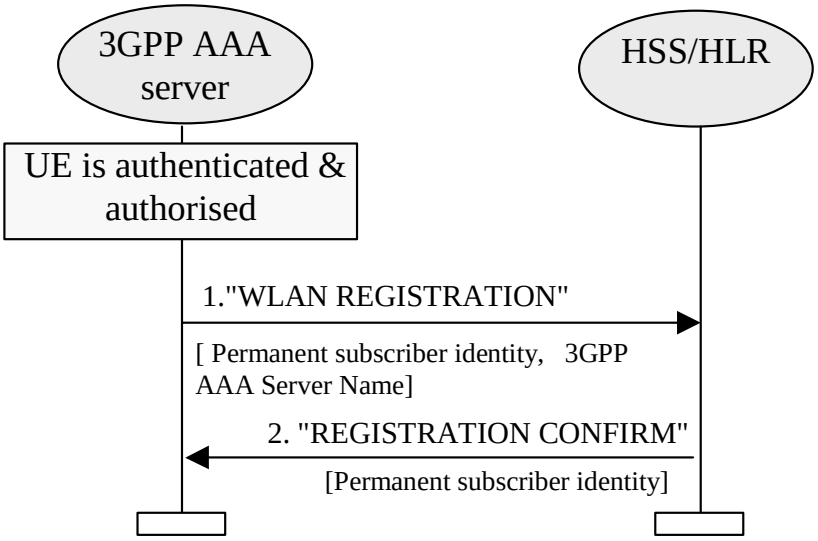
   - charging mechanism (offline / online),
   - in case of online charging. the DNS name of the subscribers online charging system

   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.

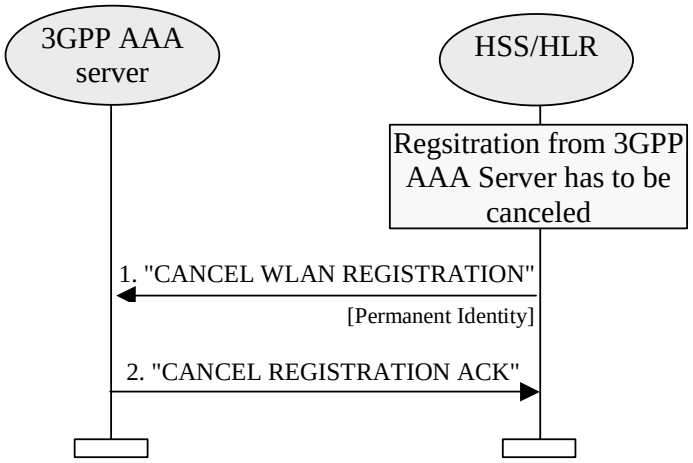


1. 3GPP AAA server initiates the signalling when a new 3GPP subscriber has been authenticated and authorised by the 3GPP AAA server. 3GPP AAA server sends WLAN REGISTRATION message to the HSS/HLR. This message contains the address/name of the 3GPP AAA Server and the permanent subscriber identifier. In 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.

A.2.5 Cancel Registration

This signalling sequence is initiated by a HSS when subscription conenction has to be removed from 2 3GPP AAA Server. This can happen when the subscription is cancelled in HSS.

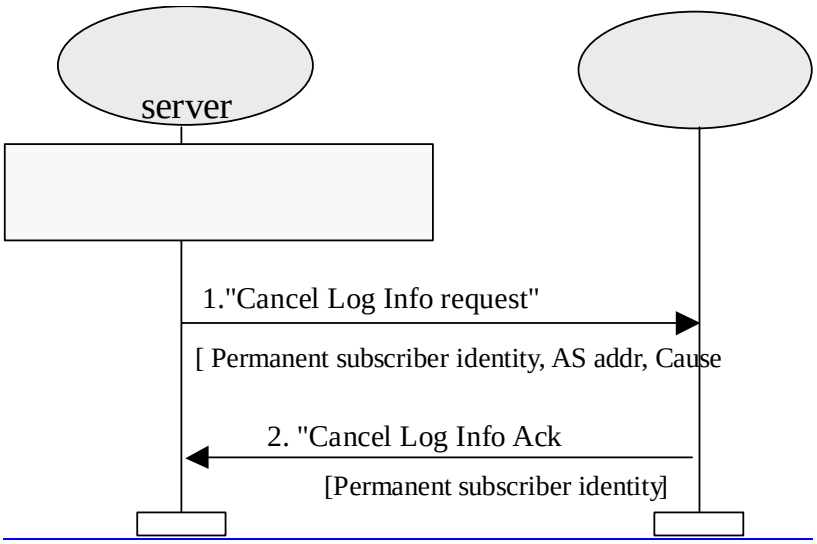


1. HSS/HLR initiates the signalling when the registration of a 3GPP subscriber has to be canceled from a 3GPP AAA server. Subscriber is identified by his permanent user identity.

2. 3GPP AAA Server confirms the reception of the CANCEL WLAN REGISTRATION message by CANCEL REGISTRATION ACK message.

A.2.6 Cancel LOG INFO (example given in the case of a R6 HSS)

The cancel log info procedure can be used by 3GPP AAA SERVER to request HSS to update subscriber status informaiton. . When WLAN user wants to log off the WLAN access network, this procedure guarantees the subscriber information is immediately deleted from HSS.



1)3GPP AAA SERVER initiates the signalling when WLAN access network informs 3GPP AAA SERVER that WLAN user wants to log off the network. 3GPP AAA SERVER sends CANCEL LOG INFO REQUEST message to HSS to request HSS remove subscriber status information,because this subsciber status information should not anymore be kept at HSS. This message contains subscriber's identity, AS address and cause. Subscriber is identified by his permanent identity.

2)When HSS receives CANCEL LOG INFO REQUEST, HSS deletes subsrciber status informion related to WLAN access network, then, HSS sends CANCEL LOG INFO ACK message to 3GPP AAA SERVER to confirm the request.

A.3 Example of Authentication procedures

A.3.1 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 0~~3~~5 (draft-arkko-pppext-eap-aka-0~~3~~5.txt). The following procedure is based on EAP/AKA authentication mechanism:

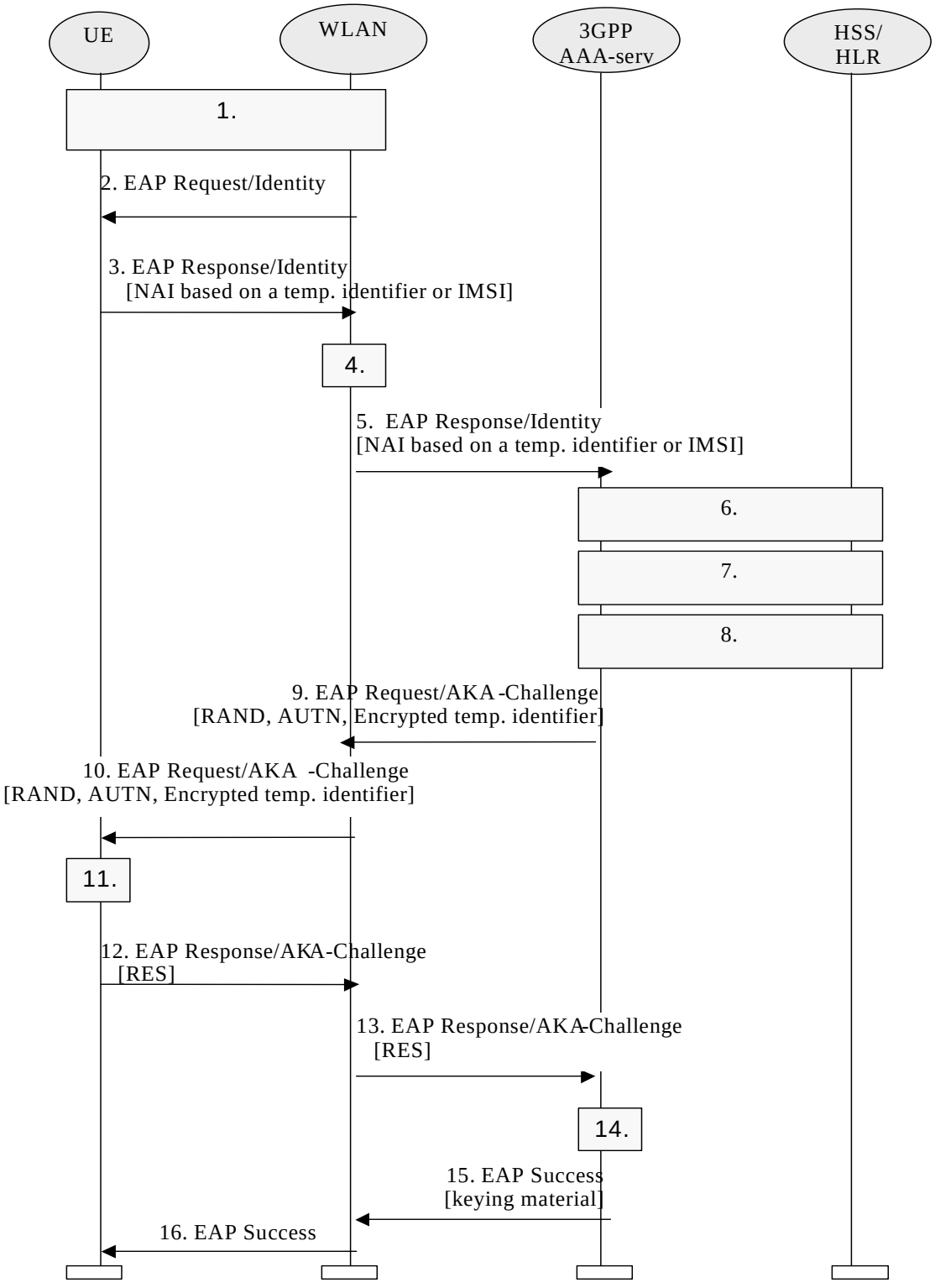

UE
WLAN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity
[NAI based on a temp. identifier or IMSI]
4.
5. EAP Response/Identity
[NAI based on a temp. identifier or IMSI]
6.
7.
8.
9. EAP Request/AKA-Challenge
[RAND, AUTN, Encrypted temp. identifier]
10. EAP Request/AKA -Challenge
[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~~the temporary identifier ~~(pseudonym)~~ allocated to UE in previous authentication ~~or, in the case of first authentication,~~ if available and valid. Otherwise, the NAI shall contain the IMSI.

Note : generating an identity conforming to NAI format from IMSI is defined in EAP/AKA draft (draft-arkko-pppext-eap-aka-0~~3~~5.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.~~ If a temporary identifier is provided, it is mapped to the corresponding IMSI.

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~~ temporary identifier is chosen and encrypted. Temporary identifier format is FFS.

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~~ temporary identifier 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.

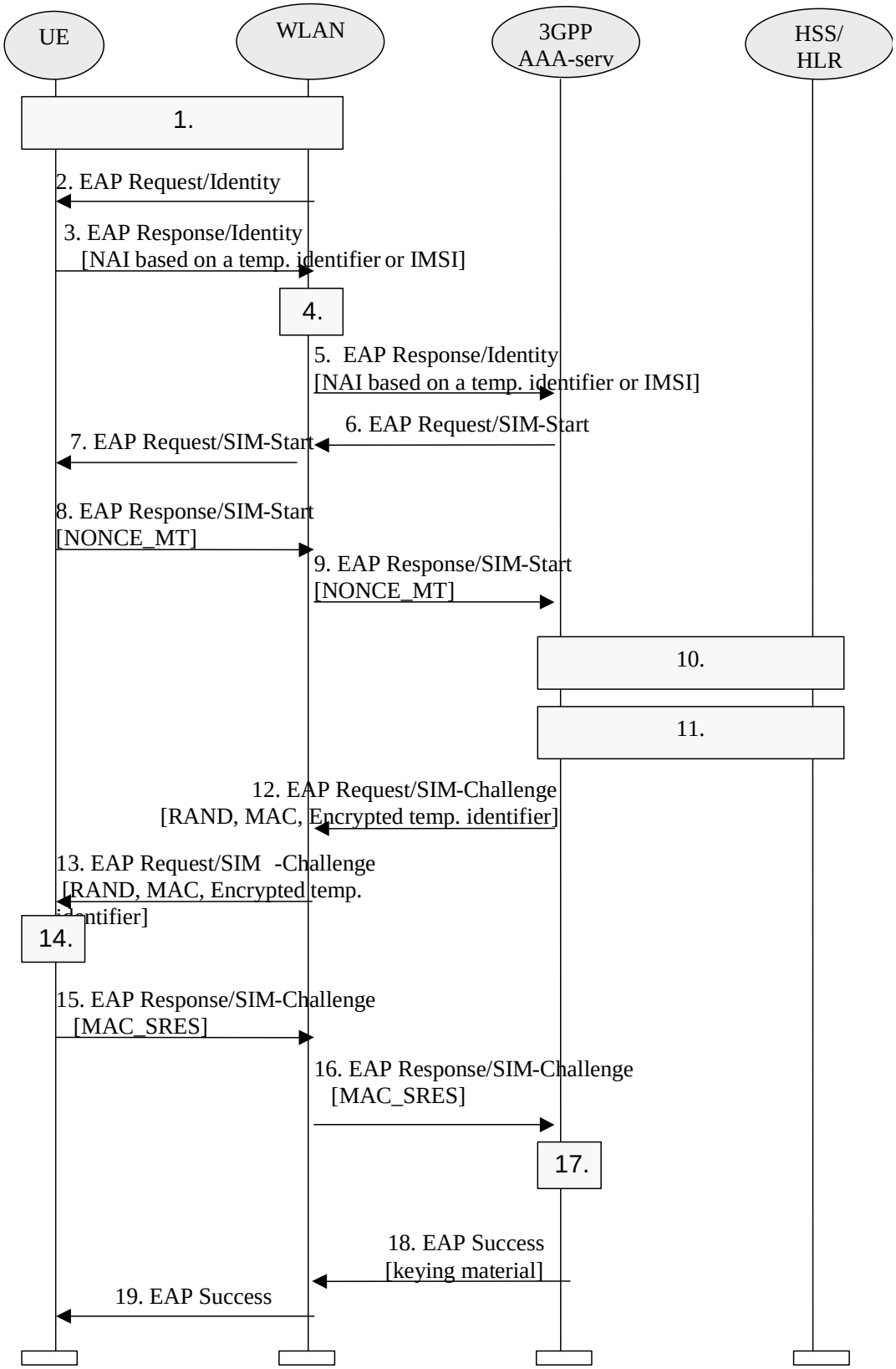
Note 2: Temporary identifier is only used for authentication purpose. User identification on the data path is done by the Access Point in a way that is proper to the WLAN.~~generation and storage is FFS.~~

A.3.2 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 0~~4~~6 (draft-haverinen-pppext-eap-sim-0~~6~~4.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 Request/SIM -Challenge [RAND, MAC, Encrypted temp. identifier]
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~~the temporary identifier ~~(pseudonym)~~ allocated to UE in previous authentication if available and valid. Otherwise, the NAI shall contain~~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-0~~4~~6.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. If a temporary identifier is provided, it is mapped to the corresponding IMSI. ~~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 temporary identifier ~~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 is only used for authentication purpose. User identification on the data path is done by the Access Point in a way that is proper to the WLAN~~generation and storage is FFS.~~

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

A.3.3 Alternative EAP initialization.

The following figure shows an example where the realm identifying the 3GPP AAA server is retrieved by a method linked with the WLAN technology. Once the Diameter connection is initialized, the 3GPP AAA server can start the EAP identity request phase if necessary.

Editor's Note : the application of this procedure to IEEE 802.11 needs to be studied further.

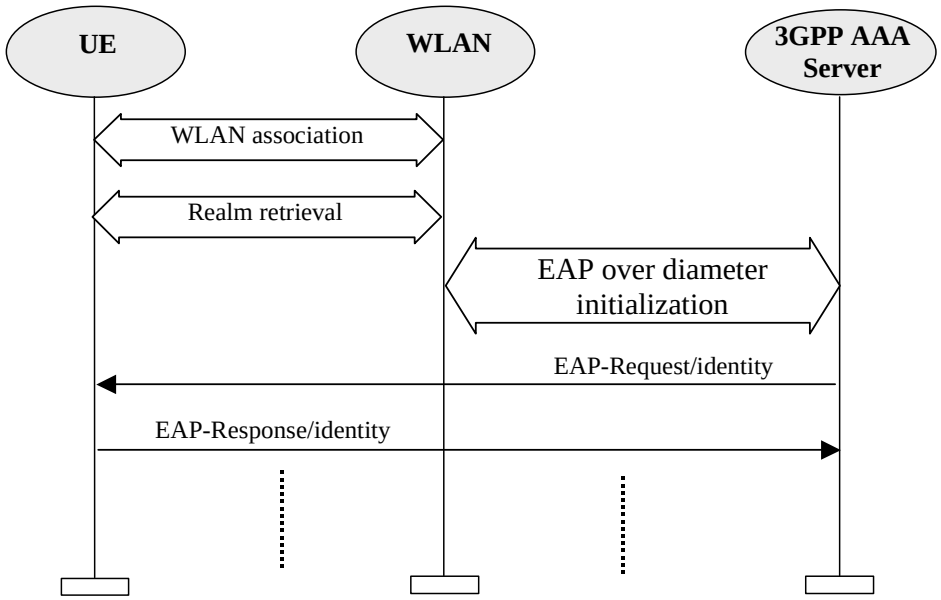
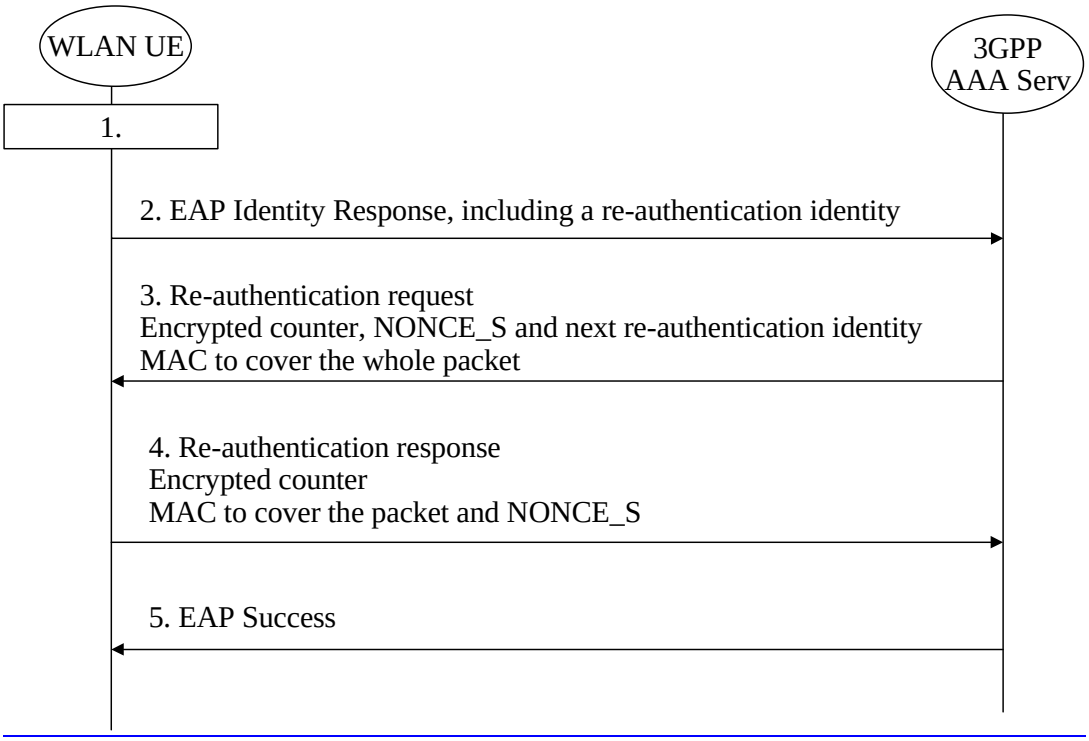


Figure 1 - end-to-end EAP initialization session

A.3.4 Re-authentication message sequence chart

The message sequence chart below illustrates the operation on re-authentication.



1. Either the UE or the WLAN initiates the authentication procedure with wireless LAN technology specific means. The WLAN UE is requested to send its identity

2. WLAN UE wishes to use the re-authentication procedure and therefore uses a re-authentication identity

3. 3GPP AAA server recognizes the re-authentication identity and agrees on using re-authentication. The 3GPP AAA server sends a re-authentication request (of the EAP type EAP/SIM or EAP/AKA) to the UE. The request contains an encrypted counter, an encrypted server challenge (NONCE_S) and a Message Authentication Code to cover the whole packet. The packet may also include an encrypted next re-authentication identity for next re-authentication

4. WLAN UE verifies the Message Authentication Code and checks that the counter value is fresh. If successful, the WLAN UE responds with a re-authentication response packet that includes the counter value encrypted and a Message Authentication Code that covers the EAP packet and the server challenge NONCE_S

5. 3GPP AAA server verifies the Message Authentication Code and the counter. If successful, the 3GPP AAA server sends EAP Success to the WLAN UE.

WLAN UE and 3GPP AAA Server derive new session keys. 3GPP AAA Server sends the session keys to WLAN.

Annex B (informative): WLAN Radio Technologies

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	High Speed Data Applications Susceptible to interference from Bluetooth and other devices	Wire Replacement; Inexpensive Low component count Low Power	Improve Spectral Efficiency over 802.11b	Products not available yet

Table 1 WLAN Technology Comparison

Annex C (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2002-08					*Converted TR23.934v0.5.0 into this TS*	*0.0.0*	*0.1.0*
2002-09					Raised to v.1.0.0 for presentation at SA#17 (same content as v.0.1.0)	0.1.0	1.0.0