ETSI TR 122 937 V11.0.0 (2012-10)

Universal Mobile Telecommunications System (UMTS);
LTE;
Requirements for service continuity between mobile and Wireless Local Area Network (WLAN) networks
(3GPP TR 22.937 version 11.0.0 Release 11)

Reference
RTR/TSGS-0122937vb00

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

For Fixed-Mobile Convergence (FMC), some scenarios require seamless roaming between a GSM/GPRS/3G mobile network and a WLAN. Both networks may be independently authenticated. To maintain the quality of the customer experience, and due to the difference of networks, handovers to support service continuity may require that the handset is authenticated to both networks simultaneously, for relatively short periods of time.

The objective of the present document is therefore to determine the requirements for seamless roaming and service continuity between a GSM/GPRS/3G mobile network and a WLAN.

An example of a use case for such a study could be where the user, on his way to the office, is having a call on a 3GPP access network using his mobile phone. He then roams onto his office WLAN (and vice versa), while still being on the line and the call is transferred without the user noticing any interruption to the network served by the WLAN..

1 Scope

The present document develops the use cases and requirements for service continuity between a 3GPP network and another network, which can be:

- a TISPAN NGN with an IMS, accessed by a WLAN.

- an ISP accessed via a WLAN

Each access network has its own separate security system and the NOs have a commercial agreement for roaming and handover.

The present document considers use cases whereby:

Editors Note: Text to be added when use cases are agreed

The present document also examines the requirements and implications of:

- service aspects: maintaining service quality and service continuity, while roaming between a 3GPP PLMN and an independently-owned WLAN;

- security aspects: while roaming between a 3GPP PLMN and a WLAN, in particular when networks may be independently authenticated.

- UICC aspects, including NAA types, personalisation and ownership.

The present document is related to ongoing standardisation efforts in the following areas:

- where the WLAN is an I-WLAN , requirements for which are described in [3];

- methods for selecting the 3GPP or the non-3GPP access network, requirements for which are described in [2].

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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 22.912: "Study into network selection requirements for non-3GPP access".

[3] 3GPP TS22.234: " Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[4] 3GPP TS 22.011: "Service accessibility".

[5] ETSI TS 102 310: "Smart Cards; Extensible Authentication Protocol support in the UICC".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Credentials: Data objects which are used to uniquely identify a subscriber and which are used in security procedures. For example, in the case of a USIM the credentials are IMSI and shared-secret Ki. The Milenage customisation parameter OPc can also be regarded also a credential, since it is derived from the Ki and is usually provisioned with the Ki.

Credential-Attach: This is a procedure whereby a credential is used to identify and authenticate a UE and to enrol it in a session with a network or subsystem.

Primary NO: The Network Operator which has the commercial relationship with the subscriber and is responsible for billing the subscriber.

Secondary NO: A Network Operator that has a commercial relationship with the Primary Network Operator by which the SNO provides services to subscribers of the PNO. The relationship could support the seamless handover of services to and from the PNO.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AAA	Authentication, Authorisation, Accounting
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EPS	Evolved Packet System
FMC	Fixed-Mobile Convergence
FMCA	Fixed-Mobile Convergence Alliance
GNAA	Generic Network Access Application (not supported on the UICC)
NAA	Network Access Application (on the UICC)
PNM	Personal Network Management
PNO	Primary Network Operator
SNO	Secondary Network Operator
VCC	Voice Call Continuity

4 Use Cases

4.1 General requirements

The subscriber possesses an UE which gives access to WLAN and 3GPP and access networks.

The UE shall support functionality to support service continuity when performing handover between the access networks to which it allows access.

Handover between networks shall be transparent to the user.

4.2 Use Case 1

4.2.1 Description

Alice is a subscriber whose PNO provides her with home connectivity to DSL via technologies including WLAN. The PNO also provides her with seamless access to its public WLANs and those of its roaming partners. The PNO is a member of the WiFi Alliance and its infrastructure requires the UE to support EAP-SIM for secure access.

The PNO also provides Alice with seamless access to the mobile networks of a SNO and its roaming partners. Her PNO's network uses its own AAA infrastructure, which was in place before the PNO formed the commercial relationship with its current SNO.

The PNO may also provide Alice with multimedia services through an IMS

Alice is at home. She wishes to have an Internet multimedia session on her hand-held dual-mode UE.

She switches on the UE and it automatically obtains a secure connection (authenticated and encrypted) to the WLAN of her WLAN provider – that being the default network when she is at home. She then connects to the desired Internet multimedia service. If that service is part of the PNO's IMS, the UE establishes a secure session with the IMS, and then identifies which public user identities Alice wants to use.

Alice needs to undertake a journey to a location in a different town but she wants to carry on with her Internet and/or IMS multimedia session during the journey. She gets into a taxi, which sets off towards a local rail station.

Within a few seconds, the taxi approaches the limit of Alice's home WLAN coverage. The UE, which is in automatic network selection mode, connects to the 3GPP mobile network of the SNO and drops the PNO's WLAN connection. Alice does not have to enter a username or password or PIN for the handover. Alice can see on the UE that the current network has changed, but the identity of the SNO is not visible to her. As far as she is aware, network service is always provided by her PNO. The Internet and/or IMS multimedia session continues uninterrupted.

When the taxi approaches the station, the UE comes within range of a public WLAN hotspot of Alice's PNO (or a roaming partner). Alice's PNO prefers that Internet and/or IMS access is provided over WLAN rather than the 3GPP network, so the UE automatically moves the Internet and/or IMS multimedia session to the WLAN.. Again, the UE indicates that the network has changed, but Alice is otherwise unaware of the change in Network Operator.

As the train leaves the station, the UE detects a fall in WLAN signal, and so re-establishes the 3G connection and then drops the WLAN connection.

Alice knows from previous experience that as she stops at various stations along the way, or passes slowly though them, her UE will try to connect to the WLAN hotspots at those stations. She decides that her user experience would be more consistent if she remained connected to the 3GPP network for the duration of the train journey. So, she uses the "User Preferred" menu function on the UE to select the "3GPP Preferred" option for the duration of her train journey.

When Alice reaches the destination town, she knows that she can get handover with service continuity between WLAN hotspots along the walk to her office building, so she decides to set the UE to "WLAN Preferred" for the duration of that journey. Alternatively, she could have switched the UE back to automatic network selection mode.

When Alice reaches her final destination (her employer's office building), she transfers to an Enterprise WLAN, from the current network. Access to the Enterprise WLAN can be done under the same PNO subscription, as it supports secure access to the Enterprise WLAN in addition to the public WLANs and 3GPP networks.

The handover between different networks can happen several times as Alice walks to her destination.

For this service, Alice receives a single bill, i.e. from the primary NO.

4.2.2 Requirements

Security and authentication

The UE shall be capable of connecting to the PNO's non-3GPP CN via a WLAN in a secure way using the appropriate security and authentication mechanisms for that network.

Note: the SNO network could be considered an IP-CAN

Note: the WLAN is not an I-WLAN in this use case.

The UE shall be capable of connecting to the SNO's 3GPP network according to 3GPP security and authentication requirements.

The UE shall be capable of connecting to the Enterprise WLAN in a secure way using the appropriate security and authentication mechanisms for that network.

The UE may be capable of connecting to the PNO's IMS network according to IMS security and authentication requirements.

Network selection/steering

Note: network selection/steering between the PNO's public WLAN and the Enterprise WLAN is out of scope, because both are non-3GPP networks. The requirements below apply only where either the target network or current network is a SNO's 3GPP network

The UE shall be able to select a target network and to hand over from the current network to the target network in mid-session while maintaining service continuity. This shall apply whether the UE is in automatic network selection mode or in user-preferred mode.

When the UE is in user-preferred mode, it may be directed by the user to select only available 3GPP networks or only available WLANs. At any time during user-preferred mode, if operation in that mode would result in loss of connectivity, e.g. due to non-availability of the selected network type, the UE shall be able to automatically revert to automatic mode until the user-preferred mode again becomes possible. The user shall be informed of the suspension and later resumption of user-preferred mode.

The UE shall be able to select and register to the target network in idle mode. Requirements for this are described in [2] and [4]

The UE shall contain policies that allow it to decide automatically to which network to initially attach, when multiple networks are available.

The PNO shall be capable of controlling and setting the UE policies related to initial attachment for network selection.

The PNO shall be capable of steering the UE to use the most appropriate network.

The PNO shall be capable of steering the UE by means of static policy (i.e. by use of a local policy), whether the UE is involved in an active session or not.

The PNO shall be capable of steering the UE by means of dynamic policy (i.e. using real-time instructions from the PNO) related to the AN capabilities (e.g. coverage, load, etc) and PNO preferences, whether the UE is involved in an active session or not.

Charging

The PNO shall be aware of the status of the UE with respect to the network attachment.

The SNO shall be capable of generating CDRs for the type of access network used by the subscriber and of providing those CDRs to the PNO.

The PNO shall be capable of charging the subscriber according to the type of access network used in its own network.

The PNO shall be capable of billing the subscriber according to the type of access network used in its own network and the SNO's network.

The PNO shall be capable of indicating to the SNO to block/enable the subscriber's access network in real time for reasons concerned with charging (e.g. subscriber's credit has expired), when using the SNO's network.

The SNO shall be capable of blocking/enabling the subscriber according to the type of access network used in its own network, when indicated by the PNO.

Mobility

Note: Service continuity between the Enterprise WLAN and the public WLAN is out of scope, because both are non-3GPP networks.

It shall be possible to support service continuity of the multimedia session, including the IMS session, if used, from the WLAN to the 3GPP network and vice-versa.

Independently from the service continuity to the final user, the UE shall be capable of providing information to the user regarding the current type of access network used.

QoS

Note: QoS considerations when handing over between the Enterprise WLAN and the public WLAN are out of scope, because both are non-3GPP networks.

The ability to maintain service continuity when changing networks shall be dependent on the QoS capabilities of the target network:

It shall be possible to release the session on the change of network if the target network does not provide adequate QoS.

When a network-change event is triggered, it shall be possible to reject that change of network if the target network does not provide a QoS that is appropriate for the service currently being accessed. However, the change of network shall not be rejected if that rejection would result in the subscriber losing all network connectivity , for example if the change is triggered by impending non-availability of the current network.

The service platform may adapt the service (e.g. degrade or enhance the service) to the capability of the target access.

It shall be possible to inform the user if the change of network is rejected or if it is allowed but the service session is lost or degraded due to the change of network.

User Identity

The PNO may provide the subscriber with a unique public identity for use on the multiple access networks of the primary and SNOs.

The PNO may provide the subscriber with multiple public identities.

Any other identifier provided by the PNO or the SNO should not be visible to the user.

4.2.3 Analysis

Seamless Mobility

This use case requires the use of different sets of credentials to access the 3GPP AN/CN and the WLAN/non-3GPP CN. Service continuity of the IP-based service, which may be part of the PNO’s IMS, must be maintained, within the limitations of QoS, etc. If considerations of service continuity require a "make-before-break" process, the UE will need to establish credential-attach to the target network before credential-attach to the current network can be released. This simultaneous credential-attach may only be required temporarily until the handover is successfully completed. Nevertheless, it may have implications on the functionality of the UICC, which are discussed elsewhere in this section (e.g. the simultaneous activation of two USIMs, which is currently prohibited by 3GPP specifications). It also has implications on the design of the UE, e.g. radio technology and battery life.

Authentication

General:

There may be a need to relax the existing Rel-8 requirements on charging, QoS and mobility, while making the existing security and trust requirements stronger.

SNO's 3GPP Network:

This network will be accessed using a USIM on the UICC. The USIM will be personalised with a set of credentials determined by the SNO.

PNO's WLAN/non-3GPP CN:

The non-3GPP CN is a TISPAN NGN with an IMS (the IMS may be invoked in this use case), or ISP accessed by a WLAN.

If handover with service continuity in requires a "make before break" process, then the NAAs or GNAAs that are used to achieve credential-attach to each network would need to be active simultaneously for at least the duration of the handover operation. Furthermore, the requirement for independent authentication and authorisation of the PNO's and SNO's networks requires the WLAN/non-3GPP CN to be accessed using a set of credentials that is independent of that used to access the 3GPP network. Possible approaches to this problem are discussed below.

Use of EAP-SIM is described in this use case, for automatic access to WLANs. It is especially suitable for WLAN roaming. EAP-SIM permits the WLAN NO to take advantage of the many available products and systems that are certified by the W-Fi Alliance. The fast re-authentication function is especially suitable for frequent and automatic handover between WLAN and 3GPP networks.

An EAP application on the UICC [5] could be used to support EAP-SIM and other standardised EAP methods. [5] stipulates that the EAP application must be located under a top-level application on the UICC. That could be an ISIM application, i.e. the ISIM application that is required for access to the PNO's IMS.. With this solution, even if the UE did not support IMS, it would still be necessary for it to select the ISIM. This should not be a problem, as the selection method for ISIM and USIM are the same.

An EAP application on the UICC [5] could be located under the SNO's USIM on the UICC, given agreement between the SNO and PNO. The USIM and EAP application would have to use different credentials and possibly different algorithm customisations. This solution would cause a problem if the SNO needed to have its own EAP application under the same USIM.

A PNO-personalised ISIM alone, i.e. without the underlying EAP application on the UICC, could support EAP-AKA, provided the EAP supplicant could select the ISIM application. However, an ISIM cannot currently support EAP-SIM, since it does not currently support authentication in GSM security context.

EAP-SIM could be supported from a SIM or USIM on the UICC. In this use case, such a (U)SIM would have to be personalised with credentials for the PNO's HSS, since the PNO's and SNO's networks are fully independent, i.e. the WLAN is not an I-WLAN. Furthermore, it would be necessary for the PNO's and SNO's (U)SIMs to be active simultaneously, if "make before break" is required for service continuity. However, the simultaneous activation of two USIMs on a UICC is currently prohibited by 3GPP specifications.

EAP-SIM could be supported from a new NAA that provides authentication functions which are identical to that of a USIM operating in GSM security context, but which could be specified by a WLAN-oriented organisation, e.g. the FMCA or the WiFi Alliance. Perhaps the WiSIM, proposed by some members of the WiMAX Forum, could be adopted or adapted. EFs (Elementary Files) for this NAA would typically be limited to those few required to support the authentication functions, thereby minimising concerns about "collisions" between files in this NAA and those in the (U)SIM. It would be up to the SNO and PNO to agree that the presence of this NAA on the UICC would not give rise to operational or security-related problems. If such problems could be addressed between 3GPP and the WLAN NAA's specifying body at the specification stage, then that would be more satisfactory than relying on ad-hoc agreements between PNOs and SNOs.

Use of a GNAA cannot currently support this use case, because EAP-SIM and EAP-AKA require the presence of a UICC in the UE. In future, however, GNAAs could include (U)SIM-like functions when UEs become available with embedded hardware functions capable of enforcing the required security policies and providing a secure execution environment.

GNAAs that utilise username/password, one-time password, certificates/private keys, etc., are out of scope of this us case and this study item, but they could be exploited in use cases where the PNO's WLAN and its WLAN roaming partners are not concerned with exploiting UICC-based applications.

Charging and billing

For the PNO to provide a unique bill to the user, it is necessary to provide adequate support for the charging information, e.g. to produce, exchange and manage the CDRs.

The PNO has the task to correlate and mediate the charging information (e.g. CDRs) to assure proper billing to the end user and proper payments to the SNO according to commercial contract.

If the solution can be based on standard roaming, all the features required for the identification of the user and the exchange of CDRs are already supported in current the 3GPP specifications, following the indication and procedures established by GSMA.

Initial network selection/steering:

For the SNO's 3GPP network, network selection shall be based on the existing 3GPP specification [4].

Network selection for WLAN could be based on appropriate UE local policy configuration, set by the PNO by means of UE configuration (e.g. OTA settings).

Steering with active connection could be based on many different criteria, such as radio quality, QoS supported, PNO and user priorities, etc.

As far as the requirement for automatic network selection, based on these criteria, is concerned it may need some additional specification.

QoS support

It is necessary to correctly manage the exchange of QoS information during the handover procedures.

4.3 Use Case 2

4.3.1 Description

This use case is the same as Use Case 1, with the following differences:

- The PNO is a 3GPP Network Operator and may provide also WLAN.
- The SNO provides WLAN.
- The PNO offers to Alice Pre-paid and Post-paid service subscription.

4.3.2 Requirements

Security and authentication

The UE shall be capable of connecting to the SNO's non-3GPP CN via a WLAN in a secure way using the appropriate security and authentication mechanisms for that network.

Note: the WLAN could be considered an IP-CAN

The UE shall be capable of connecting to the PNO's 3GPP network according to 3GPP security and authentication requirements.

The UE may be capable of connecting to the PNO's IMS according to IMS security and authentication requirements.

Network selection/steering

The UE shall contain policies that allow it to decide automatically which network to initially attach to, when multiple networks are available.

The PNO shall be capable of controlling and setting the UE policies related to initial attachment for network selection.

The PNO shall be capable of steering the UE to use the most appropriate network.

The PNO shall be capable of steering the UE by means of static policy (i.e. by use of a local policy) whether a UE is involved in active session or not.

The PNO shall be capable of steering the UE by means of dynamic policy (i.e. using real-time instructions from the PNO) related to the access network capabilities (e.g. coverage, load, and etc) and PNO preferences whether a UE is involved in active session or not.

Charging

The PNO shall be aware of the status of the UE with respect to the network attachment.

The SNO shall be capable of charging the subscriber according to the type of access network used.

The SNO shall be capable of providing on-line and off-line charging information to the PNO.

The PNO shall be capable of charging the subscriber according to the type of access networks used in its own networks.

The PNO shall be capable of indicating to the SNO to block/enable the subscriber's access network in real time for reasons concerned with charging (e.g. subscriber credit expired), when using the SNO's network.

The SNO shall be capable of blocking/enabling the subscriber according to the type of access network used in its own network, when indicated by the PNO.

The PNO shall be capable of blocking/enabling the subscriber to use the PNO network.

As a charging consequence, the PNO shall be capable of billing the subscriber according to the type of access network used in its own networks and in the SNOs network.

Mobility

It shall be possible to supportn service continuity of the multimedia session from the WLAN to the 3GPP network and vice-versa.

Independently from the service continuity to the end user, the UE shall be capable of providing information to the user regarding the current type of access network used.

QoS

The ability to maintain service continuity when changing networks shall be dependent on the QoS capabilities of the target network.

It shall be possible for the PNO to reject the change of network if the target network does not provide adequate QoS to maintain service continuity.

It shall be possible to release the session on the change of network if the target network does not provide adequate QoS to maintain service continuity.

The system may adapt the service (e.g. degrade or enhance the service) to the capability of the target access.

User identity

The PNO may provide the subscriber with a unique public identity for use on the multiple access networks of the primary and SNOs.

The PNO may provide the subscriber with multiple public identities.

Any other identifier provided by the PNO or the SNO should not be visible to the user.

4.3.3 Analysis

Authentication

Credential for IMS is the USIM or the ISIM.

Credential for the PNO's 3GPP network is the USIM

Credentials for the WLAN could be any kind of secure credential.

- In the case it is a USIM, 3GPP has already defined a solution, e.g. the I-WLAN [3], whereby the user is roaming in the SNO.
- For any other kind of secure credential (e.g. certificates, Login&PWD, etc.), the WLAN connectivity could be considered an IP-CAN to access the IMS

Initial network selection/Steering

In 3GPP Networks, network selection shall be based on the existing 3GPP specification [4].

Network selection for WLAN could be based on the I-WLAN specification [3], in the case where the I-WLAN approach is used to handover in the SNO's WLAN.

Network selection for non-3GPP WLAN could be based on appropriate UE local policy configuration, set by the PNO by means of UE configuration (e.g. OTA settings).

Steering with active connection could be based on many different criteria, such as radio quality, QoS supported, PNO and user priorities, etc.

As far as the requirement for automatic network selection, based on these criteria, is concerned it may need some additional specification.

Seamless Mobility

The ability to enable session continuity while the UE is moving between 3GPP network and non-3GPP WLAN could be based on different approaches.

If the session should be continued between a 3GPP network based on CS access and non-3GPP WLAN, anchoring the session in the PNO's IMS, as already defined in the VCC for the voice call, is a solution to be enhanced for multimedia. Extension of VCC for multimedia session continuity is under discussion in SA2.

If the session should be continued between a 3GPP network based on PS access and non-3GPP WLAN (assuring the appropriate performance for multimedia session), anchoring the session in the PNO's packet network is a solution under the work on EPS where mobility and session continuity between 3GPP access and non-3GPP IP-CAN are considered.

It has to be noted also that, in the case that the session should be continued inside a 3GPP network between the PS access and the I-WLAN access, anchoring the session in the 3GPP CN is a solution under study in SA2 in the WI "Feasibility Study of Mobility between 3GPP-WLAN Interworking and 3GPP Systems" which was approved at SA#35.

Charging and billing

For the PNO to provide a unique bill to the user, it is necessary to provide adequate support for the charging information, i.e. to produce, exchange and manage the CDRs.

The PNO has the task to correlate and mediate the charging information (e.g. CDRs) to assure proper billing to the end user and proper payments to the SNO according to commercial contract.

If the solution is based on standard roaming, all the features required for the identification of the user and the exchange of CDRs are already supported in current the 3GPP specifications, following the indication and procedures established by GSMA.

QoS support

It is necessary to correctly manage the exchange of QoS information during the handover procedure.

4.6 Use Case 3

4.6.1 Description

This the same as use case 1, except that when on the WLAN, Alice uses a VOIP service that is supported by a client on the UE. When handover to the 3GPP network occurs, the voice service switches to 3GPP CS voice service. This does not require Alice to have any manual input. Alice may be able to audibly detect the handover, e.g. by a very momentary interruption to voice contact, but she finds that quite acceptable for voice service.

4.6.2 Requirements

Security and authentication

The UE shall be capable of connecting to the PNO's non-3GPP CN via a WLAN in a secure way using the appropriate security and authentication mechanisms for that network.

Note: the WLAN is not an I-WLAN in this use case.

The UE shall be capable of connecting to the SNO's 3GPP network according to 3GPP security and authentication requirements.

The UE may be capable of connecting to the PNO's IMS network according to IMS security and authentication requirements.

Network selection/ steering

The UE shall be able to select a target network and to hand over from the current network to the target network in mid-session while maintaining service continuity.

The UE shall be able to select and register to a target network in idle mode. Requirements for this are described in [2] and [4]

The UE shall contain policies that allow it to decide automatically to which network to initially attach, when multiple networks are available.

The PNO shall be capable of controlling and setting the UE policies related to initial attachment for network selection.

The PNO shall be capable of steering the UE to use the most appropriate network.

The PNO shall be capable of steering the UE by means of static policy (i.e. by use of a local policy decision function), while the UE is not involved in any active session.

The PNO shall be capable of steering the UE by means of dynamic policy (i.e. using real-time instructions from the PNO) related to the AN capabilities (coverage, load, etc) and PNO preferences, while the UE is not involved in any active session.

The PNO shall be capable of steering the UE by means of static policy (e.g. preferred SNO's AN), while the UE is involved in an active session.

The PNO shall be capable of steering the UE by means of dynamic policy related to the AN capabilities (coverage, load, etc) and PNO preferences, while the UE is involved in an active session.

Charging

The PNO shall be aware of the status of the UE with respect to the network attachment.

The SNO shall be capable of generating CDRs for the type of access used by the subscriber and of providing those CDRs to the PNO.

The PNO shall be capable of charging the subscriber according to the type of access used in its own network .

The PNO shall be capable of billing the subscriber according to the type of access used in its own network and in the SNO’s network.

The PNO shall be capable of indicating to the SNO to block/enable the subscriber’s access in real time for reasons concerned with charging (e.g. subscriber’s credit has expired), when using the SNO’s network.

The SNO shall be capable of blocking/enabling the subscriber according to the type of access used in its own network, when indicated by the PNO.

Mobility

The system shall be capable of supporting service continuity of the voice session (including the IMS session, if used) from the WLAN to the 3GPP network and vice-versa.

Independently from the service continuity to the end user, the UE shall be capable of providing information to the user regarding the current type of access used.

The UE shall be capable of switching automatically between CS voice service and PS VOIP service, according to the current and target ANs.

QoS

In the case of voice session continuity, the ability to provide service continuity to the user when changing networks shall be dependent on the QoS capabilities of the target network:

It shall be possible to release the session on the change of network if the target network does not provide adequate QoS.

When a network-change event is triggered, it shall be possible to reject that change of network if the target network does not provide a QoS that is appropriate for the VOIP service currently being accessed. However, the change of network shall not be rejected if that rejection would result in the subscriber losing all network connectivity , for example if the change is triggered by impending non-availability of the current network.

It shall be possible to inform the user if the change of network is (a) rejected or (b) allowed but the VOIP session is lost or degraded due to the change of network.

User identity

The PNO may provide the subscriber with a unique public identity for use on the multiple networks of the PNO and SNOs.

The PNO may provide the subscriber with multiple public identities.

Any other identity, e.g. IMSI, IMPI, and etc, provided by the PNO or the SNO should not be visible to the user.

4.6.3 Analysis

Seamless mobility

The analysis in use case 1 applies without modification.

Authentication

The analysis in use case 1 applies without modification.

Charging and billing

The analysis in use case 1 applies without modification.

Network selection/steering

The analysis in use case 1 applies without modification.

QoS Support

It is necessary to correctly manage the exchange of QoS information during the handover process. The principal QoS consideration is the ability of the 3GPP network to provide CS voice service and the ability of the WLAN to provide effective VOIP service, which is relatively robust to variations in effective available bandwidth.

4.7 Use Case 4

4.7.1 Description

Alice is making a video call while walking in the city center on the 3GPP network of her PNO. At this moment Alice's PNO receives a large number of connection requests in the area, the number of requests being too many for the local cell to support. To be able to support the increase in requests, the PNO needs to divert part of the traffic. Fortunately, Alice is within range of a WLAN operated by the SNO that she can access and which can support video calls. The PNO then sends a message to Alice's UE to switch to the WLAN of the SNO so that other users not having WLAN capable handsets can connect to the 3G services.

4.7.2 Requirements

The UE should inform the user in case of automatic switch of network (e.g. display text, play a tone).

4.7.3 Analysis

Such a system switch has to be automatic, as the user is in a call and not aware of the traffic constraints.

It is understood that the automatic switch shall not occur if the preferences provisioned into the UICC are forbidding the automatic switch. In that case, the call will continue on the current network.

4.8 Use Case 5

4.8.1 Description

While registered to her 3GPP PNO, Alice is having a video call with her friend Jane while shopping. Unfortunately, the video call service is not able to be maintained and has to be downgraded to voice call. Reasons could be that Alice has moved out of the correct 3GPP coverage to continue the video call, or that an increase of call traffic in the area necessitates a temporary downgrade of the local QoS. By staying connected with the PNO, the call should automatically change into a voice call. Fortunately, Alice is within range of a WLAN operated by the SNO that she can access. So, instead of falling into voice mode, the UE switches to the WLAN and Alice is able to continue her video call, while showing the latest fashion clothes to Jane using her UE.

4.8.2 Requirements

It shall be possible for the 3GPP PNO to set preferences into the UICC concerning the automatic switch of system when QoS is downgraded (e.g. enable or disable).

It shall be possible for the user to set preferences into the UICC and/or into the ME concerning the automatic switch of system when QoS is downgraded (e.g. enable or disable), overriding the 3GPP PNO's preferences. If both sets of preferences are present, the one in the UICC shall take priority.

In case of loss of QoS, the UE shall automatically switch to the appropriate system, according to the preferences provisioned into the UICC or ME.

The UE should inform the user about the switch of network (e.g. display text, play a tone).

4.8.3 Analysis

Such a system switch has to be automatic, as the user is in a call.

Within this condition, it would be difficult for the user to continue the call while manually operating the switch of system.

It is understood that the automatic switch shall not occur if the preferences provisioned into the UICC or the ME are forbidding the automatic switch. In that case, the call will drop.

4.9 Use Case 6

4.9.1 Description

While registered to her WLAN PNO, Alice is having a video call with her friend Jane while shopping. Unfortunately, Alice moves out of WLAN coverage that is sufficient to ensure a correct data rate for a video call. By having its data rate reduced, the call should either drop or switch to voice mode, or dramatically reduce the video quality. Fortunately, Alice is under coverage of a 3GPP network operated by the SNO that she can access. So, instead of having a reduced service for the video call, the UE switches to the 3GPP network and Alice is able to continue her video call while showing the latest fashion clothes to Jane.

4.9.2 Requirements

It shall be possible for the WLAN PNO to set preferences into the UICC concerning the automatic switch of system when QoS is downgraded (e.g. enable or disable).

It shall be possible for the user to set preferences into the UICC and/or into the ME concerning the automatic switch of system when QoS is downgraded (e.g. enable or disable), overriding the WLAN PNO' preferences. If both sets of preferences are present, the one in the UICC shall take priority.

The UE shall automatically switch to the appropriate system, according to the preferences provisioned into the UICC or ME.

The UE should inform the user about the switch of network (e.g. display text, play a tone).

4.9.3 Analysis

Such a system switch has to be automatic, as the user is in a call.

Within this condition, it would be difficult for the user to continue the call while manually operating the switch of system.

It is understood that the automatic switch shall not occur if the preferences provisioned into the UICC or ME are forbidding the automatic switch. In that case, the call will either drop or continue with reduced quality.

4.10 Use Case 7

4.10.1 Description

This use case is the same as Use Case 1, with the following modification:

- The PNO is a non-3GPP Network Operator, provides I-WLAN access, IMS services
- The SNO is a 3GPP Network Operator and provides CS/PS mobile access
- The PNO have a commercial roaming agreement with the SNO that allows PNO users to roma into SNO mobile network
- The PNO provides the user with a USIM and optionally ISIM

4.10.2 Requirements

Security and authentication

The UE shall use USIM to authenticate to I-WLAN PNO and to SNO network.

The UE may use USIM or ISIM authenticate to the PNO's IMS.

Network selection/steering

The UE shall use I-WLAN procedure for the network selection and the steering in the PNO's network.

Charging

The network operator shall use 3GPP standard charging mechanism.

Mobility

It shall be possible to support service continuity of the multimedia session from the WLAN to the 3GPP network and vice-versa.

Independently from the service continuity to the end user, the UE shall be capable of providing information to the user regarding the current type of access used.

QoS

The ability to maintain service continuity when changing networks shall be dependent on the QoS capabilities of the target network.

It shall be possible for the PNO to reject the change of network if the target network does not provide adequate QoS to maintain service continuity.

It shall be possible to release the session on the change of network if the target network does not provide adequate QoS.

4.10.3 Analysis

Authentication

Credential for the I-WLAN is the USIM.

Credential for IMS is the USIM or the ISIM.

Credential for the SNO's 3GPP access network is the USIM of the PNO under a roaming agreement.

Initial network selection/Steering

In 3GPP Networks, network selection shall be based on the existing 3GPP specification [4].

Network selection for I-WLAN could be based on the I-WLAN specification [3].

Steering with active connection could be based on many different criteria, such as radio quality, QoS supported, PNO and user priorities, etc.

As far as the requirement for automatic network selection, based on these criteria, is concerned it may need some additional specification.

Seamless Mobility

The VCC Rel-8 needs additional requirement to support multimedia sessions to be applicable to this scenario

Charging and billing

For the PNO to provide a unique bill to the user, it is necessary to provide adequate support for the charging information, i.e. to produce, exchange and manage the CDRs.

The PNO has the task to correlate and mediate the charging information (e.g. CDRs) to assure proper billing to the end user and proper payments to the SNO according to commercial roaming contract.

If the solution is based on standard roaming, all the features required for the identification of the user and the exchange of CDRs are already supported in current the 3GPP specifications, following the indication and procedures established by GSMA.

QoS support

It is necessary to correctly manage the exchange of QoS information during the handover procedure.

5 Harmonized requirements

5.1 Service aspects

The system shall be capable of supporting multimedia, voice and internet session continuity from the WLAN access network to the 3GPP access network and vice-versa, where supported by considerations of QoS and where the NOs support compatible services. Voice session continuity includes the case where VOIP service is provided over the WLAN and CS voice service is provided over the 3GPP network.

The system shall be capable of assuring service continuity to the end user, when moving between WLAN access network and the 3GPP access network.

The PNO may provide the subscriber with a unique public identity for use on the multiple access networks of the primary and SNOs.

The PNO may provide the subscriber with multiple public identities.

Any other identifier provided by the PNO or the SNO should not be visible to the user.

Independently from the service continuity to the end user, the UE may be capable of providing information to the user regarding the current type of access used.

It shall be possible to release the session on the change of network if the target network does not provide adequate QoS.

When a network-change event is triggered, it shall be possible to reject that change of network if the target network does not provide a QoS that is appropriate for the service currently being accessed. However, the change of network shall not be rejected if that rejection would result in the subscriber losing all network connectivity , for example if the change is triggered by impending non-availability of the current network.

The service platform may adapt the service (e.g. degrade or enhance the service) to the capability of the target access.

It shall be possible to inform the user if the change of network is (a) rejected or (b) allowed but the service session is lost or degraded due to the change of network.

The UE shall contain policies that allow it to decide automatically to which network to initially attach, when multiple networks are available.

The UE shall be able to select and register to the target network in idle mode. Requirements for this are described in [2]

The UE shall be able to select a target network and to hand over from the current network to the target network in mid-session while maintaining service continuity. This shall apply whether the UE is in automatic network selection mode or in user-preferred mode. This shall apply regardless of in which CN the service session is anchored.

The user shall be able to switch the UE into user-preferred mode,. In that mode, the UE may be directed by the user to select only available 3GPP networks or only available WLANs. At any time during user-preferred mode, if operation in that mode would result in loss of connectivity, e.g. due to non-availability of the selected network type, the UE shall be able to automatically revert to automatic mode until the user-preferred mode again becomes possible. The user shall be informed of the suspension and later resumption of user-preferred mode.

A set of manageable criteria and functions, both automatic and manual, shall be provided for intelligent handover with service continuity between the PNO’s and SNO’s access networks

The PNO shall be capable of controlling and setting the UE policies related to initial attachment for network selection.

The PNO shall be capable of steering the UE to use the most appropriate network.

The PNO shall be capable of steering the UE by means of static policy (i.e. by use of a local policy decision function), while the UE is not involved in any active session.

The PNO shall be capable of steering the UE by means of dynamic policy (i.e. using real-time instructions from the PNO) related to the AN capabilities (coverage, load, etc) and PNO preferences, while the UE is not involved in any active session.

The PNO shall be capable of steering the UE by means of static policy (e.g. preferred SNO's AN), while the UE is involved in an active session.

The PNO shall be capable of steering the UE by means of dynamic policy related to the AN capabilities (coverage, load, etc) and PNO preferences, while the UE is involved in an active session.

Where the WLAN is an I-WLAN, the UE shall use I-WLAN procedure for the selection and the steering in the PNO network

Where both 3GPP (e.g. 3G) and the non-3GPP networks (e.g. WLAN) support access to an IMS, it shall be possible to access the IMS of at least the PNO seamlessly on all access networks that the user is allowed to access under his agreement with the PNO.

The PNO may provide the subscriber with a unique public identity for use on the multiple access networks of the PNO and SNOs.

The PNO may provide the subscriber with multiple public identities.

Other identifiers provided by the PNO or the SNO should not be visible to the user.

The UE shall support at least one method of access to the PLMN of the 3GPP NO. The NAA for that shall support AAA services to the HSS of that NO. It would normally be a USIM on a UICC.

TheUE shall support at least one method of access to the WLANs of an Enterprise and to the public WLANs of the WLAN NO.

The UE shall support the case where each type of network may require a separate NAA with its own credentials. In such a case, and where service continuity requires the handover between 3GPP networks and WLAN to be handled on a "make before break" basis, it shall be possible for both NAAs to be active simultaneously. This shall apply during the period of network handover.

Device Management settings are to be obtained from and controlled by the Primary NO.

5.2 Security aspects

The UE shall be capable of connecting to the non-3GPP CN via a WLAN in a secure way using the appropriate security and authentication mechanisms for that network. This applies if the non-3GPP CN and WLAN is operated by the PNO or by the SNO.

The UE shall be capable of connecting to the 3GPP CN via its RAN, according to 3GPP security and authentication requirements. This applies if the 3GPP CN/RAN is operated by the PNO or by the SNO.

Where required by the intended usage of the UE, the UE shall be capable of connecting to the Enterprise WLAN in a secure way using the appropriate security and authentication mechanisms for that network.

It shall be possible for the 3GPP NO and the WLAN NO to operate their own completely separate security systems, including independent authentication centres in their respective CNs.

The NAA(s) used for WLAN access shall include an application or applications to support EAP-SIM and EAP-AKA.

The UE may be capable of connecting to the PNO's IMS network according to IMS security and authentication requirements.

Where the WLAN is an I-WLAN, the following requirements apply:

The UE shall use a single USIM to authenticate to the I-WLAN and to the 3GPP network.

The UE may use USIM or ISIM to authenticate to the IMS of the PNO.

5.3 UICC aspects

The UICC shall be able to support separate NAAs for the 3GPP access and WLAN access, where the credentials in each NAA are different. This does not preclude support for the two networks using the same NAA, or for two NAAs with the same credentials.

The UICC shall support USIM and SIM for 3GPP network access.

The UICC shall support one or more NAA(s) for WLAN access that can be used for EAP-SIM and EAP-AKA.. The UICC should also support.

Where the UICC supports separate NAAs for 3GPP access and WLAN access, the UICC shall permit simultaneous sessions with both NAAs on different logical channels.

The UICC shall be capable of supporting an ISIM for secure access to the IMS of the PNO.

5.4 Charging aspects

A user shall be able to receive a single, itemised bill from the PNO covering use of both access-network types and IMS services and representing a single user identity (single phone number).

A user may opt to receive a single, itemised bill covering use of all access networks and IMS and representing multiple user identities, e.g. a private and a business identity. This covers the cases of a small business user who requires a split between personal and business use and where an Enterprise needs bills for its employees, split into personal and business use.

The PNO shall be aware of the status of the UE with respect to the network attachment.

The SNO shall be capable of generating CDRs for the type of access used by the subscriber and of providing those CDRs to the PNO.

The PNO shall be capable of charging the subscriber according to the type of access used in its own network.

The PNO shall be capable of indicating to the SNO to block/enable the subscriber's access in real time for reasons concerned with charging (e.g. subscriber's credit has expired), when using the SNO's network.

The SNO shall be capable of blocking/enabling the subscriber according to the type of access used in its own network, when indicated by the PNO.

Where the WLAN is an I-WLAN, the network operator shall use 3GPP standard charging. This includes the case where the WLAN NO is the PNO and has a roaming agreement with the 3GPP NO who is the SNO.

6 Recommendations

6.1 General recommendations and suggested workplan

This section shall contain an indication of the parts already covered by current specification, the parts requiring additional standardization effort, a workplan harmonized with current standardization activity (e.g. VCC), and an indication about potential new stage 1 specifications.

It is strongly recommended to reuse the mechanisms already defined in 3GPP specification and the roaming mechanisms.

It is strongly recommended to use the flexibility already defined in 3GPP specification, such as taking benefit from the possibility to establish multiple ISIM on the UICC when multiple IMS subscriptions are needed.

6.2 List of recommended requirements

This section shall contain a list of requirements to agreed to be potentially transferred to specifications

Security aspects

It shall be possible for the 3GPP NO and the WLAN NO to operate their own completely separate security systems, including independent authentication centres in their respective CNs.

The UE shall be capable of connecting to the non-3GPP network via a WLAN in a secure way using the appropriate security and authentication mechanisms for that network.

The UICC shall be able to support separate NAAs for the 3GPP access and WLAN access, where the credentials in each NAA are different.

Where the UICC supports separate NAAs for 3GPP access and WLAN access, the UICC shall permit simultaneous sessions with both NAAs on different logical channels.

In the case the PNO (non-3GPP operator with WLAN coverage) have a commercial roaming agreement with the SNO (3GPP operator) that allows PNO users to roam into SNO mobile network, the already defined I-WLAN specification [3] allows to re-use USIM authentication and network selection mechanism.

The UE shall be capable of connecting to the 3GPP network via a WLAN in a secure way using I-WLAN security and authentication mechanisms for that network as already defined in [3].

The UE shall support already defined security and authentication requirements to connect to the 3GPP network (e.g. USIM-AKA, SIM-AKA) or to the 3GPP IMS domain (e.g. IMS-AKA, HTTP digest).

Note: the WLAN network could be considered an IP-CAN when used to access the IMS domain

Service aspects

It shall be possible to support service continuity of the multimedia session, including the IMS session, if used, from the WLAN to the 3GPP network and vice-versa

The system shall be capable of assuring service continuity to the end user, when moving between WLAN access network and the 3GPP access network.

In the case service continuity is required, there is an ongoing work in the Release 8 to define multimedia sessions continuity

The UE shall be capable of providing information to the user regarding the current type of access used.

The ability to maintain service continuity when changing networks shall be dependent on the QoS capabilities of the target network.

It shall be possible for the PNO to reject the change of network if the target network does not provide adequate QoS to maintain service continuity.

It shall be possible to release the session on the change of network if the target network does not provide adequate QoS.

The system may adapt the service (e.g. degrade or enhance the service) to the capability of the target access.

Charging aspects

The NOs shall be aware of the status of the UE with respect to the network attachment and shall be capable of charging the subscriber according to the type of access used.

The NOs shall be capable of collecting on-line and off-line charging information.

Annex A:
Change history

Change history											
TSG SA#	**SA Doc.**	**SA1 Doc**	**Spec**	**CR**	**Rev**	**Rel**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
SP-38								Raised to v.2.0.0 by MCC for approval at SA#38 (same technical content as v.1.2.0)	1.2.0	2.0.0	SMLSWLAN
SP-38								Raised to v.8.0.0 by MCC following approval at SA#38 (same technical content as v.1.2.0)	2.0.0	8.0.0	SMLSWLAN
SP-40	SP-080309	S1-080568	22.937	0001	-	Rel-8	D	Change of Reference number for TR 22.812 to TR 22.912 (ANT-NSR)	8.0.0	8.1.0	SMLSWLAN
SP-46	-	-	-	-	-	-	-	Updated to Rel-9 by MCC	8.1.0	9.0.0	
2011-03	-	-	-	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0	
2012-09	-	-	-	-	-	-	-	Updated to Rel-11 by MCC	10.0.0	11.0.0	

History

Document history		
V11.0.0	October 2012	Publication