

Source: TSG CN WG 1
Title: 3GPP System to WLAN Interworking; UE to Network protocols;
Stage 3
Agenda item: 9.18
Document for: INFORMATION,- Draft technical report 3GPP TS 24.234 v1.0.0

Presentation of Technical Report to TSG or WG

Presentation to: TSG CN Meeting #22
Document for presentation: TR, Version 1.0.0
Presented for: Information

Abstract of document:

The scope of this TS is to specify the UE and WLAN AAA Server functionalities for WLAN PLMN selection, WLAN Selection (radio selection), WLAN authentication and WLAN Access authorization.

Changes since last presentation to TSG Meeting #:

None. The TS is presented first time to the plenary.

Outstanding Issues:

- Completed work: this version of the TS contains detailed definition of WLAN PLMN selection, WLAN authentication procedures and WLAN access authorization.
 - Remaining topics: main remaining work is on WLAN selection procedures and WLAN parameters.
 - Scenario 3 does not affect this TS.
-

Contentious Issues:

WLAN selection procedures: contributions on the topic were postponed from CN1#32 to next meeting in January 2004 due to the need of feedback from SA1 on the requirements for this procedure.

3GPP TS 24.234 V1.0.0 (2003-12)

Technical Specification

**3rd Generation Partnership Project;
Technical Specification Group Core Network;
3GPP System to WLAN Interworking;
UE to Network protocols;
Stage 3
(Release 6)**



The present document has been developed within the 3rd Generation Partnership Project (3GPPTM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPPTM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

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

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2003, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword.....	6
Introduction.....	6
1 Scope.....	7
2 References.....	7
3 Definitions, symbols and abbreviations.....	8
3.1 Definitions.....	8
3.2 Symbols.....	9
3.3 Abbreviations.....	9
4 General.....	9
4.1 3GPP WLAN Interworking System.....	9
4.2 WLAN UE Identities.....	9
4.2.1 General.....	9
4.2.2 Root NAI.....	10
4.2.3 Decorated NAI.....	10
5 UE to WLAN protocols.....	10
5.1 WLAN protocols.....	10
5.2 3GPP WLAN selection.....	10
5.2.1 Case of IEEE 802.11 WLANs.....	10
5.3 3GPP WLAN PLMN Selection.....	11
5.3.1 General.....	11
5.3.2 Network Advertisement.....	11
5.3.2.1 UE procedures.....	11
5.3.3 Network selection.....	12
5.3.3.1 UE procedures.....	12
5.3.3.1.1 Automatic Network Selection Mode Procedure.....	12
5.3.3.1.2 Manual Network Selection Mode Procedure.....	12
5.3.3.1.3 Other Automatic Network Selection Mode Procedures.....	13
5.4 List of forbidden PLMNs for WLAN access.....	13
6 UE to 3GPP Network protocols.....	13
6.1 UE to 3GPP AAA Server protocols.....	13
6.1.1 WLAN Access Authentication and Authorization protocols.....	13
6.1.1.1 UE procedures.....	14
6.1.1.1.1 User Identity Privacy.....	14
6.1.1.1.2 EAP AKA Authentication.....	14
6.1.1.1.3 EAP SIM based Authentication.....	14
6.1.1.1.4 Re-authentication.....	14
6.1.1.2 3GPP AAA Server procedures.....	14
6.1.1.2.1 User Identity Privacy.....	14
6.1.1.2.2 EAP SIM and EAP AKA based Authentication.....	14
6.1.1.2.3 3GPP AAA Server Operation in the Beginning of Authentication.....	15
6.1.1.2.4 Re-authentication.....	15
6.1.1.2.5 WLAN Access Authorization.....	15
7 List of parameters.....	15
7.1 PLMN List.....	15
7.2 I-WLAN SSID.....	16
Annex <A> (normative): <Normative annex title>.....	16
Annex (informative): Figures applicable to 3GPP WLAN IW model.....	16
Access Control Reference Model.....	16
Network Advertising and Selection.....	17

Annex <X> (informative): Change history19

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

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

The present document specifies the WLAN selection, WLAN PLMN selection, WLAN Authentication and WLAN Access Authorization procedures used for the interworking of the 3GPP System and WLANs.

The present document is applicable to the WLAN User Equipment (UE) and the network. In this technical specification the network includes the WLAN and 3GPP network.

WLAN selection and WLAN PLMN selection are performed between the WLAN UE and the WLAN.

Authentication signalling is transported through 3GPP AAA proxies in roaming situations. This document does not specify additional functionality for 3GPP-AAA proxies.

WLAN authentication and authorization signalling is carried between WLAN-UE and WLAN by WLAN Access Technology specific protocols. The transport of WLAN authentication signalling in the PLMN networks is done over Wt/Ws reference point as defined in 3GPP TS 29.234 [3].

These procedures are defined in terms of EAP messages which are encapsulated in RADIUS and/or Diameter frames in the Wt/Ws reference point. Details of the security framework for the end-to-end WLAN authentication are covered in 3GPP TS 33.234 [5]. The transport of the end-to-end WLAN authentication signalling between WLAN and 3GPP network are covered in 3GPP TS 29.234 [3].

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 23.122: " Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".
- [2] 3GPP TS 23.234: "3GPP System to WLAN Interworking; System Description"
- [3] 3GPP TS 29.234: "3GPP System to WLAN Interworking; Stage 3 Description"
- [4] 3GPP TS 31.102: "Characteristics of the USIM Application".
- [5] 3GPP TS 33.234: "WLAN Interworking Security."
- [6] RFC 2284 (March 1998): "PPP Extensible Authentication Protocol (EAP)".
- [7] RFC 1035 (November 1987): "Domain Names – Implementation and specification".
- [8] RFC 2486 (January 1999): "The Network Access Identifier"
- [9] IETF Internet-Draft: "EAP AKA Authentication". draft-arkko-pppext-eap-aka-09, work in progress.
- [10] IETF Internet-Draft: "EAP SIM Authentication". draft-haverinen-pppext-eap-sim-10, work in progress.
- [11] IEEE Std 802.11-1999, Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE, Sep. 1999.

- [12] IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-00, work in progress.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [2] apply.

3GPP - WLAN Interworking (WLAN-3GPP IW)
3GPP AAA server
3GPP AAA proxy
Interworking WLAN
WLAN UE
WLAN Roaming

For the purposes of the present document, the following terms and definitions apply:

Active scanning: capability of a WLAN UE to actively solicit support for a specific SSID by for probing it.

Associated SSID: The SSID the UE used for association with a WLAN AP.

Broadcast SSIDs: The SSID available in the beacon signal.

Passive scanning: capability of a WLAN UE to look for the support for a specific SSID by listening to the SSIDs broadcast in the beacon signal.

PLMN selection: Procedure for the selection of a PLMN according to TS 23.122 [1] clause 3.1, either manually or automatically.

Selected SSID: This is the SSID that has been selected according to clause 5.2.1, either manually or automatically.

Selected WLAN PLMN: This is the PLMN that has been selected according to clause 5.3, either manually or automatically.

Supported PLMN: A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).

WLAN PLMN Selection: Usage of the supported PLMN list received in FFS message from WLAN AN and selection among those PLMNs.

WLAN selection: Procedure for the selection among the available WLAN APs

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [2] apply.

3GPP - WLAN Interworking (WLAN-3GPP IW)
3GPP AAA server
3GPP AAA proxy
Interworking WLAN
WLAN UE
WLAN Roaming

For the purposes of the present document, the following terms and definitions given in draft-adrangi-eap-network-discovery-and-selection [12] apply.

Decorated NAI
Root NAI

3.2 Symbols

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

Wr	Reference point between a WLAN and a 3GPP AAA Server/Proxy (control signalling)
Ws	Interface between a 3GPP AAA Server and 3GPP AAA Proxy (control signalling)
Wx	Reference point between an HSS and a 3GPP AAA Server

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorisation and Accounting
AKA	Authentication and Key Agreement
EAP	Extensible Authentication Protocol
I-WLAN	Interworking WLAN
NAI	Network Access Identifier
PDN	Packet Data Network
SSID	Service Set ID
WLAN	Wireless Local Area Network

4 General

Editor's Note: Provides general overview of WLAN-3GPP IW system.

4.1 3GPP WLAN Interworking System

The 3GPP AAA server is located in the home network and it is responsible for access control. The 3GPP AAA server interfaces to a WLANs, via the Wr interface, and to 3GPP AAA proxies in other 3GPP networks, each with their own interfaces to WLAN, via the Ws interface, and the 3GPP AAA proxy then communicates with the WLAN via the Wr interface.

The Wr, Ws and Wx reference points are defined in 3GPP TS 23.234 [2].

The WLAN-UE is equipped with an UICC (or SIM card) in order to access the WLAN interworking service.

The 3GPP AAA proxy relays access control (authentication and access authorization) signalling to the home 3GPP AAA server. The 3GPP AAA proxy is transparent to signalling within the scope of this specification. Within the scope of this specification signalling the Wr and Ws interfaces are therefore identical.

The 3GPP AAA server procedures covered in this specification are:

- authentication of the 3GPP subscriber based on the SIM/USIM credentials; and
- access authorization of the 3GPP subscriber based on the WLAN access authorization information retrieved from HLR/HSS.

Editor's note: Figure 1 in Annex B shows the WLAN access control model applicable to 3GPP WLAN IW. Figures 2 and 3 in Annex B show the Network Selection model applicable to this specification.

Other functionalities of the 3GPP AAA server are covered in 3GPP TS 29.234 [3].

4.2 WLAN UE Identities

4.2.1 General

WLAN UEs use Network Access Identifier (NAI) as identification towards the 3GPP WLAN AAA server. The NAI is structured according to RFC 2486 [10A]. The NAI realm shall be in the form of a domain name as specified in

RFC 1035 [7], the NAI username shall comply with draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10].

4.2.2 Root NAI

This is the NAI format when the WLAN UE authenticates directly to HPLMN (see draft-adrangi-eap-network-discovery-and-selection-00 [18] and TS 23.234 [2])

Editor's note: CN1 believe that the specification of the NAI should appear in 23.003, and therefore this subclause will reference that specification. The following text represents material that has been extracted from a past version of 23.234 and could form the basis of some material of 23.003.

The WLAN shall derive the NAI realm from a PLMN_ID as described in the following steps:

- 1. To retrieve the PLMN ID from the IMSI take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [6A]) 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.*

4.2.3 Decorated NAI

This is the NAI format when the WLAN authenticates to HPLMN via VPLMN (see draft-adrangi-eap-network-discovery-and-selection-00 [18])

Upon reception of network advertisement information from the WLAN, the WLAN UE identifies that WLAN PLMN selection shall be performed as specified in subclause 5.3. In this case, the WLAN UE shall decorate the NAI using the identity of the selected PLMN as specified below.

Editor's Note: NAI construction in this scenario is FFS and depends on current discussions in SA2.

5 UE to WLAN protocols

5.1 WLAN protocols

User and control plane traffic from and to UE has to be transported over the WLAN hop.

5.2 3GPP WLAN selection

5.2.1 Case of IEEE 802.11 WLANs

In the case of IEEE 802.11 WLANs, the WLAN network name is provided in the WLAN beacon signal in the SSID information element. There may be also the possibility for a UE to actively solicit support for a specific SSID by probing it and receiving a reply in case the access point would support it as defined in IEEE 802.11-1999 [11]

The UE listens to the selected SSIDs in the beacons signal or probes for them. The UE shall go through different steps until the WLAN selection is performed. The parameter used to perform the WLAN selection is the SSID.

1. By default, a pre-configured SSID shall be used for WLAN selection.
 - Primarily, it should be checked whether the preconfigured SSID is available in the beacon signal. If not, and if the WLAN UE supports de active mode the preconfigured SSID should be probed
 - If the previous does not succeed, the process should be moved to step 2
2. The I-WLAN SSID (defined in Clause 7) shall be used.
 - Primarily, it should be checked whether the I-WLAN SSID is available in the beacon signal. If not, and if the WLAN UE supports de active mode the preconfigured SSID should be probed
 - If the previous does not succeed, the process should be moved to step 3
3. The UE may try to authenticate in the available SSIDs in the beacon signals.

Editors Note: Radio network selection is currently defined in TS 23.234 [2]. Though, further details should be placed in this TS.

5.3 3GPP WLAN PLMN Selection

5.3.1 General

Editor's Note: Covers how WLAN UE performs WLAN PLMN selection.

The WLAN UE identifies itself to the WLAN by inserting its NAI in EAP-Response/Identity message. In the case when the WLAN cannot derive the 3GPP AAA Server or Proxy where to route the UE's EAP authentication signalling to, it is said that the WLAN has no direct roaming relationship with the user's home network.

WLAN uses realm part of NAI to route EAP authentication signalling to the Home 3GPP AAA server of the subscriber with whom the WLAN UE performs authentication. This procedure is out of the scope of this specification.

In the first EAP-Response/Identity message, the WLAN UE shall build the realm part of NAI in a way that it identifies the HPLMN.

Editor's note: the above sentence may need to be modified according to SA2's discussions on whether VPLMN ID can also be used in initial identification (i.e. whether Decorated NAI can be included in initial EAP-Response/Identity message).

If the WLAN can derive the 3GPP AAA server by using the realm, then there is no special processing in the UE for network selection and the WLAN just forwards the EAP authentication signalling to the 3GPP AAA server.

If the WLAN cannot derive the 3GPP AAA server by using the realm, then there is a need to WLAN PLMN selection in the UE. In this case the WLAN UE receives 'Supported PLMNs list' containing the PLMN IDs of the WLAN provider's roaming partners.

Upon reception of the 'Supported PLMNs list' in a FFS message (see draft-adrangi-eap-network-discovery-and-selection-00 [18]), the WLAN UE shall perform WLAN PLMN selection as as specified in 5.3.3.

5.3.2 Network Advertisement

5.3.2.1 UE procedures

Upon reception of a FFS message (see draft-adrangi-eap-network-discovery-and-selection-00 [18]) including the list of Supported PLMNs the WLAN UE shall:

- Perform WLAN PLMN selection according to 5.3.3
- Decorate NAI as specified in clause 4.2 and using the PLMN ID of the Selected PLMN
- Attempt to authenticate as specified in clause 6.1.1 and using the NAI determined in the prior step

If the Selected PLMN is HPLMN, then decoration is not necessary as HPLMN ID is already contained in the root NAI.

Editor's note: the possibility of using the Decorated NAI (i.e. the NAI decorated using VPLMN ID) at initial identification, is still under discussion in SA2. If agreed, this option will be added to clause 6.1.

Editor's note: A new draft, "Network Discovery and Selection within the EAP Framework"[18], has been submitted to IETF for network discovery and selection using EAP signalling. This TS is at the moment consistent with the recommendations included in this draft. Further changes are needed when the different options in the draft have been evaluated and after SA2's discussions on NAI decoration are completed.

The draft includes two options for Network discovery information transfer:

- to push the Supported PLMNs list to the UE in the 1st Identity_request message. The UE decides whether to respond with Decorated NAI or Root NAI
- to push the Supported PLMN list to the UE in a subsequent Identity_request message. The UE will use the Decorated NAI

5.3.3 Network selection

5.3.3.1 UE procedures

Upon successful completion of WLAN selection the WLAN UE may need to select a PLMN through which to authenticate, if more than one was available behind the chosen radio network.

The WLAN UE shall perform WLAN PLMN selection only after successful WLAN selection. WLAN PLMN selection procedure is completely independent of the result of the PLMN selection under other radio access technologies as specified in TS 23.122 [3].

The selection of PLMNs within different radio access technologies than WLAN, is not part of WLAN PLMN selection procedure.

The signal quality shall not be used as a parameter of WLAN PLMN selection.

Editor's note: the selection is done in two steps - first WLAN and then PLMN. Once WLAN is selected then all PLMNs are received with the same signal quality.

Editor's Note: The format of the list of supported PLMNs and transport of the list from WLAN to the WLAN UE are FFS.

5.3.3.1.1 Automatic Network Selection Mode Procedure

The WLAN UE shall select and attempt to authenticate with a PLMN, in the following order:

- i) HPLMN;
- ii) PLMNs in the "User Controlled PLMN Selector for WLAN access " data field in the WLAN UE (in priority order
- iii) PLMNs in the "Operator Controlled PLMN Selector for WLAN access ",if available, data field in the WLAN UE (in priority order);

Editor's note: bullet iii may require changes to 31.102

Editor's note: the term WLAN UE is temporal in the TS until SA1 gives an indication of whether the list in iii shall be stored in the USIM or in the UE.

Editor's note: it is FFS what should be the behaviour of the WLAN UE when no suitable PLMN (according to the selection criteria above) is found.

If successful authentication is achieved, the WLAN UE shall indicate to the user the Selected PLMN.

5.3.3.1.2 Manual Network Selection Mode Procedure

The WLAN UE shall indicate to the user the PLMNs which are available, using as a basis the Supported PLMNs list received from WLAN AN.

If displayed, PLMNs from the Supported PLMNs list shall be presented in the following order:

- i) HPLMN;
- ii) PLMNs in the "User Controlled PLMN Selector for WLAN access" data field in the WLAN UE (in priority order);
- iii) PLMNs in the "Operator Controlled PLMN Selector for WLAN access " data field in the WLAN UE (in priority order);

Editor's note: bullet iii may require changes to 31.102.

Editor's note: the term WLAN UE is temporal in the TS until SA1 gives an indication of whether the list in iii shall be stored in the USIM or in the UE.

Editor's note: it is FFS what should be the behaviour of the WLAN UE when no suitable PLMN (according to the selection criteria above) is found.

If a PLMN was selected before the procedure and if the user does not select a PLMN, the selected PLMN shall be the one that was selected before the PLMN selection procedure started.

If successful authentication is achieved, the WLAN UE shall indicate the selected PLMN.

5.3.3.1.3 Other Automatic Network Selection Mode Procedures

The support of other additional automatic network selection modes is implementation specific.

5.4 List of forbidden PLMNs for WLAN access

The WLAN UE shall contain a list of "Forbidden PLMNs for WLAN access". The list shall be removed at switch off. The list is defined in clause 7.3.

The WLAN UE shall not use the "Forbidden PLMNs for WLAN access" available from other accesses for WLAN PLMN selection nor Authentication procedures.

Upon reception of an EAP-Failure message in response to an EAP-Response/Identity message, the WLAN UE shall add the PLMN identity (which was used to decorate the NAI in EAP-Response/Identity) to the list.

Editor's note: there is no such an error cause in EAP-Authentication as 'WLAN services not allowed in this PLMN' only Authentication failure. The AAA server always handles the authentication and it is at home. The only possibility would be that the AAA proxy is not willing to give service (all PLMNs in network advertisement information are forbidden to the user).

6 UE to 3GPP Network protocols

6.1 UE to 3GPP AAA Server protocols

6.1.1 WLAN Access Authentication and Authorization protocols

Editor's Note: Functionality in WLAN UE and 3GPP AAA server for identification, full authentication and re-authentication. Procedures are defined in [9] and [10]. This TS should specify the mandatory and optional features from SIM and AKA drafts. As an example Reauthentication and Privacy support are optional in the EAP- SIM and EAP-AKA drafts but mandatory for 3GPP I-WLAN UE and network.

WLAN authentication signalling shall be executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and enabling the access to the WLAN network or to the WLAN and 3GPP network.

The WLAN UE and 3GPP AAA server shall support EAP authentication procedures as specified in draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10].

Other EAP authentication methods than those specified in [13] and [14] may be supported by the WLAN UE but are not part of 3GPP WLAN IW therefore are out of the scope of this specification.

WLAN authentication signalling for 3GPP-WLAN interworking shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 2284 [6].

WLAN access authorization shall be performed upon successful user authentication in the 3GPP AAA Server and it includes access rules as defined by the operator (see clause 6.1.1.3).

6.1.1.1 UE procedures

6.1.1.1.1 User Identity Privacy

In both EAPAKA and EAP SIM based authentications, the support of user identity privacy is mandatory for the WLAN UE. However, the usage of user identity privacy is optional for the UE.

By default, user identity privacy should be enabled. If user identity privacy is enabled and if the WLAN UE receives a temporary identifier (pseudonym) from the 3GPP AAA server (as specified in the EAP SIM [14] and EAP AKA [13] specifications), then the WLAN UE shall use the temporary identifier in the next full authentication.

6.1.1.1.2 EAP AKA Authentication

WLAN UE with USIM inserted shall support EAP AKA based authentication. If the WLAN UE supports both methods then it shall attempt to authenticate using EAP AKA authentication as the first EAP method. The UE shall be able to accept EAP AKA based authentication in the EAP method negotiation.

6.1.1.1.3 EAP SIM based Authentication

If WLAN UE supports SIM and SIM has been inserted, then the WLAN UE shall support EAP SIM based authentication. In this case, the UE shall be able to accept EAP SIM based authentication as EAP method negotiation.

Editor's note: It is FFS whether the UE accepts EAP SIM based authentication when a UICC with USIM has been inserted

6.1.1.1.4 Re-authentication

In both EAP AKA and EAP SIM based authentication, the support of re-authentication is mandatory for the WLAN UE.

By default, re-authentication should be enabled. If re-authentication is enabled and if the WLAN UE receives a re-authentication identity from the 3GPP AAA server (as specified in the EAP SIM [14] and EAP AKA [13] specifications), then the UE shall store the information required for re-authentication and use the re-authentication identifier in the next EAP authentication.

6.1.1.2 3GPP AAA Server procedures

6.1.1.2.1 User Identity Privacy

The 3GPP AAA server shall support identity privacy, as specified in EAP SIM and EAP AKA. The 3GPP AAA server shall send a new encrypted temporary identifier to the UE in every full authentication procedure. The details of temporary identity management are specified in TS 33.234 [7].

6.1.1.2.2 EAP SIM and EAP AKA based Authentication

The 3GPP AAA server shall support both EAP SIM and EAP AKA based authentication as specified in the EAP SIM [14] and EAP AKA [13] specifications.

6.1.1.2.3 3GPP AAA Server Operation in the Beginning of Authentication

The 3GPP AAA server shall support EAP method negotiation, as specified in EAP RFC 2284 [8].

By default, the 3GPP AAA server shall propose EAP AKA as the first authentication method in EAP method negotiation. However, the following factors may influence the choice of the first authentication method the 3GPP AAA server proposes:

- 1) The format of the identity received in EAP-Response/Identity, if present. If the identity format indicates EAP SIM, then the 3GPP AAA server may propose EAP SIM as the first authentication method. For example, if the leading character in the identity is "1", the identity might be a permanent IMSI-based identity for EAP SIM. The permanent identity format is specified in EAP SIM [14] and EAP AKA [13]. The format of the pseudonyms and re-authentication identities are specified in TS 33.234 [7].
- 2) If the 3GPP AAA server is able to map the identity received in EAP-Response/Identity to a subscriber identity (IMSI), and if the 3GPP AAA server has available information that the subscriber's UICC only supports SIM based authentication, for example due to (previously) received authentication vectors (triplets rather than quintuplets), then the 3GPP AAA server may propose EAP SIM as the first authentication method.

Details of identity management and the usage of various user identities is specified in EAP SIM [14] and EAP AKA [13]. The 3GPP AAA server shall always (re)request the user identity using EAP SIM or EAP AKA mechanisms in order to ensure that it has an unmodified copy of the identity, regardless of the identity the 3GPP AAA server received in EAP-Response/Identity (see EAP SIM [14] and EAP AKA [13] for details on this requirement).

Editor's note: it is FFS whether 3GPP AAA server accepts EAP-SIM based authentication for subscribers that have USIM

6.1.1.2.4 Re-authentication

The 3GPP AAA server shall support re-authentication as specified in the EAP SIM [14] and EAP AKA [13] specifications. The usage of re-authentication is optional for the 3GPP AAA Server and defined by the home operator.

WLAN Access Authorization between the UE and the 3GPP AAA Server shall be combined with the WLAN Access Authentication and performed before service authorisation and transport IP address allocation.

The 3GPP AAA Server shall perform access authorization once user authentication succeeds but before sending EAP-Success message to the WLAN UE.

The 3GPP AAA Server shall check whether the user is allowed to use WLAN service based on the user's subscription. If the check is successful the 3GPP AAA Server shall complete the authentication procedure by sending a positive response to the WLAN UE, that is a EAP-Success message.

Additionally, the 3GPP AAA Server may apply certain access control rules (such as access scope limitation, time limitation, bandwidth control values, and/or user priority) based on user's subscription, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements.

7 List of parameters

7.1 PLMN List

Editor's Note: it is FFS whether the format of PLMN list IE as specified in TS 24.008 can be re-used in this specification.

7.2 I-WLAN SSID

Annex <A> (normative):
<Normative annex title>

Annex (informative):
Figures applicable to 3GPP WLAN IW model

Editor's note: these figures are for information and will be removed from the Annex in the future whenif they are no longer needed.

The Access Control Reference model for 3GPP WLAN IW is illustrated in Figure 1. The generic Network Advertising and Selection scenario is illustrated in Figures 2 and 3.

Access Control Reference Model

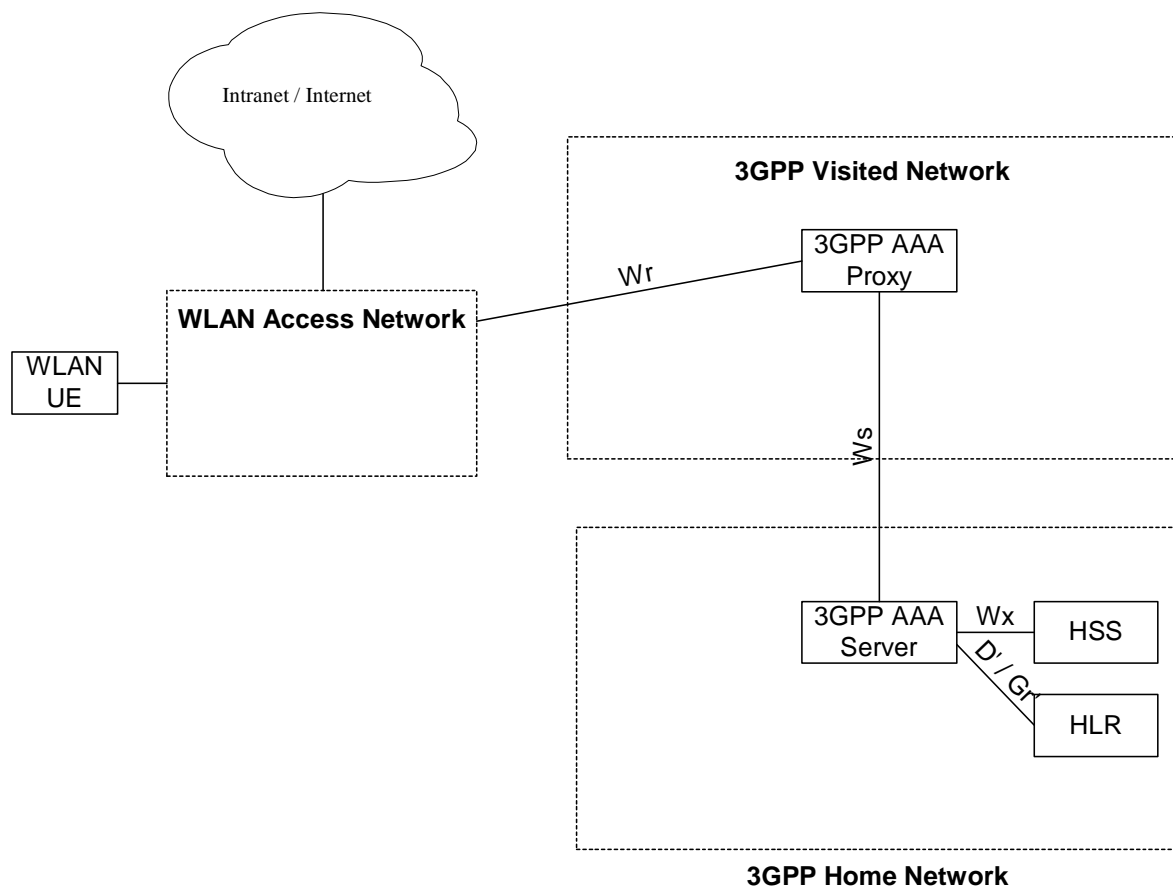


Figure 1 Access Control Reference Model

Network Advertising and Selection

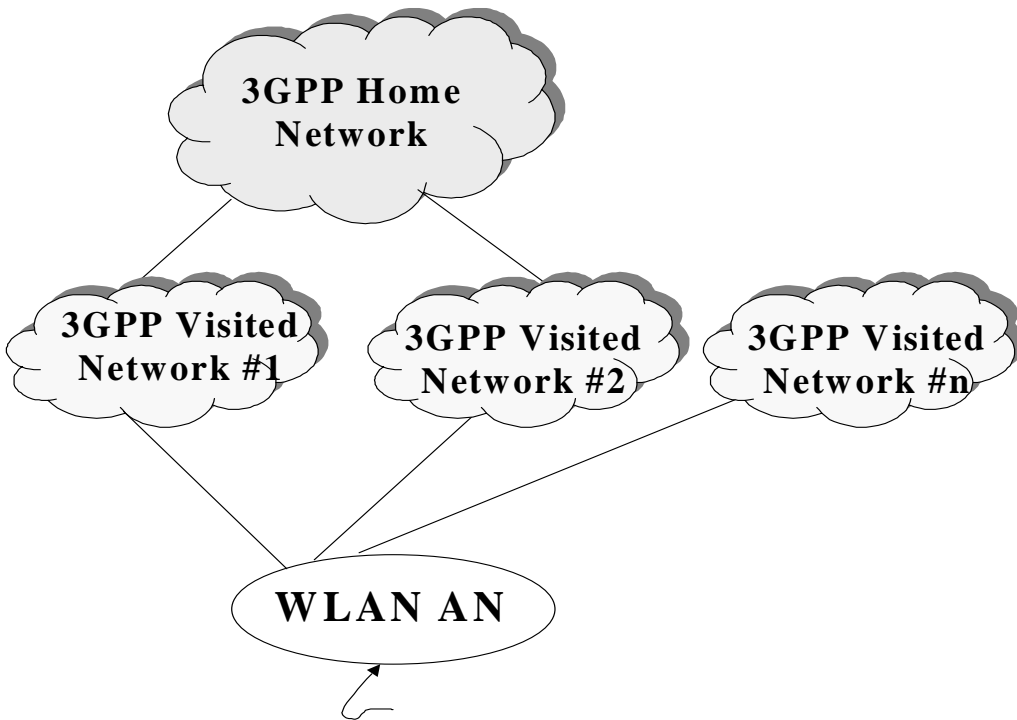


Figure 2 Network Advertising and Selection Scenario

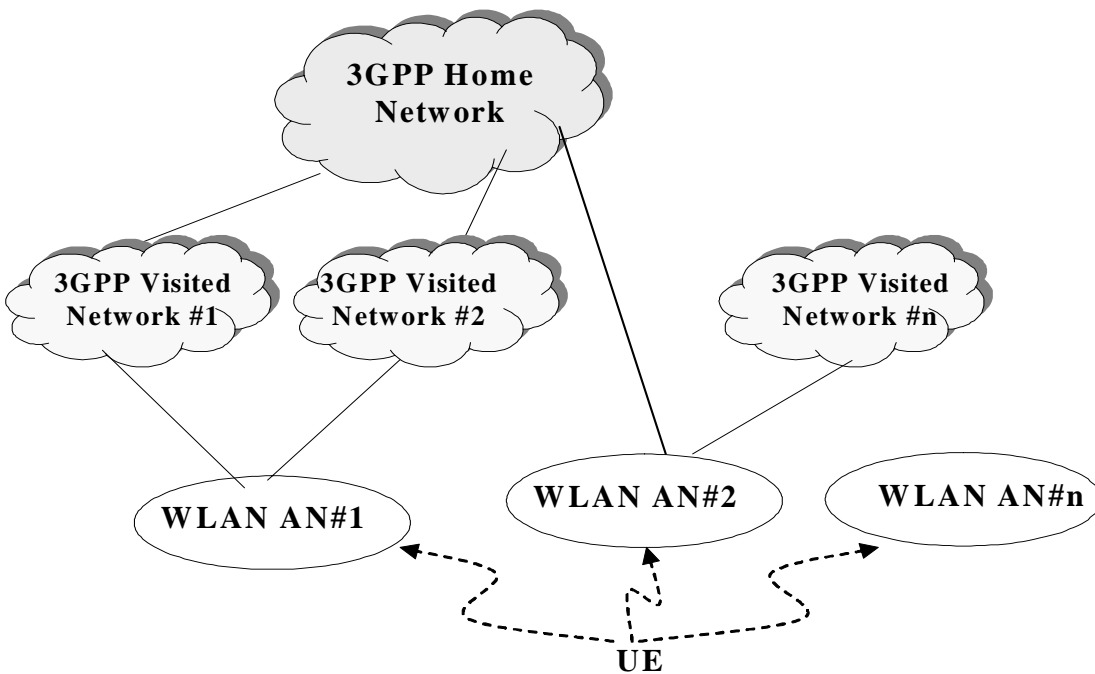


Figure 3 Network Advertising and Selection Scenario

Bibliography

The Bibliography is optional. If it exists, it shall follow the last annex in the document.

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

Bibliography format

- <Publication>: "<Title>".

OR

<Publication>: "<Title>".

Annex <X> (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
22.09.03	CN1#31				First draft. TS number assigned by MCC. Incorporates agreements from the following Tdocs: N1-031104, N1-031305, N1-031306, N1-031308, N1-031309 and N1-031310.		0.1.0
12.11.03	CN1#32	24.234			Second draft. TS sent to plenary for information. Incorporates agreements from the following Tdocs: N1-031536, N1-031685, N1-031686, N1-031691, N1-031692, N1-031693, N1-031694, N1-031695, N1-031696	0.1.0	0.2.0