ETSI TS 124 302 V8.0.0 (2009-01)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
Access to the Evolved Packet Core (EPC)
via non-3GPP access networks;
Stage 3
(3GPP TS 24.302 version 8.0.0 Release 8)

Reference
DTS/TSGC-0124302v800

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://webapp.etsi.org/IPR/home.asp).

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 Specification (TS) 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 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.

1 Scope

The present document specifies the discovery and network selection procedures for access to 3GPP Evolved Packet Core (EPC) via non-3GPP access networks and includes Authentication and Access Authorization using Authentication, Authorization and Accounting (AAA) procedures used for the interworking of the 3GPP EPC and the non-3GPP access networks.

The present document also specifies the Tunnel management procedures used for establishing an end-to-end tunnel from the UE to the ePDG to the point of obtaining IP connectivity and includes the selection of the IP mobility mode.

Editors Note: The scope of the authentication between the UE and EPC to be specified in this document is FFS.

The non-3GPP access networks considered in this present document are cdma2000® HRPD and Worldwide Interoperability for Microwave Access (WiMAX) , and any access technologies covered in 3GPP TS 23.402 [6]. These non-3GPP access networks can be trusted or untrusted access networks.

The present document is applicable to the UE and the network. In this technical specification the network is the 3GPP EPC.

NOTE: cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA).

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 TS 22.071: "Location Services (LCS); Service description".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[5] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

[6] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[7] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[8] 3GPP TR 29.803: "3GPP System Architecture Evolution: CT WG4 aspects".

[9] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols".

[10] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)".

[11] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6".

[12] 3GPPTS 24.304: "Mobility management based on Mobile IPv4; User Equipment (UE) - Foreign Agent interface".

[13] 3GPP TS 24.312: "Access Network Discovery and Selection Function (ANDSF) Management Object (MO)".

[14] 3GPP TS 25.304: "User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode".

[15] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

[16] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[17] 3GPP TS 29.273: "Evolved Packet System; 3GPP EPS AAA Interfaces".

[18] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols".

[19] 3GPP TS 29.276: "Optimized Handover Procedures and Protocols between EUTRAN Access and cdma2000 HRPD Access".

[20] 3GPP2 X.P0057-0: "E-UTRAN - HRPD Connectivity and Interworking: Core Network Aspects".

Editor's note: The above document cannot be formally referenced until it is published by 3GPP2, at which time it will be designated as X.S0057-0 rather than X.P0057-0.

[21] 3GPP2 C.P0087-0: "E-UTRAN – HRPD and CDMA2000 1x Connectivity and Interworking: Air Interface Aspects".

Editor's note: The above document cannot be formally referenced until it is published by 3GPP2, at which time it will be designated as C.S0087-0 rather than C.P0087-0.

[22] 3GPP2 C.S0024-0: "cdma2000 High Rate Packet Data Air Interface Specification".

[23] 3GPP2 C.S0024-A: "cdma2000 High Rate Packet Data Air Interface Specification".

[24] WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 2: "Architecture Tenets, Reference Model and Reference Points", November 2007.

[25] WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3: "Detailed Protocols and Procedures", November 2007.

[26] WiMAX Forum Mobile System Profile Release 1.0 Approved Specification Revision 1.4.0, April 2007.

[27] IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005: "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendments 2 and Corrigendum 1", February 2006.

[28] IETF RFC 4306 (December 2005): "Internet Key Exchange (IKEv2) Protocol".

[29] IETF RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".

[30] IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".

[31] IETF RFC 4555 (June 2006): "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[32] IETF RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".

[33] IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)"

[34] IETF RFC 3629 (November 2003): "UTF-8, a transformation format of ISO 10646".

[35] IETF RFC 1035 (November 1987): "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION".

[36] draft-ietf-mipshop-mos-dns-discovery-00.txt (April 2008): "Locating Mobility Servers using DNS".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[37] draft-ietf-mipshop-mos-dhcp-options-00.txt (April 2008): "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for Mobility Server (MoS) discovery".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[38] draft-arkko-eap-aka-kdf-09.txt (October 2008): "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[39] OMA-ERELD-DM-V1_2: "Enabler Release Definition for OMA Device Management".

[40] OMA Device Management Tree and Description Draft Version 1.2 – 15 (October 2008)

[41] "Unicode 5.1.0, Unicode Standard Annex #15; Unicode Normalization Forms", March 2008. http://www.unicode.org.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP 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 3GPP TR 21.905 [1].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.402 [6] apply:

S2a
S2c

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [10] apply:

Evolved packet core network
Evolved packet system

For the purposes of the present document, the following terms and definitions given in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] apply:

Network Access Provider
Network Service Provider

3.23 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
ANDSF	Access Network Discovery and Selection Function
ANID	Access Network Identity
APN	Access Point Name
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSMIPv6	Dual-Stack MIPv6
eAN/PCF	Evolved Access Network Packet Control Function
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway

EPS	Evolved Packet System
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
HRPD	High Rate Packet Data
HSGW	HRPD Serving Gateway
IEEE	Institute of Electrical and Electronics Engineers
IKEv2	Internet Key Exchange version 2
IPMS	IP Mobility Mode Selection
NAI	Network Access Identifier
NAP	Network Access Provider
NBM	Network based mobility management
NSP	Network Service Provider
P-GW	PDN Gateway
PDU	Protocol Data Unit
S-GW	Serving Gateway
UE	User Equipment
UICC	Universal Integrated Circuit Card
W-APN	WLAN APN
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMF	WiMAX Forum

4 General

4.1 Trusted and untrusted accesses

The HPLMN operator of the EPC selects whether a connected non-3GPP IP access network is a trusted or untrusted IP access network.

For a trusted non-3GPP IP access network the communication between the UE and the EPC is secure. For an untrusted non-3GPP IP access network the communication between the UE and the EPC is not trusted to be secure.

For a trusted non-3GPP IP access network, all communication between the access network and the EPC is transferred over pre-established secure links. For an untrusted non-3GPP IP access network an IPSec tunnel needs to be established on a per access basis, if required, to secure communication between the UE and the EPC.

4.2 cdma2000® HRPD Access System

The cdma2000® HRPD system is a wireless mobile system developed under the auspices of 3GPP2. The cdma2000® HRPD system and its access network subsystem is compliant with 3GPP2 X.P0057-0 [20] and 3GPP2 C.P0087-0 [21], which define the core network and air interface aspects, respectively.

4.3 WiMAX Access System

The WiMAX system is a wireless mobile broadband system developed under the auspices of the WMF and the IEEE. The WiMAX system and its access network subsystem are compliant with WiMAX Forum Network ArchitectureRelease 1.0 version 1.2 – Stage 2 [24]. The protocol architecture and signalling of the WiMAX system is specified in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] which supports the air interface defined in WiMAX Forum Mobile System Profile Release 1.0 Approved Specification Revision 1.4.0 [26] specifying selected profiles of IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005 [27] that are to be supported. The WiMAX Access system correspond to the WiMAX Access Service Network (ASN) and to relevant interfaces, as defined in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25].

4.4 Identities

4.4.1 User identities

The user identification shall be either the root NAI, or the decorated NAI as defined in 3GPP TS 23.003 [3], when the UE accesses the EPC via non-3GPP access networks, and gets authentication, authorization and accounting services from the EPC.

User identification in non-3GPP accesses may require additional identities that are out of the scope of 3GPP.

IETF RFC 4187 [33] and 3GPP TS 23.003 [3] provide definitions for UE and user identities although they use slightly different terms. Similar terms are also used in 3GPP TS 33.402 [15]. The following list provides term equivalencies and describes the relation between various user identities.

- The Root-NAI as specified in 3GPP TS 23.003 [3] is to be used as the permanent identity as specified in 3GPP TS 33.402 [15].
- The Fast-Reauthentication NAI as specified in 3GPP TS 23.003 [3] is to be used as the Fast-Reauthentication Identity or the re-authentication ID as specified in 3GPP TS 33.402 [15].
- The Pseudonym Identity as specified in 3GPP TS 23.003 [3] is to be used as the Pseudonym as specified in 3GPP TS 33.402 [15].

4.4.2 Identification of IP Services/PDN connections

For access to EPC the Access Point Name (APN) is used for identifying IP services/PDN connections. The detailed definition of APN as used for access to EPC is specified in 3GPP TS 23.003 [3]. APN is used in the IKEv2 signaling during tunnel establishment and tunnel modification.

4.4.3 FQDN for ePDG Selection

A Fully Qualified Domain Name (FQDN) is constructed by UE and used as input to the DNS mechanism for ePDG selection.

The detailed format of this FQDN is specified in 3GPP TS 23.003 [3].

4.4.4 Access Network Identity

For access to EPC from a trusted non-3GPP access network via S2a the UE has to use the Access Network Identity (ANID) in the key derivation (see 3GPP TS 33.402 [15]). The handling of the Access Network Identity is described in subclause 6.4.2.4 and the generic format and specific values for the Access Network Identity are defined in subclause 8.1.1.

5 Network Discovery and Selection

Editor's note: The subclauses of this main clause will describe the access network and core network discovery and selection procedures of the UE in the different non-3GPP access networks within the scope of 23.402. This will extend to both trusted and untrusted accesses.

5.1 Access network discovery and selection procedures

5.1.1 General

In the access network discovery procedure the UE gets from the ANDSF, the information of available access networks in its vicinity. The UE may obtain this information by querying the ANDSF, and may use this information when determining the presence of operator preferred access networks. Determination of the presence of access networks requires using radio access specific procedures, which are not further described here.

After determining the presence of access networks, the UE makes a selection of the access network and then attempts access to that selected access network.

5.1.2 Access network discovery procedure

5.1.2.1 Triggering the discovery of operator preferred access networks with the ANDSF

The UE may initiate communications with the ANDSF for operator preferred access network discovery:

- when conditions set up within the policies available in the UE are met; or
- when a user request for manual selection.

NOTE: The minimum allowed time interval between two consecutive UE initiated requests towards the ANDSF can be set by operator polices.

Editor's note: Additional triggers are FFS. Some triggers like the UE changing access networks could override the minimum interval setting. This issue is FFS.

5.1.2.2 Discovering availability of access networks

The UE may apply the techniques specific to the non-3GPP access to discover available non-3GPP access networks. Such techniques will not be further described here.

In addition, the UE may signal to the ANDSF to obtain information on operator preferred access networks. The discovery of the ANDSF by the UE, the connection to the ANDSF by the UE and the signalling between the UE and the ANDSF are given in subclause 6.8.

5.1.3 Access network selection procedure

5.1.3.1 cdma2000® HRPD access network selection

The access network selection process for cdma2000® HRPD access networks shall follow 3GPP2 X.P0057-0 [20].

5.1.3.2 WiMAX NAP selection

The access network selection process for WiMAX which encompass the NAP discovery and access, shall follow the WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25].

5.1.4 WiMAX System Information

The ANDSF provides the following information in order to assist with the discovery and selection of WiMAX.

1) Operating frequencies of the WiMAX cells. This includes the downlink centre carrier frequencies of the WiMAX carriers in multiple of 250 kHz;
2) NAP (Network Access Provider) ID is a business entity that provides WiMAX radio access infrastructure to one or more WiMAX NSPs (Network Service Providers). A NAP implements this infrastructure using one or more ASNs (Access Service Networks);
3) NSP ID where NSP is a business entity that provides IP connectivity and WiMAX services to WiMAX subscribers compliant with the Service Level Agreement it establishes with WiMAX subscribers;
4) MAC Version defines the version of IEEE 802.16 MAC that is supported by BS;
5) System Version indicates the Mobile WiMAX release as specified by the WiMAX Forum Mobile Air Interface System Profile [26];
6) Phy Version defines the version of IEEE 802.16 Phy that is supported by BS;

7) System bandwidth (5, 10, 20 others);

8) Duplex mode supported (TDD, FDD, HFDD);

9) Available Downlink radio Resources;

10) Cell Type (femto, pico, micro, macro);

11) TTG (Transmit Receive Gap);

12) RTG (Receive Transmit Gap); and

13) Default RSSI and CINR (average parameters).

5.2 EPC network selection

5.2.1 General

In this release of the specification, only the EPC network selection via WiMAX access is considered. The EPC network selection via cdma2000® HRPD access is given in 3GPP TS 23.122 [4] and will no longer be described in this specification.

5.2.2 Identification of the EPC by the WiMAX access network

The NSP indication can be provided to the UE in accordance to WiMAX Forum Network Architecture Release 1.0 version 1.2 [25]. The WiMAX access network should advertise the NSP identity of the EPC in the MCC, MNC format.

5.2.3 Selection at switch-on or recovery from lack of coverage

5.2.3.1 UE selection modes

There are two modes of network selection, namely, manual network selection and automatic network selection.

At switch-on or following recovery from lack of coverage, the UE shall follow one of the following two procedures depending on its operating mode.

5.2.3.2 Manual EPC network selection (WiMAX)

The manual network selection for WiMAX access shall follow the WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] with the following exceptions and additions:

- When presenting the list of available networks for user selection, the UE shall provide the network name of the related MCC + MNC pair. If that is not possible, the UE shall provide the MCC + MNC pair; and

- If the UE is unable to register to the user selected NSP, further UE action is implementation dependent.

5.2.3.3 Automatic EPC network selection (WiMAX)

The automatic network selection for WiMAX access shall follow the WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] without any exceptions or additions.

5.2.4 EPC network selection for emergency case (WiMAX)

NOTE: Procedures for EPC network selection for emergency accesses are not specified for this release of the specification.

5.3 Network reselection

5.3.1 General

The network reselection procedure shall be executed based on the user"s request or the operator"s policy. Such operator policy for supporting network reselection can be provided by the ANDSF or can be pre-provisioned in the UE.

5.3.2 UE procedures

The UE may retrieve information from ANDSF, which includes available access network and operator"s policy as specified in subclause 6.8.2.

Editor's note: How does the information which is retrived from the ANDSF impact the network reselection procedure is FFS.

The network reselection procedure can be in automatic mode or manual mode dependent on UE configuration settings. The manual mode resleection shall follow the behaviour described in subclause 5.2.3.2. The automatic mode reselection shall follow the behaviour described in subclause 5.2.3.3.

5.3.3 EPC procedures

The ANDSF shall send available access network(s) and operator"s policy to the UE in response to the UE"s request or based on the network triggers as specified in subclause 6.8.2.

6. UE – EPC Network protocols

Editor's note: The subclauses of this main clause deals with the UE – EPC protocol specifics. However care will be taken to ensure no duplication of protocol specification is done here for what applies and is done in the SDOs that specify protocol signalling towards their non-3GPP access. Instead references will be made to the specifications of those SDOs. What must be covered here are the 3GPP specifics.

6.1 General

6.2 Trusted and Untrusted Accesses

Editor's note: This subclause details what is needed and has to be done by the UE to determine and conclude on whether to attempt trusted or untrusted access.

6.2.1 General

For a UE, the trust relationship of a non-3GPP IP access network is determined by the home PLMN operator. That trust relationship is indicated to the UE via the following methods:

- Pre-configured policies in the UE by the home PLMN operator.
- Dynamic indication during 3GPP-based access authentication.

For a trusted non-3GPP IP access network, the UE shall follow the access methods given in subclause 6.4. For an untrusted non-3GPP IP access network, the UE shall follow the access methods given in subclause 6.5.

If the dynamic trust relationship indication is received during 3GPP-based access authentication, the UE shall rely on the dynamic trust relationship indication. Otherwise the UE shall follow the pre-configured policies for a specific non-3GPP access network. If no dynamic indicator is received, and no pre-configured policy matches a specific non-3GPP access network where the UE attempts to access, the UE shall follow the procedure defined in subclause 6.2.4.

6.2.2 Pre-configured policies in the UE

The following types of policies can be pre-configured on the UE by the home PLMN operator:

- Pre-configured trust relationship policies for specific non-3GPP access technologies and/or PLMNs, and operate based on subclause 6.4. For example, the UE may be configured to consider:
  - an access network of access technology X1 from PLMN Y1 is trusted; and/or
  - any access network of access technology X2 is trusted; and/or
  - any access network from PLMN Y2 is trusted; and/or
  - any access network is trusted.

Editor's note: The format of the configuration policies is FFS.

Editor's note: Other types of policies are FFS.

6.2.3 Dynamic Indication

If the UE performs 3GPP-based access authentication, the 3GPP AAA server may send a trust relationship indicator of the non-3GPP access network to the UE during the EAP-AKA or EAP-AKA' based access authentication (i.e. EAP-AKA, EAP-AKA') as specified in 3GPP TS 33.402 [15]. The indicator is sent using a AT_TRUST_IND attribute, by extending the EAP-AKA (and EAP-AKA') protocol as specified in subclause 8.2 of IETF RFC 4187 [33]. This attribute is provided in EAP-Response/AKA-Challenge or EAP-Response/AKA'-Challenge message payload respectively. The detailed coding of this attribute is described in subclause 8.2.3.1.

6.2.4 No trust relationship information

If no dynamic indicator is received, and no pre-configured policies matches a specificy non-3GPP access network where the UE attampts to access, the UE shall consider it as untrusted network and operate based on subclause 6.5.

6.3 IP Mobility Mode Selection

Editor's note: This subclause describes the IP mobility mode selection process. In particular this subclause needs to cover the information needed and who shall provide such information and at what point in time. The criteria on which IP Mobility Mode is selected shall also be described.

6.3.1 General

The IP mobility mechanisms supported between 3GPP and non-3GPP accesses within an operator and its roaming partner's network may be based on either:

a) Static Configuration; or

b) Dynamic Configuration.

The choice between a) and b) depends upon operators' preferences and/or roaming agreement.

6.3.1.1 Static Configuration of Inter-technology Mobility Mechanism

For networks deploying a single IP mobility management mechanism, the statically configured mobility mechanism can be access type and/or roaming agreement specific. The information about the mechanism to be used in such scenario is expected to be provisioned into the terminal and the network.

In static configuration, if the network detects a mismatch between the IP mobility mode mechanism parameters pre-configured in the network and in the UE, the network shall not provide any service to the UE.

Editor"s note: It is FFS how the network detects the mismatch.

6.3.2.1 Dynamic Configuration of Inter-technology Mobility Mechanism

Dynamic IP Mobility Mode Selection (IPMS) consist of two components:

- IP MM protocol selection between Network Based Mobility (NBM) and DSMIPv6
- Decision on IP address preservation if NBM is selected

Upon initial attachment to a non-3GPP access and upon handoff to non-3GPP accesses, the UE performs IPMS by providing an indication during network access authentication for EPC. For trusted access, the indication is provided before an IP address is allocated to the UE, while in untrusted access network, the indication is provided during IKEv2 tunnel establishment with the ePDG

When the UE provides an explicit indication for IPMS, then the network shall provide the indication to the UE identifying the selected mobility management mechanism.

NOTE: The scenarios for mobility mode selection are described in subclause 4.1.3.2.1 and subclause 4.1.3.2.2 of 3GPP TS 23.402 [6].

6.3.2.1.1 IPMS indication

6.3.2.1.1.1 IPMS indication from UE to 3GPP AAA server

During network access authentication, UE may provide an explicit indication to the 3GPP AAA server about the supported mobility protocol by using an attribute in the EAP-AKA and EAP-AKA' protocols, to extend these protocols as specified in subclause 8.2 of IETF RFC 4187 [33]. This attribute is provided in EAP-Response/AKA-Challenge and corresponding EAP-AKA' message payload.

The UE may provide the indication for IPMS using AT_IPMS_IND attribute in EAP-AKA or EAP-AKA' if the UE receives the AT_RESULTS_IND attribute within the EAP-Request/AKA-Challenge message , or the EAP-Request'/AKA-Challenge' message when EAP-AKA' is used, received from the 3GPP AAA server. If the UE provides the AT_IPMS_IND attribute within the EAP-Response/AKA-Challenge message payload, or the EAP-Response'/AKA-Challenge' message payload when EAP-AKA' is used, the UE shall also provide the AT_RESULT_IND attribute within the message. The UE indicates support for one or more mobility protocols in AT_IPMS_IND attribute as follows:

- the UE shall indicate support for DSMIPv6 if the UE supports DSMIPv6; and
- the UE shall indicate support for MIPv4 if the UE supports MIPv4; and
- during initial attach, the UE should indicate support for NBM if the UE supports address preservation based on NBM between the access it is attaching to and all other accesses that the UE supports.; or
- upon handover, the UE shall indicate support for NBM if the UE supports address preservation based on NBM while moving from source access network to target non-3GPP access network that the UE is attaching to.

The preference of protocol may be indicated based on the policies configured on the UE. The detailed coding of this attribute is described in subclause 8.2.1.1.

Editor"s note: It is FFS if and how the UE provides an indication for scenarios where EAP-AKA based authentication is not performed in trusted access networks.

Editor"s note: The attribute AT_IPMS_IND defined in this subclause requires registration with the IANA. At the time of freezing of release 8, MCC should make this registration.

6.3.2.1.1.2 IPMS indication from 3GPP AAA server to UE

A 3GPP AAA server supporting IPMS shall include the AT_RESULT_IND attribute within the EAP-Request/AKA-Challenge and corresponding EAP-AKA' message payload.

If the UE provided an explicit indication as described in subclause 6.3.2.1, the 3GPP AAA server shall inform the UE of its decision on the mobility protocol and IP preservation mode by invoking an EAP-Request/AKA-Notification dialogue or an EAP-Request'/AKA-Notification' dialogue when EAP-AKA' is used.

On selecting the mobility protocol based on UE indication, access network capabilities and network policies, the AAA server shall indicate the selected protocol to the UE by using the AT_IPMS_RES attribute.

If the AT_IPMS_RES attribute indicates DSMIPv6 then the UE shall follow the procedures defined in 3GPP TS 24.303 [11].

If the AT_IPMS_RES attribute indicates MIPv4 support, then the UE shall follow the procedures defined in 3GPP TS 24.304 [12].

The detailed coding of this attribute is described in subclause 8.2.1.2.

Editor"s note: The attribute AT_IPMS_RES defined in this subclause requires registration with the IANA. At the time of freezing of release 8, MCC should make this registration.

6.4 Authentication and authorization for accessing EPC via a trusted non-3GPP access network

6.4.1 General

For access to the EPC via a trusted non-3GPP access network, a connection shall be established between the UE and the trusted non-3GPP access network using signalling procedures specific to the trusted non-3GPP access network and is out of scope of this present document.

Access authentication signalling for access to the EPC shall be executed between the UE and 3GPP AAA server to ensure mutual authentication of the user and the EPC. Such authentication is based on IETF protocols as specified in 3GPP TS 33.402 [15].

EAP-AKA is executed between the UE and EPC via a trusted non-3GPP access network in the case of connectivity to the EPC. In the case of the access network not supporting EAP-AKA, the UE shall access to the EPC only via S2cand shall perform the EAP-AKA authentication during S2c bootstrapping as specified in 3GPP TS 24.303 [11] and 3GPP TS 33.402 [15].

6.4.2 UE procedures

6.4.2.1 Identity Management

The user identities to be used by the UE in the authentication and authorization for accessing EPC via a trusted non-3GPP access are the Root-NAI (permanent identity), Fast-Reauthentication NAI(Fast-Reauthentication Identity) and Pseudonym Identity and these identities are described in subclause 4.4.

6.4.2.2 EAP-AKA based Authentication

The UE shall support EAP-AKA based authentication as specified in IETF RFC 4187 [33] and EAP-AKA" based authentication as specified in draft-arkko-eap-aka-kdf[38]. 3GPP TS 33.402 [15] specifies the conditions under which one or the other of these two methods is used.

During network access authentication, the UE may provide an explicit indication for IPMS by adding an attribute in the EAP-AKA payload as defined in subclause 6.3.2.1.

During network access authentication, the 3GPP AAA server may provide the Access Network Identity to the UE, see subclause 6.4.2.4.

6.4.2.3 Full Authentication and Fast Re-authentication

The UE shall support both full authentication and fast re-authentication for EAP AKA as specified in IETF RFC 4187 [33] and for EAP-AKA" as specified in draft-arkko-eap-aka-kdf [38].

Full authentication is performed to generate new keys. The initial authentication shall be a full authentication as specified in 3GPP TS 33.402 [15]. For a full authentication either the Permanent Identity or the Pseudonym Identity is used.

A fast re-authentication is an authentication procedure which uses the Fast Re-authentication Identity and results in a refresh of existing keys.

The Permanent Identity is based on the IMSI of the UE. The Pseudonym Identity or the Fast Re-authentication Identity or both are provided to the UE by the AAA server during the previous authentication procedure. The UE shall use the temporary identity (the Pseudonym Identity or the Fast Re-authentication Identity) only once.

If during an authentication request, the UE receives an EAP-Request/AKA-Identity message containing AT_PERMANENT_ID_REQ, the UE shall return the Permanent Identity in the AT_IDENTITY attribute of the EAP-Response/AKA_Identity. If the UE receives an EAP-Request/AKA"-Identity message containing AT_PERMANENT_ID_REQ, the UE shall return the Permanent Identity in the AT_IDENTITY attribute of the EAP-Response /AKA"-Identity message.

If during an authentication request, the UE receives an EAP-Request/AKA-Identity message which contains AT_FULLAUTH_ID_REQ, the UE shall return the Pseudonym Identity as the AT_IDENTITY within EAP-Response/AKA_Identity message if available. If the UE receives an EAP-Request/AKA"-Identity message containing AT_FULLAUTH_ID_REQ, the UE shall return the Pseudonym Identity as the AT_IDENTITY within the EAP-Response /AKA"-Identity message if available. Otherwise the UE shall return the Permanent Identity.

If during an authentication request, the UE receives an EAP-Request/AKA-Identity message or EAP-Request/AKA"-Identity message respectively, which contains AT_ANY_ID_REQ, the UE shall return the Fast Re-authentication Identity if available as the AT_IDENTITY. Otherwise the UE shall return the Pseudonym Identity.

6.4.2.4 Handling of the Access Network Identity

6.4.2.4.1 General

The 3GPP AAA server provides the UE with the Access Network Identity in EAP signalling. The UE can also obtain the Access Network Identity by access network specific means, which are out of scope of the present document. For some access networks the Access Network Identity can also be configured into the UE and the 3GPP AAA server.

NOTE: According to 3GPP TS 33.402 [15], the Access Network Identity is used by HSS and UE to generate transformed authentication vectors and therefore the Access Network Identity needs to be identical in the HSS and in the UE. The trusted access network first sends the Access Network Identity to the 3GPP AAA server via the STa reference point and the 3GPP AAA server sends the Access Network Identity to HSS via the SWx reference point, see 3GPP TS 29.273 [17], and to the UE as specified in this specification.

6.4.2.4.2 Access Network Identity indication from 3GPP AAA server to UE

When the 3GPP AAA server sends an EAP Request' or AKA-Challenge' message to the UE, the 3GPP AAA server shall include the Access Network Identity to be used when generating transformed authentication vectors, using the AT_KDF_INPUT attribute as described in subclause 8.2.2. The value and coding of this attribute is described in subclause 8.1.1.

6.4.2.4.3 UE check of ANID for HRPD CDMA 2000® access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' specified in draft-arkko-eap-aka-kdf [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to an eHRPD network, the locally determined ANID is "HRPD". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.2.4.4 UE check of ANID for WiMAX access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' specified in draft-arkko-eap-aka-kdf [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to a WiMAX access network, the locally determined ANID is "WiMAX". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.2.4.5 UE check of ANID for WLAN access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' specified in draft-arkko-eap-aka-kdf [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to an WLAN network, the locally determined ANID is "WLAN". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.2.4.6 UE check of ANID for ETHERNET access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' specified in draft-arkko-eap-aka-kdf [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to an Ethernet network, the locally determined ANID is "ETHERNET". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.3 3GPP AAA server procedures

6.4.3.1 Identity Management

The 3GPP AAA selects the pseudonym identity or the Fast Re-authentication Identity and returns the identity to the UE during the Authentication procedure as specified in 3GPP TS 33.402 [15]. The AAA server shall maintain a mapping between the UE's permanent identity and the pseudonym identity and between the UE's permanent identity and the Fast Re-authentication Identity.

6.4.3.2 EAP-AKA based Authentication

The 3GPP AAA server shall support EAP AKA based authentication as specified in IETF RFC 4187 [33] and EAP-AKA" based authentication as specified in draft-arkko-eap-aka-kdf [38]. 3GPP TS 33.402 [15] specifies the conditions under which one or the other of these two methods is used. If the UE provides an explicit indication for the supported mobility protocols and the network supports multiple IP mobility mechanisms, then the network shall select the protocol to be used and communicate the decision to the UE by using the attribute defined in subclause 6.3.2.1.1.2 in the EAP-Response/AKA-Notification message.

6.4.3.3 Full authentication and Fast Re-authentication

The 3GPP AAA shall support full re-authentication and fast re-authentication as specified in IETF RFC 4187 [33].

The decision to use the fast re-authentication process is taken by the home network (i.e. the 3GPP AAA server) and is based on operator policies. If fast re-authentication is to be used, the home network shall indicate this to the UE by providing the Fast Re-authentication Identity to the UE during the authentication process.

When initiating an authentication, the home network shall indicate the type of authentication required by including either AT_PERMANENT_ID_REQ or AT_FULLAUTH_ID_REQ for Full authentication and AT_ANY_ID_REQ for Fast re-authentication in the EAP-Request/AKA_Identity message or the EAP-Request/AKA"-Identity message respectively.

The home network (i.e. the 3GPP AAA server) may upon receiving the EAP-Response/AKA_Identity message, or EAP-Request/AKA"-Identity message respectively, containing the Fast Re-authentication Identity in AT_IDENTITY, decide to proceed with the fast re-authentication or choose instead to initiate a full authentication. This decision is based on operator policies.

6.4.4 Multiple PDN Support for trusted non-3GPP access

Connectivity to Multiple PDNs via trusted non-3GPP access is supported in the EPS when the network policies, the non-3GPP access and user subscription allow it. The UE can establish connection to additional PDNs over S2a interface by sending a trigger for additional PDN connectivity specific to the non-3GPP access. The UE shall include an APN in this trigger to connect to the desired PDN. The UE shall also indicate the attach type to the trusted non-3GPP access during additional PDN connectivity. The attach type shall distinguish between initial attach and handover attach.

NOTE: The indication about Attach type is non-3GPP access network specific and its coding is specified in the specifications of the corresponding non-3GPP access networks.

If the UE supports dynamic mobility management mechanism then UE shall use the same mobility protocol selected by the network during initial authentication. The UE shall follow the procedures described in 3GPP TS 24.303 [11] to connect to multiple PDNs over S2c interface.

6.5 Access authentication and authorization in an untrusted non-3GPP access network

Editor's note: This subclause will contain a description of the access authentication and authorization procedures and tunnel management procedures needed when the UE attaches to an untrusted non-3GPP access network (reference point S2b or S2c).

6.5.1 General

In order to attach to the evolved packet core network (EPC) via untrusted non-3GPP IP access, the UE first needs to be configured with a local IP address from the untrusted non-3GPP access network. Once the UE is configured with a local IP address, the UE shall select the Evolved Packet Data Gateway (ePDG) as described in subclause 7.2.1 and shall initiate the IPsec tunnel establishment procedure as described in subclause 7.2.2.

6.5.2 Access authentication and authorization

Editor's note: This subclause will contain a description of the access authentication and authorization procedures needed when the UE attaches to an untrusted non-3GPP access network (reference point S2b or S2c). Section 6.1.1 of 3GPP TS 24.234 [9] can be considered as a basis for this subclause.

6.5.2.1 General

Authentication signalling for untrusted non-3GPP access to the EPC shall be executed between the UE and the 3GPP AAA server in the EPC to ensure mutual authentication of the user and the EPC.

Authorization of EPC access shall be performed by the 3GPP AAA server upon successful user authentication.

Access authentication signalling shall be based on IETF protocols, for e.g., Extensible Authentication Protocol (EAP) as specified in IETF RFC 3748 [29].

Editor's note: The choice of an authentication protocol is FFS.

6.5.2.2 UE procedures

6.5.2.3 3GPP AAA server procedures

Editor's note: It is assumed that within the present report, like in 3GPP TS 24.234 [9], no distinction needs to be made between roaming and non-roaming scenarios. I.e. within the scope of this report, the SWa and SWd reference points defined in 3GPP TS 23.402 [6] are considered to coincide. The SWd reference point between 3GPP AAA proxy and 3GPP AAA server will be described by CT4 in 3GPP TR 29.803 [8].

6.5.3 Multiple PDN support for untrusted non-3GPP access network

Connectivity to multiple PDNs via untrusted non-3GPP access when PMIPv6 is used is supported in the EPS when the network policies and the user subscription allow it. The UE shall establish connection to multiple PDNs when PMIPv6 is used by the ePDG, by establishing a new IPSec tunnel with the same ePDG as described in subclause 7.2.2. The UE shall follow the procedures described in 3GPP TS 24.303 [11] to connect to multiple PDNs over S2c interface.

6.6 UE - 3GPP EPC (cdma2000® HRPD Access)

Editor's note: This clause and its subclauses is for detailing the protocols needs for cdma2000® HRPD. There is no intention to duplicate what, for the terminal to cdma2000® HRPD access network, is done in other SDOs eg. 3GPP2. The intention is to detail the exceptions and the additions needed for the UE to access and obtain services in EPC via that specific non-3GPP access.

6.6.1 General

3GPP2 X.P0057-0 [20] defines the interworking architecture for access to the EPC via cdma2000® HRPD access networks. In particular, 3GPP2 X.P0057-0 [20] describes support for a UE using the cdma2000® HRPD air interface to access the EPC architecture defined in 3GPP TS 23.402 [6] by:

- specifying the use of the interface across the S2a reference point between the 3GPP2 HRPD Serving Gateway (HSGW) and the PDN Gateway (P-GW) in the EPC by referencing 3GPP TS 29.275 [18],
- specifying the use of the interface across the S101 reference point between the eAN/PCF in the 3GPP2 HRPD access network and the MME in the EPC by referencing 3GPP TS 29.276 [19],
- specifying the use of the user plane interface across the S103 reference point between the EPC Serving Gateway (S-GW) and the HSGW by referencing 3GPP TS 29.276 [19], and
- describing the internal functions and responsibilities of the HSGW.

3GPP2 C.P0087-0 [21] defines the signalling requirements and procedures for UEs accessing the EPC via 3GPP2 HRPD access networks using the cdma2000® HRPD air interface. In particular, 3GPP2 C.P0087-0 [21]:

- defines the signalling extensions to the cdma2000® HRPD air interface defined in 3GPP2 C.S0024-0 [22] and 3GPP2 C.S0024-A [23] necessary to support interworking with the EPC and E-UTRAN, and
- defines the UE and eAN/PCF procedures and signalling formats to support bidirectional handoff between E-UTRAN and cdma2000® HRPD.

6.6.2 Non-emergency case

6.6.2.1 General

Subclauses 6.6.2.2 through 6.6.2.7 describe the particular requirements for access to the EPC via a cdma2000® HRPD access network in support of non-emergency accesses and services.

6.6.2.2 UE identities

The UE and network shall use the root NAI as specified in 3GPP TS 23.003 [3] for EPC access authentication when the UE obtains service via a cdma2000® HRPD access network connected to an EPC in the UE's HPLMN.

Editor's note: Whether the UE and network shall use the root NAI or decorated NAI for EPC access authentication when the UE obtains service from the EPC via a cdma2000® HRPD access network serving as a VPLMN is for further study.

Additionally, the UE and network shall use the Fast-Reauthentication NAI and the Pseudonym Identity as described in subclause 4.4.

6.6.2.3 cdma2000® HRPD access network identity

The access network identity is described in 3GPP TS 23.003 [3] subclause 6.4.2.4. For a cdma2000® HRPD network, the value and encoding of the access network identity is described in subclause 8.1.1. The 3GPP AAA server, HSS, and any visited network AAA proxy shall use this access network identifier during EAP-AKA authentication procedures (see 3GPP TS 33.402 [15]).

6.6.2.4 PLMN system selection

The UE shall rely on information provisioned by the home operator to facilitate the PLMN system selection process described in 3GPP TS 23.122 [4].

6.6.2.5 Trusted and untrusted accesses

The UE shall determine the trust relationship for access to the EPC via a cdma2000® HRPD access network as described in subclause 4.1.

6.6.2.6 IP mobility mode selection

The UE and network shall perform IP mobility mode selection as described in subclauses 6.3.2 and 6.4.3.2

6.6.2.7 Authentication and authorization for accessing EPC

Editor's note: This subclause will identify any particular options, if any, with respect to the authentication and authorization processes used by the UE and 3GPP AAA server for UEs accessing the EPC via a cdma2000® HRPD access network. In particular, any requirements defined in 3GPP2 X.P0057-0 [20] or 3GPP2 C.P0087-0 [21] which mandate the use of any options described in subclause 6.4 or 3GPP TS 33.402 [15] should be identified within this subclause.

6.6.3 Emergency case

NOTE: Procedures for handling emergency accesses or services are not specified within this release of the specification.

6.7 UE - 3GPP EPC (WiMAX Access)

Editor's note: This clause and its subclauses is for detailing the protocols needs for WiMAX. There is no intention to duplicate what, for the terminal to WiMAX access network, is done in other SDOs eg. IEEE. The intention is to detail the exceptions and the additions needed for the UE to access and obtain services in EPC via that specific non-3GPP access.

6.7.1 General

The WiMAX system and its access network subsystem are described within WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 2 [24]. The protocol architecture and signalling of the WiMAX system is specified in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25]. This protocol architecture and signalling supports the air interface defined in WiMAX Forum Mobile System Profile Release 1.0 Approved Specification

Revision 1.4.0 [26] which specifies selected profiles of IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005 [27].

6.7.2 Non-emergency case

6.7.2.1 General

Subclauses 6.7.2.2 through 6.7.2.7 describe the particular requirements for access to the EPC via a WiMAX access network in support of non-emergency accesses and services.

6.7.2.2 UE identities

The UE and network shall use the root NAI as specified in 3GPP TS 23.003 [3] for EPC access authentication when the UE obtains service via a WiMAX access network connected to an EPC in the UE's HPLMN.

Editor's note: Whether the UE and network shall use the root NAI or decorated NAI for EPC access authentication when the UE obtains service from the EPC via a WiMAX access network serving as a VPLMN is for further study.

Additionally, the UE and network shall use the Fast-Reauthentication NAI and the Pseudonym Identity as described in subclause 4.4.

6.7.2.3 WiMAX access network identity

Editor's note: The means for signalling the WiMAX access network identity to the UE or the means for enabling the UE to derive the access network identity from already available data is FFS. Additionally, the specific value for the WiMAX access network identity is FFS.

6.7.2.4 PLMN system selection

The UE shall use WIMAX-specific procedures described in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] to select the highest priority PLMN which is available and allowable.

6.7.2.5 Trusted and untrusted accesses

The UE shall determine the trust relationship for access to the EPC via a WiMAX access network as described in subclause 4.1.

6.7.2.6 IP mobility mode selection

The UE and network shall perform IP mobility mode selection as described in subclauses 6.3.2 and 6.4.3.2.

6.7.2.7 Authentication and authorization for accessing EPC

Editor's note: This subclause will identify any particular options, if any, with respect to the authentication and authorization processes used by the UE and 3GPP AAA server for UEs accessing the EPC via a WiMAX access network. In particular, any requirements defined in WiMAX specifications which mandate the use of any options described in subclause 6.4 or 3GPP TS 33.402 [15] should be identified within this subclause.

6.7.3 Emergency case

NOTE: Procedures for handling emergency accesses or services are not specificed within this release of the specification

6.8 Communication over the S14

Editor's note: This subclause will detail all the communications between UE and ANDSF over the S14 reference point. The scope of this communication will be driven by what is in the stage 2 - 3GPP TS 23.402 [6].

6.8.1 General

In order to assist the UE with performing access network discovery and selection, a set of information needs to be provided to the UE. This information contains the access network discovery and selection information to assist the UE with selecting the access network, and/or the inter-system mobility policy to control and assist the UE with performing the inter-system change.

This set of information can either be provisioned in the UE by the home operator, or provided to the UE by the ANDSF over the S14 reference point via pull or push mechanisms as defined in 3GPP TS 23.402 [6] by means of the access network discovery and selection procedures as described in subclause 6.8.2.

The ANDSF is located in the subscriber's home operator network and needs to be known to the UE or discovered by the UE. Through push mechanisms the ANDSF can provide assistance information at any time to the UE. Through pull mechanisms the UE can send a request to the ANDSF in order to get assistance information for access network discovery and selection.

6.8.2 Interaction with the Access Network Discovery and Selection Function

Editor's note: This subclause will detail the protocol interactions between UE and the ANDSF over the S14 reference point in trusted and untrusted non-3GPP accesses.

6.8.2.1 General

The S14 interface enables IP level communication between the UE and ANDSF. The protocols supported by the S14 interface are realized above the IP level. Both pull and push mechanisms may be supported for communication between the UE and the ANDSF. A combination of pull and push mechanisms may also be supported.

The information is transferred between the UE and ANDSF using OMA DM as defined in OMA-ERELD-DM-V1_2 [39] with the management object as specified in 3GPP TS 24.312 [13].

6.8.2.2 UE procedures

6.8.2.2.1 UE discovering the ANDSF

The IP address of the ANDSF can be provisioned in the UE by the home operator. If not provisioned in the UE, the domain name or the IP address of the ANDSF can also be discovered by the UE by means of the DHCP query as specified in draft-ietf-mipshop-mos-dhcp-options [37]. The ANDSF IP address by which the UE can contact the ANDSF can also be obtained by the UE through a DNS lookup as specified in IETF RFC 1035 [35]. The QNAME shall be set to the ANDSF-SN FQDN.

Editor's note: The way ANDSF-SN FQDN is defined and its relation with OMA-DM bootstrapping process for ANDSF are FFS.

Editor's note: When a UE is roaming, how the UE's location can be obtained by the ANDSF in order to provide the corresponding information to that UE is FFS.

Editor's note: The granularity of the UE's location that the UE provides to the ANDSF is FFS.

Editor's note: Other solution for the UE to retrieve the IP address of the ANDSF is FFS.

When performing DNS resolution, the UE shall build a Fully Qualified Domain Name (FQDN) for the DNS request and select the IP address of the ANDSF included in the DNS response message.

When performing DHCP resolution, the UE shall perform DHCP query and select the IP address of the ANDSF offered by the DHCP Server, or perform another DNS query to get the IP address of the ANDSF when the DHCP Server only provides the domain name of the ANDSF.

6.8.2.2.2 Role of UE for Push model

Editor's note: The following are FFS:-
- registration by the UE to the ANDSF; and
- the methods and mechanisms in the UE to validate information received from the ANDSF is indeed meant for that UE
- the privacy issues related to provision of location of the UE to the ANDSF and
- the type of location information, the accuracy and how this information is conveyed.

6.8.2.2.3 Role of UE for Pull model

In the pull model of communication, the UE sends a query to ANDSF to retrieve or update inter-system mobility policy or information about available access networks in its vicinity or both. The UE will wait for an implementation dependent time for an answer from the ANDSF. If ANDSF does not respond within that time, further action by the UE is implementation dependent. The UE may store the information with version identifier received from network. The ANDSF can generate the version identifier e.g. by using time stamp, version number or some other unique identifier as specified in OMA Device Management Tree and Description Draft Version 1.2 [40]. The UE may include the following information in the request:

1) UE"s current location;

Editor's note: The granularity of location information (e.g. GPS, cell identity, etc.) is FFS.

Editor's note: It is FFS how to comply with location services requirements in 3GPP TS 22.071 [2], especially referring to local, national and regional privacy requirements and to the confidentiality of location information. In some countries it is not allowed to store the user's location information.

2) UE capabilities (e.g. list of access networks that can be selected); and

Editor's note: Other information that may be provided by the UE in request message is FFS.

3) Version identifier of the previous update received from network.

6.8.2.2.4 UE using information provided by ANDSF

The specific requirements for network detection and selection may take into account of the UE's local policy, e.g. user preference setting, access history, etc, along with the information provided by the ANDSF when selecting an access network. The local policy and the information provided by the ANDSF shall be used by the UE in an implementation dependent way to limit the undesired alternating between access systems, e.g. ping-pong type of inter-system changes. However, the use of such information from the ANDSF shall not be in contradiction to functions specified in 3GPP TS 23.122 [4], 3GPP TS 25.304 [14] and 3GPP TS 36.304 [16].

6.8.2.3 ANDSF procedures

6.8.2.3.1 General

The ANDSF provides information about inter-system mobility policy or information about available access networks in the vicinity of the UE or both. The inter-system mobility policies may be organized in a hierarchy and a priority order among multiple policies may determine which policy has the highest priority. The policies may indicate preference of one access network over another or may restrict inter-system mobility to a particular access network under certain conditions. The ANDSF may also specify validity conditions which indicate when a policy is valid. Such conditions may be based on time duration, location, etc.

Editor's note: The exact description and scope of policies applicable for different access networks is FFS

6.8.2.3.2 Role of ANDSF for Push model

In the push model, the ANDSF may update the inter-system mobility policy or information about available access networks in the vicinity of the UE or both based on network triggers. The ANDSF shall be able to limit the information provided to the UE. This can be based on UE"s current location, UE capabilities, etc.

Editor's note: On the ANDSF side, for the PUSH model to function correctly, the ANDSF:-
- needs the IP address and current location of the UE; and
- needs to be updated if the IP address or the location of the UE changes; and
- must have an agreed method with the UE to check that provided information is meant for intended recipient.

Editor's Note: The criteria governing the interval at which information is pushed by ANDSF to UE is FFS.

6.8.2.3.3 Role of ANDSF for Pull model

On receipt of the request message the ANDSF sends a response to the UE. The response includes inter-system mobility policy or information about available access networks in the vicinity of the UE or both. In case of information about available access networks, the ANDSF provides the following information about each available access networks:

1) Type of Access network (e.g. WLAN, WiMAX);
2) Access Network Identifier (e.g. SSID of WLAN network);
3) The PLMN(s) it provides access to; and
4) A preference value indicating the serving operator"s preference to access a particular access network.
5) Operator differentiated text field.

Editor's note: The exact information provided for each access network is FFS

7 Tunnel management procedures

Editor's note: This main clause and its subclause shall detail the tunnel management procedures and protocol for the access tunnel to the access network. In this subclauses only untrusted accesses shall be considered.

7.1 General

The purpose of tunnel management procedures is to define the procedures for establishment or disconnection of an end-to-end tunnel between the UE and the ePDG. The tunnel establishment procedure is always initiated by the UE, whereas the tunnel disconnection procedure can be initiated by the UE or the ePDG.

The tunnel is an IPsec tunnel (see IETF RFC 4301 [30]) established via an IKEv2 protocol exchange IETF RFC 4306 [28] between the UE and the ePDG. The UE may indicate support for IETF RFC 4555 [31]. The security mechanisms for tunnel setup using IPsec and IKEv2 are specified in 3GPP TS 33.234 [7].

7.2 UE procedures

7.2.1 Selection of the ePDG

For dynamic selection of the ePDG the UE shall support the implementation of standard DNS mechanisms in order to retrieve the IP address(es) of the ePDG. The input to the DNS query is a FQDN, containing the VPLMN ID or HPLMN ID as Operator Identifier, depending on whether the UE is roaming or not.

Editor"s note: the exact format of this FQDN is FFS and needs to be specified in TS 23.003, independently from W-APN and APN.

Editor"s note: it is FFS how the UE determines it"s roaming status.

Upon reception of a DNS response containing one or more IP addresses of ePDGs, the UE shall select an IP address of ePDG with the same IP version as its local IP address.

The UE shall select only one ePDG also in case of multiple PDN connections.

Editor"s note: it is FFS if during handover the UE could connect to two different ePDGs.

7.2.2 Tunnel establishment

Once the ePDG has been selected, the UE shall initiate the IPsec tunnel establishment procedure using the IKEv2 protocol as defined in IETF RFC 4306 [28].

The UE shall send an IKE_SA_INIT request message to the selected ePDG in order to setup an IKE connection. Upon receipt of an IKE_SA_INIT response, the UE shall send an IKE_AUTH request message to the ePDG, including the type of IP address (IPv4 or IPv6 or both) that needs to be configured in an IKEv2 CFG_REQUEST Configuration Payload. If the UE requests for both IPv4 and IPv6 address, it shall send two configuration attributes in the CFG_REQUEST Configuration Payload, one for the IPv4 address and the other for the IPv6 address. The IKE_AUTH request message shall contain in "IDr" payload the APN and in the "IDi" payload the NAI. The UE may also request the Home Agent identity for DSMIPv6 related signalling, by including a corresponding CFG_REQUEST Configuration Payload containing a HA-APN built as specified in 3GPP TS 23.003 [3]. The IKE_AUTH request message may contain in a notify payload an indication that MOBIKE is supported by the UE.

Editor's note: it is FFS which type of attribute (private or assigned by IANA) is used in the configuration payload.

During the IKEv2 authentication and tunnel establishment, UE shall provide an explicit indication about the supported mobility protocol as described in subclause 6.3.2.

During the IKEv2 authentication and tunnel establishment, UE shall provide an indication about Attach Type, which indicates Initial Attach or Handover Attach. To indicate attach due to handover the UE shall include the allocated home address(es) during the IKEv2 tunnel setup. For initial attach the UE shall not include the allocated home address(es) during the IKEv2 tunnel establishment.

The UE shall support IPSec ESP (see IETF RFC 4303 [32]) in order to provide secure tunnels between the UE and the ePDG as specified in 3GPP TS 33.402 [15].

During the IKEv2 authentication and tunnel establishment, if the UE supports DSMIPv6, the ePDG may provide the Home Agent identity to the UE. The Home Agent identity returned by the ePDG shall include the HA-APN the UE inserted in the correspondent CFG_REQUEST and either the available Home Agent address (IPv4 address or IPv6 address or both) or the Home Agent FQDN. In the latter case the UE shall perform a DNS query with the received Home Agent FQDN as described in 3GPP TS 24.303 [11].

Editor's note: It is FFS how ePDG can support the delivery of HA identities for multiple APNs.

7.2.3 Tunnel modification

This procedure is used if MOBIKE as defined in IETF RFC 4555 [31] is supported by the UE.

When there is a change of local IP address for the UE, the UE shall update the IKE security association with the new address, and shall update the IPsec security association associated with this IKE security association with the new address. The UE shall then send an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification to the ePDG.

If, further to this update, the UE receives an INFORMATIONAL request with a COOKIE2 notification present, the UE shall copy the notification to the COOKIE2 notification of an INFORMATIONAL response and send it to the ePDG.

7.2.4 Tunnel disconnection

7.2.4.1 UE initiated disconnection

The UE shall use the procedures defined in the IKEv2 protocol (see IETF RFC 4306 [28]) to disconnect an IPsec tunnel to the ePDG. The UE shall close the incoming security associations associated with the tunnel and instruct the ePDG to

do the same by sending the INFORMATIONAL request message including a "DELETE" payload. The DELETE payload shall contain either:

i) Protocol ID set to "1" and no subsequent Security Parameters Indexes (SPIs) in the payload. This indicates closing of IKE security association, and implies the deletion of all IPsec ESP security associations that were negotiated within the IKE security association.

ii) Protocol ID set to "3" for ESP. The Security Parameters Indexes included in the payload shall correspond to the particular incoming ESP security associations at the UE for the given tunnel in question.

7.2.4.2 UE behaviour towards ePDG initiated disconnection

On receipt of the INFORMATIONAL request message including "DELETE" payload, indicating that the ePDG is attempting tunnel disconnection, the UE shall:

i) Close all security associations identified within the DELETE payload (these security associations correspond to outgoing security associations from the UE perspective). If no security associations were present in the DELETE payload, and the protocol ID was set to "1", the UE shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the ePDG.

ii) The UE shall delete the incoming security associations corresponding to the outgoing security associations identified in the "DELETE" payload.

The UE shall send an INFORMATIONAL response message. If the INFORMATIONAL request message contained a list of security associations, the INFORMATIONAL response message shall contain a list of security associations deleted in step (ii) above.

If the UE is unable to comply with the INFORMATIONAL request message, the UE shall send INFORMATION response message with either:

i) A NOTIFY payload of type "INVALID_SPI", for the case that it could not identify one or more of the Security Parameters Indexes in the message from the ePDG; or

ii) A more general NOTIFY payload type. This payload type is implementation dependent.

7.3 3GPP AAA server procedures

The UE – 3GPP AAA server procedures are as specified in 3GPP TS 29.273 [17] and 3GPP TS 33.402 [15].

7.4 ePDG procedures

7.4.1 Tunnel establishment

Upon receipt of an IKE_AUTH request message from the UE requesting the establishment of a tunnel, the ePDG shall proceed with authorization and authentication. The procedure is based on the one described in 3GPP TS 33.234 [7], with the following differences:

- ePDG is substituted for PDG,
- EAP-SIM authentication is not allowed,
- dynamical configuration of two types of IP addresses (IPv4 and IPv6),
- allocation of Home Agent address(es) for subsequent DSMIPv6 related signalling,
- instead of W-APN the full APN is transferred.

The ePDG shall proceed with IPsec tunnel setup completion and relay in the IKEv2 Configuration Payload (CFG_REPLY) of the final IKE_AUTH response message the remote IP address assigned to the UE. If the UE requested both an IPv4 and an IPv6 address, both are allocated to the UE via a single CFG_REPLY Configuration Payload containing two configuration attributes, one for the IPv4 address, the other for the IPv6 address, else only the IP address of the requested IP version is allocated. If the UE requested the Home Agent identity, the ePDG may allocate

these in a CFG_REPLY Configuration Payload with the corresponding number of configuration attributes. An IPsec tunnel is now established between the UE and the ePDG. The ePDG also includes the identity of the associated PDN (APN) in the IDr payload of IKEv2. If the UE provided APN to the ePDG during the tunnel establishment, the ePDG shall not change the provided APN.

If the UE indicates Handover Attach by including the allocated home address(es) and the ePDG obtains one or more PDN GW identities from the AAA server, the ePDG shall use these identified PDN GWs in the subsequent PGW selection process. If the UE indicates Initial Attach i.e. home address(es) not included, the ePDG may run its initial PDN GW selection process to determine the PDN GW without using the received PDN GW identities.

Editor's note: In case of IPv6, it is FFS whether an IPv6 address or an IPv6 prefix is allocated to the UE.

Editor's note: The implications of the IP mobility mode selection procedure on this section are FFS.

The ePDG shall support IPSec ESP (see IETF RFC 4303 [32]) in order to provide secure tunnels between the UE and the ePDG as specified in 3GPP TS 33.402 [15].

7.4.2 Tunnel modification

When receiving an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification, the ePDG shall check the validity of the IP address and update the IP address in the IKE security association with the values from the IP header. The ePDG shall reply with an INFORMATIONAL response.

The ePDG may initiate a return routability check for the new address provided by the UE, by including a COOKIE2 notification in an INFORMATIONAL request and send it to the UE. When the ePDG receives the INFORMATIONAL response from the UE, it shall check that the COOKIE2 notification payload is the same as the one it sent to the UE. If it is different, the ePDG shall close the IKE security association by sending an INFORMATIONAL request message including a "DELETE" payload.

If no return routability check is initiated by the ePDG, or if a return routability check is initiated and is successfully completed, the ePDG shall update the IPsec security associations associated with the IKE security association with the new address.

7.4.3 Tunnel disconnection

7.4.3.1 ePDG initiated disconnection

The ePDG shall use the procedures defined in the IKEv2 protocol (see IETF RFC 4306 [28]) to disconnect an IPsec tunnel to the UE. The ePDG shall close the incoming security associations associated with the tunnel and instruct the UE to do likewise by sending the INFORMATIONAL request message including a "DELETE" payload. The DELETE payload shall contain either:

i) Protocol ID set to "1" and no subsequent Security Parameter Indexes in the payload. This indicates that the IKE security association, and all IPsec ESP security associations that were negotiated within it between ePDG and UE shall be deleted.

ii) Protocol ID set to "3" for ESP. The SECURITY PARAMETERS INDEXES s included in the payload shall correspond to the particular incoming ESP SECURITY ASSOCIATION at the UE for the given tunnel in question.

7.4.3.2 ePDG behaviour towards UE initiated disconnection

On receipt of the INFORMATIONAL request message including "DELETE" payload indicating that the UE is initiating tunnel disconnect procedure, the ePDG shall:

i) Close all security associations identified within the DELETE payload (these security associations correspond to outgoing security associations from the ePDG perspective). If no security associations were present in the DELETE payload, and the protocol ID was set to "1", the ePDG shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the UE.

ii) The ePDG shall delete the incoming security associations corresponding to the outgoing security associations identified in the "DELETE" payload.

The ePDG shall send an INFORMATIONAL response message. This shall contain a list of security associations deleted in step (ii) above.

If the ePDG is unable to comply with the INFORMATIONAL request message, the ePDG shall send INFORMATION response message with either:

i) a NOTIFY payload of type "INVALID_SPI", for the case that it could not identify one or more of the SECURITY PARAMETERS INDEXES in the message from the UE; or

ii) a more general NOTIFY payload type. This payload type is implementation dependent.

8. PDUs and parameters specific to the present document

Editor's note: This clause is menat to document all the differences, additions and extensions that are needed to the baseline specifications.

Editor's note: Presently only specific coding against IETF RFCs are found needed. It is FFS if codings against 3GPP2 specifcations or WiMAX specifications are needed.

8.1 3GPP specific coding information defined within present document

8.1.1 Access Network Identity format and coding

8.1.1.1 Generic format of the Access Network Identity

The Access Network Identity shall take the generic format of an octet string without terminating null characters. The length indicator for the ANID is 2 bytes long, see draft-arkko-eap-aka-kdf [38]. Representation as a character string is allowed, but this character string shall be converted into an octet string of maximum length 253 according to UTF-8 encoding rules as specified in IETF RFC 3629 [34] before the Access Network Identity is input to the Key Derivation Function, as specified in 3GPP TS 33.402 [15], or used in the Access Network Identity indication from 3GPP AAA server to UE, cf. subclause 8.2.2. The ANID is structured as an ANID Prefix and none, one or more ANID additional character strings separated by the colon character ":". In case additional ANID strings are not indicated the complete ANID consists of the ANID Prefix character string only. The ANID shall be represented by Unicode characters encoded as UTF-8 as specified in IETF RFC 3629 [34] and formatted using Normalization Form KC (NFKC) as specified in Unicode 5.1.0, Unicode Standard Annex #15; Unicode Normalization Forms [41].

8.1.1.2 Definition of Access Network Identities for Specific Access Networks

Table 8.1.1.2 specifies the list of Access Network Identities defined by 3GPP in the context of non-3GPP access to EPC.

Table 8.1.1.2: Access Network Identities

Access Network Identity		Type of Access Network
ANID Prefix	**Additional ANID strings**	
"HRPD" constant character string, see NOTE 1 and NOTE 2	No additional ANID string, see NOTE 2 and NOTE 6	cdma2000® HRPD access network
"WIMAX" constant character string, see NOTE 1	No additional ANID string, see NOTE 3 and NOTE 6	WiMAX access network
"WLAN" constant character string, see NOTE 1	No additional ANID string, see NOTE 4 and NOTE 6	WLAN access network
"ETHERNET" constant character string, see NOTE 1	No additional ANID string, see NOTE 5 and NOTE 6	Fixed access network
All other character strings	Not applicable	Not defined, see NOTE 6 and Annex B

NOTE 1: The quotes are not part of the definition of the character string.

NOTE 2: The value of the ANID Prefix for cdma2000® HRPD access networks is defined in 3GPP2 X.S0057-0 [20]. 3GPP2 is responsible for specifying possible additional ANID strings applicable to the "HRPD" ANID Prefix.

NOTE 3: WiMAX Forum is responsible for specifying possible additional ANID strings applicable to the "WIMAX" ANID Prefix.

NOTE 4: IEEE 802 is responsible for specifying possible additional ANID strings applicable to the "WLAN" ANID Prefix.

NOTE 5: IEEE 802 is responsible for specifying possible additional ANID strings applicable to the "ETHERNET" ANID Prefix.

NOTE 6: Additional ANID Prefixes and ANID strings can be added to this table following the procedure described in the informative Annex B.

8.2 IETF RFC coding information defined within present document

8.2.1 IPMS attributes

8.2.1.1 AT_IPMS_IND attribute

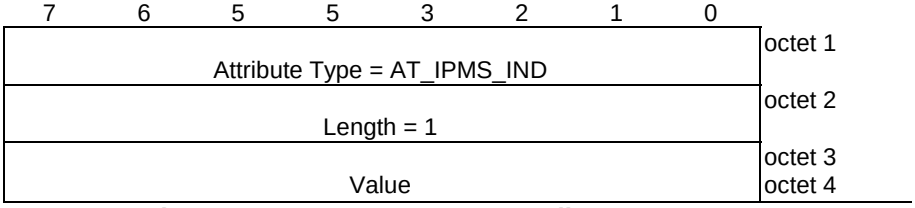

Figure 8.2.1.1: AT_IPMS_IND attribute

Table 8.2.1.1: AT_IPMS_IND attribute

Attribute Type indicates the type of attribute as AT_IPMS_IND with a value of XXXX.

Editors Note: The exact value of the attribute which will be assigned by IANA is FFS.

Length of this attribute shall be set to 1 as per IETF RFC 4187 [33]

Value

7	6	4	5	3	2	1	0	Protocol Supported
0	0	0	0	0	0	0	0	Reserved
0	0	0	0	0	0	0	1	DSMIPv6 only
0	0	0	0	0	0	1	0	NBM only
0	0	0	0	0	0	1	1	MIPv4 only
0	0	0	0	0	1	0	0	DSMIPv6 and NBM both supported
0	0	0	0	0	1	0	1	MIPv4 and NBM both supported
0	0	0	0	0	1	1	0	DSMIPv6 and NBM Supported;DSMIPv6 preferred
0	0	0	0	0	1	1	1	DSMIPv6 and NBM Supported; NBM preferred
0	0	0	0	1	0	0	0	MIPv4 and NBM supported; MIPv4 preferred
0	0	0	0	1	0	0	1	MIPv4 and NBM supported; NBM preferred
0	0	0	0	1	0	1	0	MIPv4 and DSMIPv6 supported; MIPv4 preferred
0	0	0	0	1	0	1	1	MIPv4 and DSMIPv6 supported; DSMIPv6 preferred
0	0	0	0	1	1	0	0	MIPv4, DSMIPv6 and NBM supported; MIPv4 preferred
0	0	0	0	1	1	0	1	MIPv4, DSMIPv6 and NBM supported; DSMIPv6 preferred
0	0	0	0	1	1	1	0	MIPv4, DSMIPv6 and NBM supported; NBM preferred

8.2.1.2 AT_IPMS_RES attribute

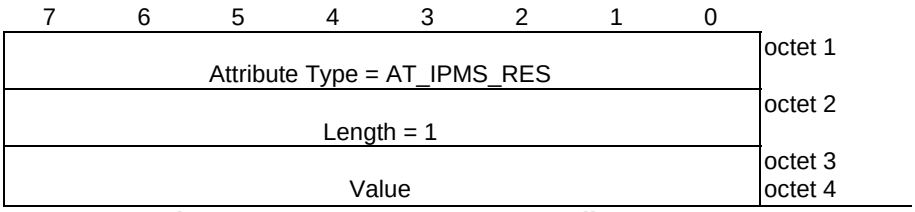

Figure 8.2.1.2: AT_IPMS_RES attribute.

Table 8.2.1.2: AT_IPMS_RES attribute

Attribute Type indicates the type of attribute as AT_IPMS_RES with a value of XXXX.

Editors Note: The exact value of the attribute which will be assigned by IANA is FFS.

The Length of this attribute shall be set to 1 as per IETF RFC 4187 [33]

Value

7	6	4	5	3	2	1	0	Protocol Selected
0	0	0	0	0	0	0	0	Reserved
0	0	0	0	0	0	0	1	DSMIPv6
0	0	0	0	0	0	1	0	NBM
0	0	0	0	0	0	1	1	MIPv4

8.2.2 Access Network Identity indication attribute

8.2.2.1 Access Network Identity in the AT_KDF_INPUT attribute

The Access Network Identity is indicated in the Network Name Field of the AT_KDF_INPUT attribute as specified in draft-arkko-eap-aka-kdf [38]. The Network Name Field shall contain the Access Network Identity as specified in subclause 8.1.1 of this specification.

NOTE: IETF in draft-arkko-eap-aka-kdf [38] refers to this specification for the value of the Network Name field.

8.2.3 Trust relationship indication attribute

8.2.3.1 AT_TRUST_IND attribute

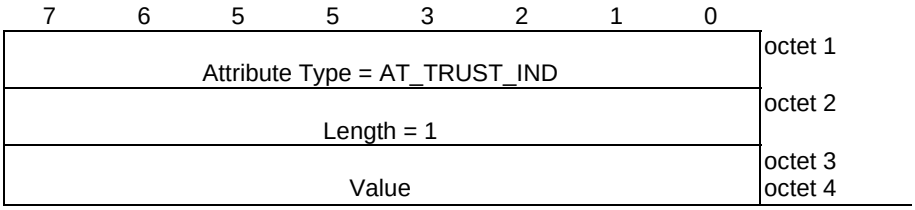

Figure 8.2.3.1-1: AT_TRUST_IND attribute

Table 8.2.3.1-1: AT_TRUST_IND attribute

Attribute Type indicates the type of attribute as AT_TRUST_IND with a value of XXXX.

Editors Note: The value of the attribute AT_TRUST_IND shall be assigned by IANA. At the time of freezing of release 8, MCC should make this registration with the IANA. The value of the new attribute should be in the skippable range 128-255.

Length of this attribute shall be set to 1 as per IETF RFC 4187 [33]

Value

7	**6**	**4**	**5**	**3**	**2**	**1**	**0**	Indicated Trust Relationship
0	0	0	0	0	0	0	0	Reserved
0	0	0	0	0	0	0	1	Trusted
0	0	0	0	0	0	1	0	UnTrusted
-	-	-	-	-	-	-	-	Rest of the values are reserved

Annex A (informative): Example signalling flows for inter-system change between 3GPP and non-3GPP systems using ANDSF

A.1 Scope of signalling flows

This annex gives examples of signalling flows for mobility between 3GPP and non-3GPP systems. These signalling flows provide as example detailed information on Network Discovery and Selection aspects involving the use of ANDSF.

A.2 Signalling flow for inter-system change between 3GPP access network and non-3GPP access network

Figure A1 below shows an inter-system change procedure between 3GPP access network and non-3GPP access network using information obtained from ANDSF.

In this example the UE uses DHCP query to obtain the FQDN of the ANDSF. The UE then uses DNS query to obtain the ANDSF IP address and transport options.

In this example flow, the communication between the UE and ANDSF does not imply use of any specific protocol.

The steps involved in inter-system change between 3GPP access network and non-3GPP access network are as follows.

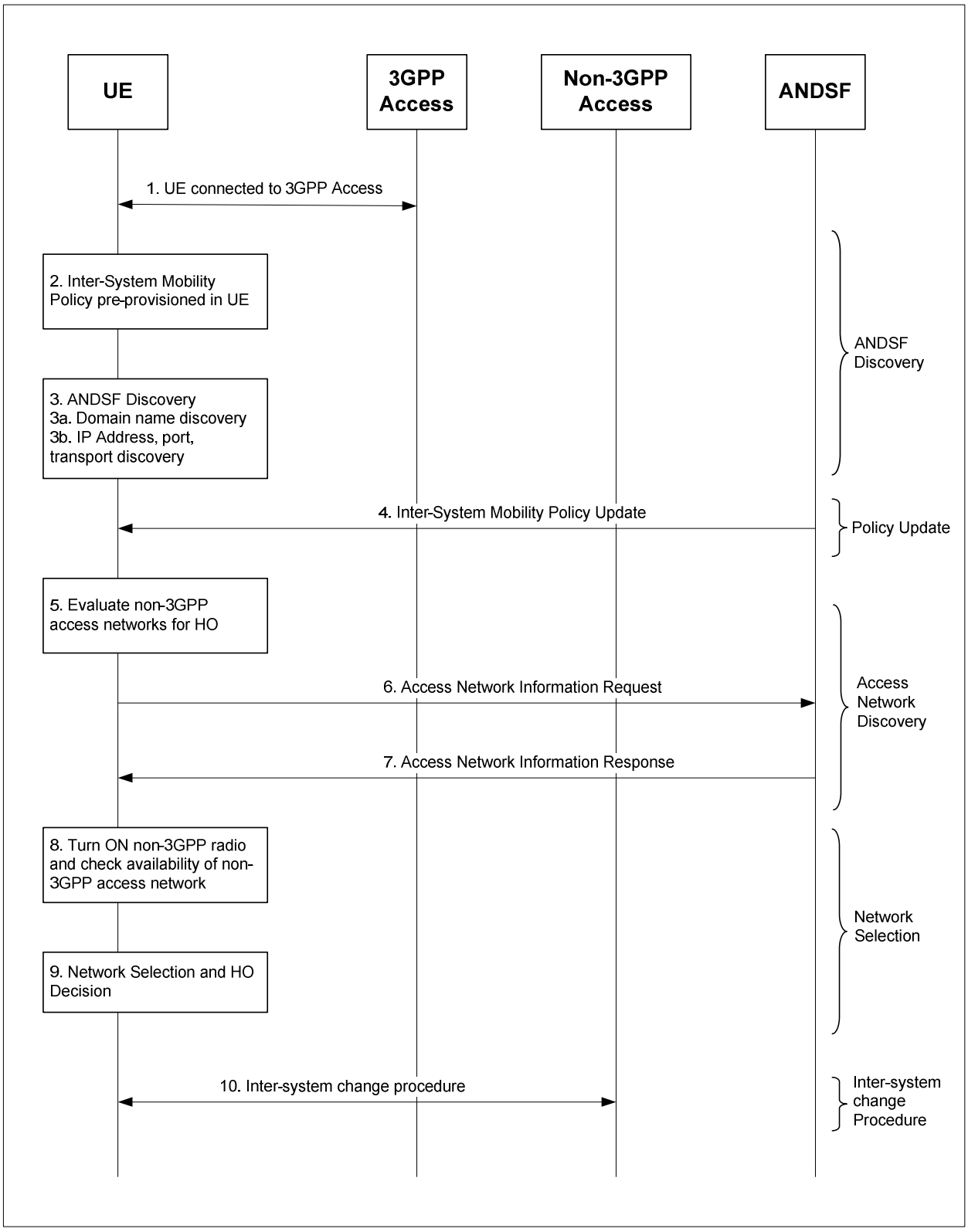

Figure A1. Procedure for Inter-system change between 3GPP access and non-3GPP using ANDSF

1. **Initial connectivity**

   The UE is connected to 3GPP network. The current applications are supported over the 3GPP access network.

NOTE: The procedure remains the same if the UE is initially connected to non-3GPP access network and wants to change to 3GPP access network.

2. **Pre-provisioned policies**

The inter-system mobility policy is pre-provisioned on the UE. Based on pre-provisioned operator policies the UE has preference for different non-3GPP networks such as WLAN, and WiMAX. The UE can select these access networks when they are available.

3. **ANDSF Discovery**

   Since the UE can support mobility to non-3GPP networks the UE performs ANDSF discovery.

   3a. The UE uses DHCPv4 query options as specified in draft-ietf-mipshop-mos-dhcp-options [37] to discover the fully qualified domain (FQDN) of the ANDSF.

   3b. The ANDSF can support multiple transport protocols (UDP, TCP or SCTP). The UE then uses the DNS query mechanism as described in draft-ietf-mipshop-mos-dns-discovery [33] to discover the IPv4 address, port number and the preferred transport protocol for communicating with the ANDSF.

4. **Policy Update based on Network Triggers**

   Based on network triggers the ANDSF sends an updated inter-system mobility policy to the UE. The inter-system mobility policy includes validity conditions, i.e. conditions indicating when the policy is valid. Such conditions can include time duration, location area, etc.

Editor's note: How the ANDSF discovers UE"s address is FFS.

5. **Evaluate which non-3GPP networks to discover**

   The inter-system mobility policies specify the access networks that the UE can select; the UE has both WLAN and WiMAX radios. In this case the operator policy allows UE to select either WLAN or WiMAX networks under all conditions. The UE obtains information about availability of both WLAN and WiMAX access networks in its vicinity.

6. **Access Network Information Request**

   The UE sends a request to ANDSF to get information about available access networks. The UE includes its preference for WLAN and WiMAX networks in the request. The UE also includes its location information in the request.

Editor"s Note: It is FFS if the ANDSF can request and retrieve the current UE location

7. **Access Network Information Response**

   The ANDSF sends a response to the UE which includes the list of available access networks types (in order of operator preferences), access network identifier and PLMN identifier. In this case the ANDSF responds with availability of both WLAN and WiMAX network in the vicinity of the UE.

8. **Evaluate candidate non-3GPP networks**

   Based on the received information the UE evaluates if it is within the coverage area of the available access networks in the order of preferences. In this case the UE has higher preference for WiMAX than WLAN. The UE powers on the WiMAX radio and checks for the presence of WiMAX network. The UE can listen to WiMAX broadcast messages (uplink/downlink channel data messages) and determines the presence of WiMAX network. Since the WiMAX network is the preferred network and since the UE has verified the presence of WiMAX network, the UE does not check for presence of WLAN network.

9. **Non-3GPP Network Selection**

   The UE selects the most preferred available access network for inter-system mobility. In this case the UE selects the WiMAX access network.

10. **Inter-system change Procedure**

    The UE initiates inter-system change procedure to the selected non-3GPP access network. The details of the inter-system change procedure are described elsewhere, see 3GPP TS 23.402 [6].

Annex B (informative): Assignment of Access Network Identities in 3GPP

This annex describes the recommended assignment procedure of Access Network Identities within 3GPP.

B.1 Access Network Identities

According to 3GPP TS 23.003 [3] the encoding of the Access Network Identity is specified within 3GPP, but the Access Network Identity definition for each non-3GPP access network is under the responsibility of the corresponding standardisation organisation respectively.

If a standardisation organisation for a non-3GPP access network determines they need to define a new Access Network Identity Prefix or additional ANID strings, they can contact the 3GPP TSG-CT WG 1 via a Liaison Statement and indicate the specific values of the Access Network Identit y Prefixes or the specific values of, or construction principles for, the additional ANID strings to be specified by 3GPP and give reference to the corresponding specification(s) of the requesting organisation. 3GPP TSG-CT WG 1 will then specify the values for the Access Network Identities by updating Table 8.1.1.2 in this specification and inform the requesting standardisation organisation.

Annex C (informative): Example usage of ANDSF

C.1 Scope of ANDSF Example

This Annex gives an example of organization of ANDSF database and how it can be used to discover access network information. In this example the UE is in 3GPP network and is trying to discover available WiMAX networks. The ANDSF database is provided by the 3GPP operator with PLMN = PLMN_3GPP.

C.2 Organization of ANDSF Coverage Map for WiMAX Network discovery

Table C1 illustrates the organization of ANDSF database for discovering WiMAX and WiFi networks. The ANDSF database provides the coverage mapping information for WiMAX and WiFi networks based on 3GPP cell identifiers. In this example the UE_Location can be specified either in terms of 3GPP parameters (PLMN + Cell Identifier) or in terms of geo spatial co-ordinates.

Table C1: ANDSF Database Organization for PLMN = PLMN_3GPP

UE_Location	AccessType = WiMAX	AccessType = WiFi
- 3GPP (CellId) - Other (Geopriv)		
Locn_1 Cell_Id = Cell_1	NSP-ID= NSP_1: -NAP_ID = NAP_1 -NAP_ID = NAP_2 NSP-ID = NSP_2 -NAP_ID = NAP_2 -NAP_ID = NAP_3	SSID = WiFi1, BSSID = BS1 SSID = WiFi2, BSSID = BS2
Locn_2 Cell_Id = Cell_2	NSP-ID = NSP_2 - NAP_ID = NAP_3	N/A
Locn_3 Cell_Id = Cell_3	N/A	SSID = WiFi1, BSSID = BS3 SSID = WiFi4, BSSID = BS4
…..	…….	…….
Locn_n Cell_Id = Cell_n	NSP-ID = NSP_1 NAP_ID = NAP_2	SSID = WiFi6, BSSID = BS5

For WiMAX network the database provides information about WiMAX NSP and NAP that provide coverage in respective 3GPP cells. Thus for example in 3GPP Cell_1, WiMAX Service provider NSP_1 provides service to WiMAX radio access providers NAP_1 and NAP-2. Similarly WiMAX Service Provider NSP_2 provides service to Network access providers NAP-2 and NAP_3 as well. Similarly in 3GPP Cell_2 WiMAX Network Service Provider NSP_2 provides service to network Access Provider NAP_3. Further it can be seen that no WiMAX coverage is available in 3GPP cell Cell_3.

C.3 Parameters in Pull mode

The UE is currently in 3GPP network. The UE sends a query to OMA ANDSF server as follows:

ANDSF_Query (UE_Location, AccessNetworkType=WiMAX)

The UE specifies the UE_Location information in terms of current 3GPP Cell Id (e.g. Cell_2)

On receipt of the query message the ANDSF looks up the UE_Location (Cell_2) in the ANDSF database and searches for a prospective WiMAX entry. In this case the ANDSF retrieves WiMAX Service provider identifier (NSP-ID) NSP_2 and WiMAX Network Access Provider Identifier (NAP-ID) NAP_3. The ANDSF retrieves the network

parameters for this combination. The ANDSF fills these parameters in the WNDS MO and sends the information back to the UE.

ANDSF_Response (UE_Location, AccessNetworkInformationRef MO=WIMAXNDS).

Annex D (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2008-01					Draft skeleton provided in C1-080125 by rapporteur to CT1#51.		0.0.0
2008-02	CT1#51				Includes the following contribution agreed by CT1 at CT1#51: C1-080568	0.0.0	0.1.0
2008-02	CT1#51 bis				Includes the following contributions agreed by CT1 at CT1#51 bis: C1-080722, C1-080765, C1-080773, C1-080783, C1-080792, C1-080793	0.1.0	0.2.0
2008-04	CT1#52				Includes the following contributions agreed by CT1 at CT1#52:- C1-080921, C1-081391, C1-081392, C1-081393, C1-081394	0.2.0	0.3.0
2008-04	email review				Incomplete implementation C1-080921	0.3.0	0.3.1
2008-05	CT1#53				Includes the following contributions agreed by CT1 at CT1#53:- C1-081575, C1-082019, C1-082066, C1-082067, C1-082074, C1-082077, C1-082078, C1-082086, C1-082091, C1-082092, C1-082093.	0.3.1	0.4.0
2008-06	CT1#54				Includes the following contributions agreed by CT1 at CT1#54:- C1-082470, C1-082563, C1-082567, C1-082569, C1-082688, C1-082803, C1-082804, C1-082809.	0.4.0	0.5.0
2008-08	CT1#55				Includes the following contributions agreed by CT1 at CT1#55:- C1-082923, C1-082982, C1-083084, C1-083171, C1-083179, C1-083262, C1-083466, C1-083480, C1-083481, C1-083512, C1-083513, C1-083514, C1-083526, C1-083603, C1-083617	0.5.0	0.6.0
2008-09					Version 1.0.0 created for presentation to TSG CT#41 for information	0.6.0	1.0.0
2008-10	CT1#55bis				Includes the following contributions agreed by CT1 at CT1#55bis:- C1-083851; C1-083976; C1-084155; C1-084383; C1-084385; C1-084386; C1-084387; C1-084388; C1-084391; C1-084393; C1-084394; C1-084395; C1-084396; C1-084482	1.0.0	1.1.0
2008-11	CT1#56				Includes the following contributions agreed by CT1 at CT1#56:- C1-084934; C1-085322; C1-085327; C1-085328; C1-085329; C1-085331; C1-085333; C1-085335; C1-085336; C1-085338; C1-085516; C1-085526; C1-085534 Editorial corrections by the rapporteur to align with drafting rules	1.1.0	1.2.0
2008-11					Version 2.0.0 created for presentation to CT#42 for approval	1.2.0	2.0.0
2008-12	CT#42				Version 8.0.0 created after approval in CT#42	2.0.0	8.0.0

History

Document history		
V8.0.0	January 2009	Publication