ETSI TS 124 303 V16.0.0 (2020-09)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Mobility management based on Dual-Stack Mobile IPv6;
Stage 3
(3GPP TS 24.303 version 16.0.0 Release 16)**

Reference
RTS/TSGC-0124303vg00

Keywords
GSM,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

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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 signalling procedures for accessing the 3GPP Evolved Packet Core network and handling the mobility between 3GPP and non-3GPP accesses via the S2c reference point defined in 3GPP TS 23.402 [3].

The present document is applicable to the User Equipment (UE) and the network node implementing the Home Agent functionality.

In addition the present document specifies the procedures used for the DSMIPv6 Home Agent discovery, for bootstrapping the DSMIPv6 security association between the UE and the Home Agent and for managing the DSMIPv6 tunnel. The specification of these procedures is compliant to IETF RFCs.

DSMIPv6 procedures can be used independently of the underlying access technology.

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] IETF RFC 5555 (June 2009): "Mobile IPv6 support for Dual Stack Hosts and Routers".

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

[4] IETF RFC 4877 (April 2007): "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".

[5] Void.

[6] Void.

[7] Void.

[8] Void.

[9] Void.

[10] IETF RFC 5026 (October 2007): "Mobile IPv6 bootstrapping in split scenario".

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

[12] IETF RFC 6610 (May 2012): "DHCP Options for Home Information Discovery in Mobile IPv6 (MIPv6)".

[13] IETF RFC 3736 (April 2004): "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[14] IETF RFC 5996 (September 2010): "Internet Key Exchange Protocol Version 2 (IKEv2)".

[15] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[16] Void.

[17] 3GPP TS 23.003: "Numbering, addressing and identification".

[18] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[19] IETF RFC 5846 (June 2010): "Binding Revocation for IPv6 Mobility".

[20] 3GPP TS 29.273: "3GPP EPS AAA interfaces".

[21] 3GPP TS 24.302: "Access to the Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[22] Void.

[23] IETF RFC 4739 (November 2006): "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[24] 3GPP TS 33.234: "Wireless Local Area Network (WLAN) interworking security".

[25] Void.

[26] IETF RFC 4039 (March 2005): "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[27] IETF RFC 6275 (July 2011): "Mobility Support in IPv6".

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

[29] IETF RFC 3963 (January 2005): "Network Mobility (NEMO) Basic Support Protocol".

[30] IETF RFC 5685 (November 2009): "Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)".

[31] IETF RFC 5648 (October 2009): "Multiple Care-of Addresses Registration".

[32] IETF RFC 6089 (January 2011): "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support".

[33] IETF RFC 6088 (January 2011): "Traffic Selectors for Flow Bindings".

[34] 3GPP TS 23.261: "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2".

[35] IETF RFC 6276 (July 2011): "DHCPv6 Prefix Delegation for Network Mobility (NEMO)".

[36] 3GPP TS 24.312: "Access Network Discovery and Selection Function (ANDSF) Management Object (MO)".

3 Definitions 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. The following terms used in this Technical Specification are defined in IETF RFC 6275 [27]: Home Address, Care-of Address, binding cache, binding cache entry.

The following terms used in this Technical Specification are defined in IETF RFC 5648 [31], and IETF RFC 6089 [32]: Binding Identification Number, Flow, Flow Binding, Flow Identifier, and Traffic Selector.

The following term used in this Technical Specification is defined in 3GPP TS 23.402 [3]: IFOM capable UE.

The following terms used in this Technical Specification are defined in 3GPP TS 23.261 [34]: routing address, routing filter, routing rule.

Home network prefix: An IPv6 prefix allocated by the Home Agent to the UE and used by the UE to configure the Home Address. The Home network prefix is uniquely allocated to a UE.

Home Agent: The Home Agent functionality consists in the DSMIPv6 anchor point functionality described in IETF RFC 5555 [2] and IETF RFC 4877 [4]. Based on 3GPP TS 23.402 [3] the HA functionality is implemented in the PDN Gateway.

3.2 Abbreviations

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

BID	Binding Identification Number
DSMIPv6	Dual-Stack MIPv6
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
FID	Flow Identifier
GW	Gateway
HA	Home Agent
MIPv6	Mobile IP version 6
TSi	Traffic Selector - Initiator
TSr	Traffic Selector - Responder
UE	User Equipment

4 General

4.1 Mobility management based on Dual-Stack Mobile IPv6

DSMIPv6 is specified in IETF RFC 6275 [27] and IETF RFC 5555 [2]. The purpose of the DSMIPv6 procedures is to establish, manage and tear down a mobility tunnel between the UE and the HA function. The mobility tunnel establishment is always initiated by the UE, while the mobility tunnel tear down can be initiated either by the UE or the network. Communication between the UE and a correspondent node shall use the bidirectional mode of operation. Route optimization mode of operation is not supported by EPC in this release.

In this specification, the IETF RFC 4877 [4] is used to secure DSMIPv6 signalling. For this purpose, the UE performs an IKEv2 exchange with the HA before establishing the mobility tunnel as described in subclause 5.1.2.2. The details of the security aspects are specified in 3GPP TS 33.402 [18].

The mobility tunnel procedures are performed by the UE for each PDN connection, meaning that if multiple PDNs are accessed by the UE, multiple instances of the procedures are needed. The multiple PDN connections behaviour is specified more in detail in subclause 4.3.

In this specification, the IETF RFC 3963 [29] is used for prefix preservation. For this purpose, the UE uses the implicit mode as stated in IETF RFC 3963 [29] to tell the HA that the home network prefix would be preserved during mobility. The support of this operation is limited to the sending and receiving of IPv6 packets containing IPv6 addresses auto-configured from the home network prefix, in addition to the IPv6 Home Address.

In this specification, the IETF RFC 5648 [31], IETF RFC 6089 [32] and IETF RFC 6088 [33] are used for IFOM. The general principles of IFOM are listed in 3GPP TS 23.261 [34]. For this purpose, the UE can decide if IFOM is to be applied to a PDN connection. The procedures used by the UE to determine which PDN connection IFOM is to be applied and how the IP flows are distributed are specified in 3GPP TS 24.302 [21].

4.2 Identities

The UE shall use Network Access Identifier (NAI) as identification towards the HA in the IKEv2 exchange. During this process, the IPsec security association between the UE and the HA is tied to the user identity, set to the NAI, and to an

SPI uniquely identifying this security association. The NAI is structured according to 3GPP TS 23.003 [17]. The NAI can be either a root NAI, a fast re-authentication NAI or pseudonym identity as specified in 3GPP TS 23.003 [17].

The UE shall use the HA-APN to identify the desired HA in the DNS-based and DHCPv6-based HA discovery procedures. The HA-APN is constructed according to 3GPP TS 23.003 [17].

NOTE: The operator is responsible to configure the DNS system so that the same PDN GW can be discovered via HA-APN and APN. A possible way of configuring the mapping between HA-APN and APN is to create the HA-APN from the respective APN by using the same Network Identifier and by adding the prefix "ha-apn" to the Operator Identifier.

The Binding Update and Binding Acknowledgement shall not explicitly carry an NAI as the IPsec security association is tied to the user identity.

4.3 Multiple PDN connectivity

This specification supports multiple PDN connectivity. The UE can setup multiple PDN connections with a given APN or multiple APNs using multiple DSMIPv6 sessions. There is one DSMIPv6 session per each PDN connection.

NOTE: When a UE is associated to multiple PDN connections, it is possible for the UE to create a tunnel loop amongst the HAs by binding home addresses to each other. This results in the possibility of HA being flooded with packets. Packet flooding is not specific to DSMIPv6 and there exist current implementations to deal with the packet flooding issue. As for the formation of tunnel loop, the solution to solve it in this current specification (Release 9) is implementation specific until a standardized solution emerges.

The procedures described in clause 5 shall be interpreted as procedures which are executed for each PDN connection the UE established. This implies that:

- For the initial attachment of a PDN connection, the UE shall perform a Home Agent address discovery (subclause 5.1.2.1), a security association establishment via IKEv2, including the EAP-AKA authentication and the IPv6 Home Network Prefix assignment (subclause 5.1.2.2), and the initial binding registration (subclause 5.1.2.4).

- The handover procedure shall be performed for each PDN connection separately as described in subclause 5.2.2.

- The re-registration procedure shall be performed for each PDN connection separately as described in subclause 5.3.2.

- The detach procedure shall be performed for each PDN connection separately as described in subclause 5.4.2 or in subclause 5.4.3.

In addition to the above procedures, the following procedures described for an IFOM capable UE configured for IFOM shall be interpreted as procedures which are executed for each PDN connection that the UE has decided to apply the IFOM procedures. This implies that:

- The attach to additional access network procedure, as described in subclause 5.6.2, shall be performed by the UE separately for each PDN connection to which the access is to be the added.

- The inter-access flow mobility procedure, as described in subclause 5.7.2, shall be performed by the UE separately for each PDN connection when IP flows are to be moved amongest access networks.

- The removal of an access network procedure, as described in subclause 5.8.2, shall be performed by the UE separately for each PDN connection using the access network to be removed.

5 Dual-Stack Mobile IPv6 Procedures

5.1 Dual-Stack Mobile IPv6 initial attach

5.1.1 General

The DSMIPv6 initial attach is performed by the UE to establish a DSMIPv6 connection with the node acting as HA. This is also known as the bootstrapping procedure as the UE establishes the security association with the HA. The initial attach involves the following tasks:

- **Discovery of the Home Agent address**. The UE needs to discover the IPv6 address as well as the IPv4 address of the HA.
- **Security association establishment**. The UE needs to establish an IPsec security association with the HA in order to secure the DSMIPv6 signalling. IKEv2 (IETF RFC 4877 [4]) is used to establish this security association.
- **IPv6 Home Network Prefix assignment**. The UE needs to be assigned an IPv6 Network Prefix of its home network in order to configure the global unicast Home Address to be used in DSMIPv6. The HA is responsible of assigning the IPv6 Home Network Prefix to the UE.
- **IPv4 Home Address assignment**. Optionally, a dual-stack UE can also request to be assigned an IPv4 Home Address to be used for IPv4-only applications. The HA is responsible of assigning the IPv4 Home Address to the UE.
- **Home link detection**. The UE needs to perform Home Link Detection before initiate registration with the HA. The DSMIPv6 Home Link Detection Function is used by the UE to detect if it is attached to the home link from a DSMIPv6 perspective.
- **Initial binding registration**. Unless the home link detection procedure indicates the UE is at home, the UE sends a Binding Update message to perform its initial registration with the HA.

If the UE is an IFOM capable UE the DSMIPv6 initial attach involves also the IFOM capability discovery.

If the UE requires additional configuration parameters, e.g. Vendor-specific options, stateless DHCPv4 and DHCPv6 as defined in IETF RFC 4039 [26] and IETF RFC 3736 [13] can be run over the DSMIPv6 tunnel.

5.1.2 UE procedures

5.1.2.1 Discovery of the Home Agent address

5.1.2.1.1 General

The first procedure the UE needs to perform for DSMIPv6 initial attach is the discovery of the node acting as the HA.

The UE can discover the IP addresses of the HA in one of the four following ways:

- via DNS;
- via attach procedure for 3GPP access or trusted non-3GPP access (if supported) based on protocol configuration options;
- via IKEv2 during tunnel setup to ePDG for untrusted non-3GPP accesses;
- via DHCPv6.

If the UE does not obtain the IP addresses of the HA via PCO during the 3GPP or trusted non-3GPP (if supported) attach or via IKEv2 signalling, it shall follow either the procedures described in subclause 5.1.2.1.5 or the procedures described in subclause 5.1.2.1.2. The UE may be configured to perform both procedures in parallel or one of the two procedures only in case the other failed.

5.1.2.1.2 Home agent address discovery based on DNS

A UE performing Home Agent discovery based on DNS shall support the implementation of standard DNS mechanisms.

The UE shall perform DNS Lookup by Home Agent Name as specified in IETF RFC 5026 [10].The QNAME shall be set to the requested HA-APN. The HA-APN shall be constructed as specified in 3GPP TS 23.003 [17]. If a HA has both an IPv4 and an IPv6 address, the corresponding DNS record should be configured with both 'AAAA' and 'A' records. Accordingly the UE should perform one DNS lookup procedure to retrieve both 'AAAA' and 'A' records. The DNS server replies with one 'AAAA' and one 'A' record.

5.1.2.1.3 Home agent address discovery based on protocol configuration options

The UE may request the IPv6 address and optionally the IPv4 address of the dual stack HA using the Protocol configuration options IE during the attach procedure for 3GPP or trusted non-3GPP access or the additional PDN connectivity procedure. The details of this procedure for the case of attach for 3GPP access are described in 3GPP TS 24.301 [15]. The details of this procedure for the case of attach for trusted non-3GPP access are described in 3GPP TS 24.302 [21].

5.1.2.1.4 Home agent address discovery based on IKEv2 signalling

The UE may request the IPv6 and optionally the IPv4 address of the HA during the tunnel establishment procedure with the ePDG. The details of this procedure are described in 3GPP TS 24.302 [21].

5.1.2.1.5 Home agent address discovery based on DHCPv6

The HA address discovery via DHCPv6 is possible in the following cases:

- in 3GPP access, or
- in trusted non-3GPP access, when a DHCPv6 relay exists in the trusted non-3GPP access and the PDN GW is the DHCPv6 server, or
- in trusted non-3GPP access, when the DHCPv6 server is in the trusted non-3GPP access and it has the HA addresse information from static configuration, or received via STa reference point as specified in 3GPP TS 29.273 [20].

A UE performing HA discovery based on DHCPv6 shall support the implementation of stateless DHCPv6 as specified in IETF RFC 3736 [13] and the DHCPv6 options as specified in IETF RFC 6610 [12].

In order to discover the address of the HA the UE shall send an Information-Request message including the "MIP6 Home Network ID FQDN Option" as described in IETF RFC 6610 [12].

In order to connect to a HA for a specific target PDN, the UE shall include the desired HA-APN in the Home Network Identification FQDN field contained in the "MIP6 Home Network ID FQDN Option" as described in IETF RFC 6610 [12].

NOTE: The new options described in IETF RFC 6610 [12] are applicable to DSMIPv6.

The HA information is provided to the UE as described in IETF RFC 6610 [12] in the sub-option contained in the "MIP6 Identified Home Network Information Option". The sub-option can be:

- a "MIP6 Home Agent Address Network Information Option" (the IPv6 address and if available, the IPv4 address of the HA); or
- a "MIP6 Home Agent FQDN Network Information Option" (the HA FQDN) as described in IETF RFC 6610 [12].

In the latter case the UE shall perform a DNS Lookup by Home Agent Name as specified in IETF RFC 5026 [10]. The QNAME shall be set to the received HA FQDN.

If a HA has both an IPv4 and an IPv6 address, the corresponding DNS record should be configured with both 'AAAA' and 'A' records. Accordingly the UE should perform one DNS lookup procedure to retrieve both 'AAAA' and 'A' records. The DNS server replies with one 'AAAA' and one 'A' record.

5.1.2.1a IFOM capability discovery

An IFOM capable UE shall perform HA IFOM capability discovery, i.e. an IFOM capable UE shall discover whether the HA supports IFOM or not. The HA IFOM capability can be performed using the following methods:

- as part of attach procedure for 3GPP access based on protocol configuration options;
- as part of a IKEv2 tunnel setup procedure with the HA; or
- using the information received from ANDSF.

The IFOM capable UE shall support HA IFOM capability discovery performed through IKEv2 tunnel setup procedure. The HA IFOM capability discovery performed within IKEv2 tunnel setup procedure with the HA is described in subclause 5.1.2.2.

If the IFOM capable UE supports IPv6 Home Network Prefix assignment via PCO, the IFOM capable UE shall support HA IFOM capability discovery via PCO.

The IFOM capable UE may use inter system routing policies (see 3GPP TS 24.302 [21] and 3GPP TS 24.312 [36]) to perform the HA IFOM capability discovery for a specific APN. If the IFOM capable UE uses inter system routing policies to perform HA IFOM capability discovery, the UE may skip performing the HA IFOM capability discovery via PCO or the HA IFOM capability discovery via IKEv2.

5.1.2.2 Security association establishment and IPv6 Home Network Prefix assignment

The UE shall support the IKEv2 protocol (see IETF RFC 5996 [14]) for negotiating the IPsec security association to secure DSMIPv6 signalling and shall support EAP over IKEv2 as described in IETF RFC 5996 [14] to perform authentication with an AAA server. In a case an additional authentication and authorization of the IPSec security association is needed with an external AAA server, then the additional authentication steps during the IKEv2 exchange shall be supported as specified in IETF RFC 4739 [23] and the UE shall follow the WLAN UE procedure described in 3GPP TS 33.234 [24].

The UE shall support IPsec ESP (see IETF RFC 4303 [11]) in order to provide authentication of Binding Update and Binding Acknowledgement messages as specified in IETF RFC 4877 [4]. The UE shall support multiple authentication exchanges in the IKEv2 protocol as specified in IETF RFC 4739 [23] in order to support authentication with an external AAA server. The UE shall support the redirect mechanism as defined in IETF RFC 5685 [30].

The UE shall initiate the security association establishment procedure by sending the IKE_SA_INIT request message defined in IETF RFC 5996 [14] to the HA. The UE shall indicate support for the HA reallocation by including a REDIRECT_SUPPORTED payload in the IKE_SA_INIT request as specified in IETF RFC 5685[30]. On receipt of an IKE_SA_INIT response, the UE shall send an IKE_AUTH request message including the MN-NAI in the IDi payload and the Access Point Name (APN) of the target PDN the UE wants to connect to in the IDr payload. The APN shall be formatted as defined in 3GPP TS 23.003 [17]. The username part of the MN-NAI included in "IDi" payload may be an IMSI, pseudonym or re-authentication ID. The UE shall include in the IDi payload the same MN-NAI it includes in the EAP-Response/Identity within the EAP-AKA exchange.

In the very first EAP-Response/Identity within the IKEv2 exchange the UE shall include a NAI whose username is derived from IMSI. In subsequent exchanges the UE should use pseudonyms and re-authentication identities provided by the 3GPP AAA server as specified in IETF RFC 4187 [28].

NOTE: Fast re-authentication mechanism is optional, and therefore is an implementation option in the UE and operator configuration issue (i.e. it also depends on whether the AAA server sent a re-authentication ID during previous EAP authentication) whether to use it during security association establishment.

EAP-AKA over IKEv2 shall be used to authenticate UE in the IKE_AUTH exchange, while public key signature based authentication with certificates shall be used to authenticate the HA.

During the IKEv2 exchange, the HA may trigger the UE to perform the HA reallocation procedure. If the UE receives as part of the IKE_AUTH response message a REDIRECT payload containing the IP address of a target HA as specified in subclause 5.1.3.1, the UE shall initiate a new IKEv2 security association with the target HA. The UE shall terminate the IKEv2 security association with the initial HA by sending an IKEv2 Informational message with a DELETE payload as specified in IETF RFC 5996 [14].

During the IKEv2 exchange, the UE shall request the allocation of an IPv6 home prefix through the Configuration Payload in the IKE_AUTH request message. Since in EPS a unique IPv6 prefix is assigned to the UE, the UE shall include a MIP6_HOME_PREFIX attribute in the CFG_REQUEST payload of the IKE_AUTH request message as described in IETF RFC 5026 [10]. In addition the UE may include the INTERNAL_IP6_DNS attribute in the CFG_REQUEST as described in IETF RFC 5996 [14] to request the DNS server IPv6 address of the PLMN it is connecting to via DSMIPv6. In the same way the UE may include the INTERNAL_IP4_DNS attribute in the CFG_REQUEST payload to request the IPv4 address of the DNS server.

During the IKEv2 exchange, if the UE receives an IKE_AUTH response message containing a Notify Payload with a Private Notify Message Type MAX_CONNECTION_REACHED as specified in 3GPP TS 24.302 [21], the UE shall close the related IKEv2 security association states. As long as none of existing IKEv2 security association is released, the UE shall not attempt to establish any additional IKEv2 security association.

The UE shall then auto-configure a Home Address from the IPv6 prefix received from the HA and shall run a CREATE_CHILD_SA exchange to create the security association for the new Home Address. In the CREATE_CHILD_SA exchange the UE shall include the Home Address and the appropriate selectors in the TSi (Traffic Selector-initiator) payload to negotiate the IPsec security association for protecting the Binding Update and Binding Acknowledgement messages as specified in IETF RFC 4877 [4].

If the UE knows the IPv6 Home Network Prefix of a PDN connection for which the security association is to be setup, the UE shall insert a PDN Identifier notify payload, as defined in annex B, in the IKE_AUTH request message. The PDN Identifier notify payload shall contain the IPv6 Home Network Prefix of the PDN connection for which the security association is being set up. If the UE does not know the IPv6 Home Network Prefix of the PDN connection for which the security association is to be set up, the UE shall not include the PDN Identifier notify payload in the IKE_AUTH request message.

If an IFOM capable UE performs HA IFOM capability discovery via IKEv2 procedure, the IFOM capable UE shall include the IFOM Capability notify payload (as specified in the Annex B.2) in the IKE_SA_INIT request message to perform HA IFOM capability discovery. If the IFOM capable UE receives in the IKE_SA_INIT response message the IFOM Capability notify payload, the IFOM capable UE shall behave as an IFOM capable UE configured for IFOM as the received payload indicates that the HA supports IFOM. If the IFOM capable UE does not receive in the IKE_SA_INIT response message the IFOM Capability notify payload, the IFOM capable UE shall behave as a UE which is not IFOM capable as the received payload indicates that the HA does not support IFOM.

5.1.2.3 Home Link Detection

The DSMIPv6 Home Link Detection Function is used by the UE to detect if an access interface is on the home link for a PDN connection from a DSMIPv6 perspective. The Home Link Detection function shall be performed before sending DSMIPv6 Binding Update via the same access interface.

To perform the Home Link Detection procedure, the UE shall compare the assigned Home Network Prefix for a PDN connection with the IPv6 prefix or prefixes included in the Prefix Information Option in the Router Advertisements received on the local link. The Home Network Prefix can be assigned in a 3GPP access via PCO, as specified in 3GPP TS 24.301 [15], or via IKEv2 as specified in subclause 5.1.2.2. If there is a match between the Home Network Prefix and one of the local prefixes, the UE is attached on the home link over the respective access interface and shall not send a Binding Update to the HA unless the UE currently has a valid DSMIPv6 Binding Update list entry. If the UE has a valid DSMIPv6 Binding Update list entry, the UE shall proceed to perform the action specified in subclause 5.2.2.4. If there is not any match, the UE shall proceed as specified in subclause 5.1.2.4.

NOTE: The UE does not need to run IKEv2 for home link detection if the Home Network prefix is dynamically received in a PCO Information Element.

If the IFOM capable UE performs the Home Network Prefix assignment via Protocol Configuration Option, the IFOM capable UE shall perform in the PDN CONNECTIVITY REQUEST message both Home Network Prefix assignment and the IFOM capability discovery.

5.1.2.4 Initial binding registration and IPv4 Home Address assignment

After establishing the security association and obtaining the IPv6 Home Address, the UE shall send a Binding Update message as specified in IETF RFC 6275 [27] and IETF RFC 5555 [2] in order to register its Home Address and Care-of Address at the HA, if it detects it is in the foreign network.

If both IPv4 and IPv6 Care-of Address are received at the foreign network, the UE shall first attempt to use the IPv6 Care-of Address for its binding registration.

If IPv6 Care-of Address is used for initial binding registration, the UE shall send the Binding Update message to the IPv6 address of the HA. In this Binding Update message the H (home registration) and A (acknowledge) bits shall be set. If the UE needs an IPv4 Home Address, the UE shall include the 0.0.0.0 address in the IPv4 Home Address option to request a dynamic IPv4 Home Address.

When IPv6 Care-of Address is used for initial binding registration, the Alternate Care-of Address option shall be used by the UE to carry the Care-of Address inside a Mobility Header which is protected by ESP. If this option is present, the address included in this option is the same address present in the source address of the IPv6 packet. The Alternate Care-of Address option shall not be included if a BID mobility option is added in the same Binding Update message.

If IPv4 Care-of Address is used for initial binding registration, the UE shall send the Binding Update as follows (see IETF RFC 5555 [2]):

- The IPv6 packet, with the IPv6 Home Address as the Source Address field of the IPv6 header, shall be encapsulated in UDP.
- The UE shall include the IPv4 Care-of Address as the Source Address field of the IPv4 header and the HA IPv4 address as the Destination Address field of the IPv4 header.
- The UE shall include the IPv4 Care-of Address option containing the IPv4 Care-of Address. The IPv4 Care-of Address option shall not be included if a BID mobility option is added in the same Binding Update message.
- The UE shall set the H (home registration) and A (acknowledge) flags.
- The UE shall set the F (UDP encapsulation required) flag to 0.
- The UE shall set the R (Mobile Router Flag) flag to 1.
- If the UE needs an IPv4 Home Address, the UE shall include an IPv4 Home Address option with the 0.0.0.0 address in the Binding Update message, as defined in IETF RFC 5555 [2].

If the UE is an IFOM capable UE configured for IFOM, the UE extends the Binding Update with the following options:

a) The UE shall set the O (Overwrite) flag to "1";

b) The UE shall include a BID identifier mobility option in the Binding Update as specified in IETF RFC 5648 [31];

   - The UE shall set the BID-PRI field to assign the priority to the BID as indicated in IETF RFC 6089 [32]; and

c) The UE may create one or more routing rules with the HA. For each routing rule that the UE wants to register with the HA, the UE shall include a FID mobility option containing one traffic selector as specified in IETF RFC 6089 [32].

   - The FID field shall be set to an arbitrary value;
   - The FID-PRI field shall be set to the assigned priority of the FID as indicated in IETF RFC 6089 [32];
   - A Binding Reference suboption shall be included as defined in IETF RFC 6089 [32]. As indicated in IETF RFC 6089 [32] the value assigned to the BID is the same included in the BID mobility option included in the Binding Update; and
   - Traffic selector suboption shall be set as specified in IETF RFC 6089 [32] and IETF RFC 6088 [33]. The parameters described in the traffic selector suboption represent the routing filter that corresponds to the routing rule that the UE wants to register with the HA.

According to IETF RFC 6089 [32], traffic selector suboption contains parameters identifying downlink traffic, hence routing rules registered with the HA bind either a Care-of Address or a Home Address to the downlink traffic. The same bound IP address shall be used by the IFOM capable UE configured for IFOM to route the corresponding uplink traffic (i.e. asymmetrical routing is not allowed in this version of the specification).

When the UE receives the Binding Acknowledgement from the HA, it shall validate it based on the rules described in IETF RFC 6275 [27] and IETF RFC 5555 [2]. If the Binding Acknowledgement contains the successful status code 0

("Binding Update Accepted"), the UE shall create an entry for the registered Home Address in its Binding Update List and may start sending packets containing its IPv6 Home Address or other IPv6 addresses auto-configured from the assigned home network prefix.

If the Binding Acknowledgement contains a value of 128, the UE may re-send the BU as specified in IETF RFC 6275 [27]. If the Binding Acknowledgement contains a value from 129 to 133 as specified in IETF RFC 6275 [27] or a value from 140 to 143 as specified in IETF RFC 3963 [29], the UE shall not send the BU to the HA and should discover another HA.

If the Binding Acknowledgment contains an IPv4 Address Acknowledgement option with status code value from 0 to 127 (indicating success), the UE shall create two entries in its Binding Update List, one for the IPv6 Home Address and another for the IPv4 Home Address. If the Binding Acknowledgement contains an IPv4 Address Acknowledgment option with status code indicating error (i.e. 128 or higher), the UE shall create an entry only for the IPv6 HoA in its binding update list. Moreover, if the status code is 129 ("Administratively prohibited") or 132 ("Dynamic IPv4 home address assignment not available"), the UE shall not re-send the Binding Update and it shall use only the IPv6 HoA. If the Binding Acknowledgement contains an IPv4 Address Acknowledgement option with status 128 ("Failure, reason unspecified"), 130 ("Incorrect IPv4 home address"), 131 ("Invalid IPv4 address") or 133 ("Prefix allocation unauthorized") it shall re-send the Binding Update including the 0.0.0.0 address in the IPv4 Home Address option. If the Binding Acknowledgement does not contain an IPv4 Address Acknowledgment option, the UE shall create an entry only for the IPv6 HoA in its binding update list.

NOTE 1: The value to be used to identify the IPv4 address acknowledgement option in the mobility header is 30;

If the Binding Acknowledgment contains a BID mobility option, the UE shall process it as specified in IETF RFC 5648 [31]. If the Binding Acknowledgment contains one or more flow mobility options, the UE shall process it as specified in IETF RFC 6089 [32].

If the status field of the BID mobility option is set to zero, the IFOM capable UE configured for IFOM applies to every examined BID option the status code contained in the status field of the Binding Acknowledgement message as indicated in IETF RFC 5648 [31]. If the value of the status field assigned to a BID mobility option is equal to 4 ("MCOA NOTCOMPLETE"), 164 ("MCOA MALFORMED"), 165 ("MCOA NON-MCOA") or 167 ("MCOA UNKOWN COA"), the IFOM capable UE configured for IFOM performs the operations described in IETF RFC 5648 [31].

NOTE 2: the above error cases, e.g. 165 ("MCOA NON-MCOA BINDING EXISTS"), that do not apply to the case of initial attach can apply to other use cases (e.g. attach to additional access).

When processing a FID mobility option, if the value of the status field of the FID mobility option is 129 ("Flow binding rejected"), 130 ("Flow identification mobility option malformed"), 131 ("BID not found") or 132 ("FID not found"), the IFOM capable UE configured for IFOM performs the operations described in IETF RFC 6089 [32].

The UE may then send data traffic either with the IPv6 Home Address or with the IPv4 Home Address. If the UE is located on an IP6-enabled link, it shall send IPv6 packets as described in IETF RFC 6275 [27]; IPv4 traffic shall be encapsulated in IPv6 packets as described in IETF RFC 5555 [2]. If the UE is located on an IPv4-only link and the Binding Acknowledgement contains the NAT detection option with the F flag set, the UE shall send IPv6 and IPv4 packets following the vanilla UDP encapsulation rules specified in IETF RFC 5555 [2]. Otherwise the UE shall send IPv6 and IPv4 packets encapsulated in IPv4 as specified in IETF RFC 5555 [2].

Once the DSMIPv6 tunnel is established, the UE may build a DHCPv4 or DHCPv6 message as described in IETF RFC 4039 [26] or IETF RFC 3736 [13] respectively and send it via the DSMIPv6 tunnel as described in IETF RFC 6275 [27] in order to retrieve additional parameters, e.g. Vendor-specific options. The UE may also request additional IPv6 prefix(es) with length of /64 or shorter by using DHCPv6 Prefix Delegation as defined in IETF RFC 6276 [35].

5.1.3 HA procedures

5.1.3.1 Security association establishment and IPv6 Home Network Prefix assignment

The HA shall support the IKEv2 protocol (see IETF RFC 5996 [14]) for negotiating the IPsec security association to secure DSMIPv6 signalling and shall support EAP over IKEv2 as described in IETF RFC 5996 [14] to perform UE authentication with an AAA server. If an additional authentication and authorization of the IPSec security association

were needed with an external AAA server, then the additional authentication steps during the IKEv2 exchange shall be supported as specified in IETF RFC 4739 [23] and the HA shall follow the PDG procedure defined in 3GPP TS 33.234 [24].

The HA shall support IPsec ESP (see IETF RFC 4303 [11]) in order to provide authentication of Binding Update and Binding Acknowledgement messages as specified in IETF RFC 4877 [4]. The HA shall support multiple authentication exchanges in the IKEv2 protocol as specified in IETF RFC 4739 [23] in order to support authentication with an external AAA server.

The HA shall complete the IKE_SA_INIT exchange as specified in IETF RFC 5996 [14]. The HA shall include in the IDr the same value included by the UE in the IDr payload of the request.

Upon successful authorization and authentication, the HA shall accept the security association establishment request by sending the IKE_AUTH response message with the CFG_REPLY payload including the IPv6 Home Network Prefix allocated to the UE in the MIP6_HOME_PREFIX attribute. This prefix information shall include the prefix length as specified in IETF RFC 5026 [10]. If the UE included the INTERNAL_IP6_DNS or the INTERNAL_IP4_DNS in the CFG_REQUEST payload, the HA shall include the same attribute in the CFG_REPLY payload including zero or more DNS server addresses as specified in IETF RFC 5996 [14].

If the HA needs to reject a IKEv2 security association establishment due to the network policies or capabilities to indicate that no more IKEv2 security association establishment request with any APN can be accepted for the UE, the HA shall include in the IKE_AUTH response message containing the IDr payload a Notify Payload with a Private Notify Message Type MAX_CONNECTION_REACHED as specified in 3GPP TS 24.302 [21].

If the UE included a PDN Identifier notify payload within the IKE_AUTH request message, the HA may apply the following procedure:

1) Process the PDN Identifier notify payload according to IETF RFC 5996 [14]; and

2) Use the IPv6 prefix contained in the payload to identify the PDN connection for which the security association is being set up and

   - if the HA is able to identify the PDN connection for which the security association is being set up, the HA shall insert the previously assigned IPv6 Home Network Prefix in the MIP6_HOME_PREFIX attribute in the CFG_REPLY payload; or

   - if the HA is not able to identify the PDN connection for which the security association is being set up, the HA shall ignore the content of the received PDN Identifier notify payload and allocate an IPv6 Home Network Prefix as described below.

When allocating an IPv6 Home Network Prefix, the HA shall apply one of the following procedures:

- If the IKEv2 message is received over an existing PDN connection, the assigned IPv6 network prefix of the PDN connection shall be sent to the UE as IPv6 Home Network Prefix in the MIP6_HOME_PREFIX attribute; or,

- If the IKEv2 message is not received over an existing PDN connection, and the UE has an existing PDN connection which has no IPSec security association established, the assigned IPv6 network prefix of the PDN connection shall be sent to the UE as IPv6 Home Network Prefix in the MIP6_HOME_PREFIX attribute; or,

- If the IKEv2 message is not received over an existing PDN connection, and the UE does not have an existing PDN connection which has no IPSec security association established, a new IPv6 network prefix shall be allocated and sent to the UE as IPv6 Home Network Prefix in the MIP6_HOME_PREFIX attribute.

An IFOM capable Home Agent shall implement the IFOM Capability notify payload. If the UE included the IFOM Capability notify payload within the IKE_SA_INIT request message, the HA shall perform the following procedures:

- process the IFOM Capability notify payload according to IETF RFC 5996 [14];

- if the HA is IFOM capable, the HA includes the IFOM Capability notify payload in the IKE_SA_INIT response message; and

- if the HA is not IFOM capable, the HA ignores the IFOM Capability notify payload received from the UE and in the IKE_SA_INIT response message will not include the IFOM Capability notify payload.

If the 3GPP AAA server triggers the HA to perform a HA reallocation procedure as specified in 3GPP TS 33.402 [18], the HA learns the IP address of the target HA as specified in 3GPP TS 29.273 [20]. The HA shall provide to the UE the

target HA IP address in the REDIRECT payload during IKE_AUTH exchange as specified in 3GPP TS 33.402 [18]. The encoding of the REDIRECT payload in the IKE_AUTH response message is specified in IETF RFC 5685 [30]. The HA shall not assign an IPv6 prefix to the UE in the IKE_AUTH exchange. The HA shall remove the states of the IKEv2 security association with the UE after receiving an IKEv2 Informational message with a DELETE payload from the UE.

5.1.3.2 Initial binding registration and IPv4 Home Address assignment

When the HA receives a Binding Update message from the UE, it shall validate it as described in IETF RFC 6275 [27] and in IETF RFC 5555 [2]. If the Alternate Care-of Address option is present, the HA shall verify the correctness of the Alternate Care-of Address option. If the Care-of Address specified in the Alternate Care-of Address option and in the Source Address field of the IPv6 header of the Binding Update packet are different, the HA shall reject the request by returning a Binding Acknowledgement with status code 128. If the HA accepts the Binding Update message, it shall create a new entry in its binding cache for UE, marking it as a home registration. The lifetime of this binding cache entry is set based on operator's policies. The HA shall not perform a Duplicate Address Detection on the IPv6 Home Address of the UE because of the uniqueness of the IPv6 prefix assigned by the HA to the UE. Then the HA shall send a Binding Acknowledgement with R bit set to "1" as specified in IETF RFC 6275 [27] and IETF RFC 3963 [29]. The HA may include the Binding Refresh Advice mobility option following rules defined in IETF RFC 6275 [27] to indicate the remaining time until the UE should send a new home binding update.

If the Binding Update contains an IPv4 Home Address option with the 0.0.0.0 IPv4 address, the HA shall assign an IPv4 Home Address to the UE, including an IPv4 Address Acknowledgement option in the Binding Acknowledgement message, as specified in IETF RFC 5555 [2]. If no IPv4 addresses are available at the HA, the HA shall send a Binding Acknowledgement with status code 132 in the IPv4 address acknowledgement option.

If in the received Binding Update the IPv4 Care-of Address in the IPv4 Care-of Address option is not the same as the IPv4 address in the Source Address in the outer IPv4 header then a NAT was in the path. This information shall be included in the Binding Acknowledgement within a NAT Detection option with the F flag set and the Binding Acknowledgement shall be encapsulated based on the vanilla UDP encapsulation specified in IETF RFC 5555 [2].

If a NAT was not detected, the HA shall send the Binding Acknowledgement without any UDP encapsulation; the message shall be encapsulated in an IPv4 header if the Care-of Address is IPv4 or in an IPv6 header if the Care-of Address is IPv6 as specified in IETF RFC 5555 [2].

If the Binding Update contains a BID mobility option, the HA shall process it as specified in IETF RFC 5648 [31]. If one or more FID mobility options are included in the received Binding Update, the HA shall process it as specified in IETF RFC 6089 [32] and IETF RFC 6088 [33]. If binding update is accepted and IP flow mobility is supported, the HA shall insert the BID mobility option into the Binding Acknowledgement message as specified in IETF RFC 5648 [31]. In addition, if the received Binding Update contains FID mobility option, the HA shall create the flow bindings accordingly and insert the FID mobility option into the Binding Acknowledgement message as specified in IETF RFC 6089 [32].

If the binding update is accepted for both IPv4 and IPv6 home addresses, the HA creates two bindings, one for each home address as specified in IETF RFC 5555 [2]. The HA shall link the IPv4 home address binding to the IPv6 home address binding.

NOTE: How the linkage between the two bindings (e.g. separate or single binding cache entry) is performed is implementation specific.

When the binding cache entry is created for the UE, the HA shall tunnel all packets destined to the IPv6 Home Address, the home network prefix and all packets destined to the IPv4 Home Address (if present) to the UE's Care-of Address. If a NAT was detected, packets shall be encapsulated in UDP and IPv4 based on vanilla UDP encapsulation specified in IETF RFC 5555 [2]. If the Care-of Address is an IPv6 address, IPv4 and IPv6 packets shall be encapsulated in an IPv6 header as specified in IETF RFC 6275 [27] and in IETF RFC 5555 [2]; otherwise, if the Care-of Address is an IPv4 address, IPv4 and IPv6 packets shall be encapsulated in an IPv4 header as specified in IETF RFC 6275 [27] and in IETF RFC 5555 [2]. If the HA has multiple binding cache entries with flow bindings (see 3GPP TS 23.261 [34]), the HA shall route all packets destined to the IPv6 Home Address, the home network prefix, the IPv6 prefix(es) assigned through DHCP prefix delegation (if present) and all packets destined to the IPv4 Home Address (if present) as described in IETF RFC 6089 [32].

After the DSMIPv6 tunnel is established, if DHCPv6 Prefix Delegation request is received, the HA may assign additional IPv6 prefix(es) with length of /64 or shorter to the UE as defined in IETF RFC 6276 [35]. Once the DHCPv6 Prefix Delegation procedure has been completed, the HA shall add the assigned delegated prefix(es) into the binding

cache entry as defined in IETF RFC 6276 [35]. When the delegated prefix(es) is included in the binding cache entry for UE, the HA shall tunnel all the packets destined to the delegated prefix(es) to the UE's Care-of Address.

5.1.3.3 Binding Error message

When the HA receives a Binding Update and detects an unrecognized Mobility Header, the HA shall send a Binding Error message with status value 2 "Unrecognized MH Type value" as specified in IETF RFC 6275 [27]. The HA shall include the Home address that was contained in the Home Address destination option.

If NAT was not detected, the HA shall send the Binding Error without any UDP encapsulation; the message shall be encapsulated in an IPv4 header if the Care-of Address is IPv4 or in an IPv6 header if the Care-of Address is IPv6 in the same manner as the Binding Acknowledgement encapsulation specified in IETF RFC 5555 [2].

If NAT was detected, the HA shall send the Binding Error encapsulated in UDP and IPv4 based on vanilla UDP encapsulation specified in IETF RFC 5555 [2].

5.2 Dual-Stack Mobile IPv6 handover

5.2.1 General

The DSMIPv6 handover procedure is performed by the UE to update its Care-of Address at the HA after a movement between two different accesses (e.g. a movement from a 3GPP to a non-3GPP access). The procedure is also used when the Care-of Address is changed for other reasons (e.g. re-allocation of a local IP address or equivalent). When this procedure takes place, the UE has already a valid registration at the HA, which implies that the HA has an entry in its binding cache for that UE and a security association to secure DSMIPv6 signalling is in place between the UE and the HA.

The procedure involves performing the Home Link Detection, setup a security association with the HA if there is no security association existing, and the exchange of a Binding Update and a Binding Acknowledgement between the UE and the HA. For the handover procedure, at the previous access the UE shall already perform discovery of the HA address, and may set up a security association with it, as these steps are part of the initial attach procedure described in subclause 5.1.2.

There are different handover scenarios:

- handover from home link to a foreign link;
- handover from a foreign link to another foreign link; and
- handover from a foreign link to a home link.

5.2.2 UE procedures

5.2.2.1 General

Following a change of access, the UE configures an IP address on the target access system. The details of IP address configuration can be access specific. The handling of the received Binding Acknowledgement is the same as specified in subclause 5.1.2.4.

5.2.2.2 Handover from home link to a foreign link

If the access network supports IPv6, as soon as the UE has received via a Router Advertisement at least an IPv6 prefix which is not present in its Prefix List, the UE shall perform the Home Link detection as specified in subclause 5.1.2.3.

If the UE detects that it is moving from home link to foreign link, and if there is no security association existing with the HA, the UE shall perform the Security association establishment and Home Address assignment procedure with the HA as specified in subclause 5.1.2.2.

Then the UE shall perform the initial binding registration and IPv4 Home Address assignment as specified in subclause 5.1.2.4. In order to maintain IP address preservation for the IPv4 address used in the home link, the UE shall

include the IPv4 address used on the home link in an IPv4 Home Address option in the same Binding Update message. The IFOM capable UE configured for IFOM shall extend the Binding Update message as described in subclause 5.1.2.4.

If the UE does not have an IPv4 Home Address but wants to configure one, the UE shall include the IPv4 Home Address option with the 0.0.0.0 address as specified in subclause 5.1.2.4.

If the access network supports only IPv4, as soon as the UE has configured an IPv4 Care-of Address, the UE shall send a Binding Update tunnelled in UDP as specified in IETF RFC 5555 [2]. The UE shall set the F flag to "0". The UE shall set the R flag to "1".

Independent of an IPv6 or IPv4 access network the UE shall set the Key Management Capability (K) bit in the Binding Update message.

If the UE receives, as response to an outstanding binding registration, a binding acknowledgment having a status code equal to 135 ("Sequence number out of window") and a sequence number different from the one used in the outstanding binding registration, the UE shall accept the binding acknowledgment and process it as specified in IETF RFC 6275 [27].

5.2.2.3 Handover from a foreign link to another foreign link

If the access network supports IPv6, as soon as the UE has received via a Router Advertisement at least an IPv6 prefix which is not present in its Prefix List, the UE shall perform the Home Link detection as specified in subclause 5.1.2.3.

If the UE detects it is not attached to the home link, the UE shall send a Binding Update to the HA including the newly configured IP address as the Care-of Address in the Source IP address of the packet and optionally in the Alternate Care-of Address Option IETF RFC 6275 [27]. The UE build the Binding Update message as specified in IETF RFC 6275 [27].

If the UE has been assigned also an IPv4 Home Address and wants to update also the binding for it, the UE shall include the IPv4 Home Address option including the assigned IPv4 Home Address in the same Binding Update message.

If the UE has been assigned also an IPv4 Home Address and wants to release it, the UE shall not include any IPv4 Home Address option in the same Binding Update.

If the UE does not have an IPv4 Home Address but wants to configure one, the UE shall include the IPv4 Home Address option with the 0.0.0.0 address as specified in subclause 5.1.2.4.

If the access network supports only IPv4, as soon as the UE has configured an IPv4 Care-of Address which is different from the previous Care-of Address, the UE shall send a Binding Update tunnelled in UDP as specified in IETF RFC 5555 [2]. The UE shall set the F flag to "0". The UE shall set the R flag to "1".

Independent of an IPv6 or IPv4 access network the UE shall set the Key Management Capability (K) bit in the Binding Update message.

If the UE is an IFOM capable UE configured for IFOM, the UE extends the Binding Update with the following options:

a) the UE shall set the O (Overwrite) flag to "0";

b) the UE shall include a BID identifier mobility option in the Binding Update as specified in IETF RFC 5648 [31];

- the UE shall set the BID field to the value registered with the Home Agent;
- the UE shall set the BID-PRI field to assign the priority to the BID as indicated in IETF RFC 6089 [32];
- if the newly configured IP address used as Care-of Address is an IPv6 address, the UE shall not insert any Alternate Care-of Address option in the Binding Update message;
- if the newly configured IP address used as Care-of Address is an IPv4 address, the UE shall not insert any IPv4 Care-of Address option in the Binding Update message; and
- the UE shall insert the newly configured IP address used as Care-of Address in the Care-of Address field of the BID identifier mobility option insertd in the Binding Update message;

c) the UE may create one or more routing rules. For each routing rule that the UE wants to register with the HA, the UE shall include a FID mobility option containing one traffic selector as specified in IETF RFC 6089 [32]. Traffic selectors are defined in IETF RFC 6088 [33]:

- the UE shall set the FID field to an arbitrary value;
- the UE shall set the FID-PRI field to assign the priority to the routing filter as indicated in IETF RFC 6089 [32];
- the UE shall include a Binding Reference suboption as indicated in IETF RFC 6089 [32]. The value assigned to the BID identifies the routing address that the UE wants to use to exchange the packets matching the routing filters; and
- traffic selector suboption shall be set as specified in IETF RFC 6089 [32] and IETF RFC 6088 [33]. The parameters described in the traffic selector suboption represent the routing filter that corresponds to the routing rule that the UE wants to register with the HA;

d) The UE may insert a flow summary mobility option (as described in IETF RFC 6089 [32]).

- If the UE wants to keep some routing rules previously registered unmodified, i.e. no flow handover, the UE lists the values of the FIDs identifying the routing rules that the UE wants to keep unmodified in the flow summary mobility option; and
- If the UE wants to remove one or more previously registered routing rules, the UE does not include in the flow summary mobility option the FIDs identifying the routing rules that the UE wants to remove; and

e) the UE may modify one or more routing rules with the HA. For each routing rule that the UE wants to modify, the UE shall include a FID mobility option as specified in IETF RFC 6089 [32].

- the UE shall set the FID field to the value identifying the routing filter the UE wants to handover;
- the UE shall set the FID-PRI field to assign the priority to the BID as indicated in IETF RFC 6089 [32]; and
- the UE shall include a Binding Reference suboption as indicated in IETF RFC 6089 [32]. The value assigned to the BID identifies the routing address that the UE wants to use to exchange the packets matching the routing filters.

The UE shall process the binding acknowledge message as described in subclause 5.1.2.4.

5.2.2.4 Handover from a foreign link to a home link

If the access network supports IPv6, as soon as the UE has received via a Router Advertisement message at least an IPv6 prefix which is not present in its Prefix List, the UE shall perform the Home Link detection as specified in subclause 5.1.2.3 to detect if the UE is attaching to the home link. If the UE detects it is attached to the home link and there is a valid DSMIPv6 Binding Update list entry at the UE, the UE shall send a Binding Update with the Lifetime field set to "0" in order to remove the binding at the HA, as specified in IETF RFC 6275 [27]. If an IPv4 home address was assigned to the UE, as an optimization the UE may not include the IPv4 home address option as the binding for the IPv4 home address will be removed by the HA. Independent of an IPv6 or IPv4 access network the UE shall set the Key Management Capability (K) bit in the de-registration Binding Update message. The UE may preserve the IKEv2 session in order to avoid re-establishing the session when the next handover occurs. If there is not a safe assumption that the UE will remain in the home link (e.g. switching off the non-3GPP radio interface in case of a dual radio terminal), the UE should preserve the IKEv2 session.

If the UE receives a Binding Revocation Indication message from the HA while there is an outstanding unacknowledged Binding Update with Lifetime field set to "0" message, the UE need not send a Binding Revocation Acknowledgement as specified in subclause 5.4.2.1.

5.2.3 HA procedures

5.2.3.1 Handover from home link to a foreign link

In case of UE handover from home link to foreign link, the HA shall support the initial registrstion procedure as specified in subclause 5.1.3.

The error codes used in the Binding Acknowledgement are the same as specified in subclause 5.1.3.2.

5.2.3.2 Handover from a foreign link to another foreign link

When the HA receives a Binding Update from the UE, the HA shall validate it as described in IETF RFC 6275 [27] and in IETF RFC 5555 [2]. If the validation is successful, the HA shall update the binding cache entry related to the Home Address included in the Binding Update.

If the Binding Update is an IPv6 packet, with the Alternate Care-of Address option present, the HA shall verify the correctness of the Alternate Care-of Address option. If the Care-of Address specified in the Alternate Care-of Address option and in the Source Address field of the IPv6 header of the Binding Update packet are different, the HA shall reject the request by returning a Binding Acknowledgement with status code 128. If the option is valid, the HA shall update the binding cache entry with the Care-of Address in the Source Address of the IPv6 header.

If the Binding Update outer header is an IPv4 header and the IPv4 Care-of Address in the IPv4 Care-of Address option is the same as the IPv4 address in the Source Address in the outer IPv4 header, the HA shall update the binding cache entry with the Care-of Address in the IPv4 Care-of Address option and shall send a Binding Acknowledgment encapsulated in IPv4 as specified in IETF RFC 5555 [2].

If in the received Binding Update the IPv4 Care-of Address in the IPv4 Care-of Address option is not the same as the IPv4 address in the Source Address in the outer IPv4 header then a NAT was in the path. This information shall be included in the Binding Acknowledgement within a NAT Detection option with the F bit set. The Binding Acknowledgment shall be encapsulated in UDP and the binding cache updated as specified in IETF RFC 5555 [2].

If the Binding Update contains an IPv4 Home Address option with an IPv4 Home Address previously assigned, the HA shall update also the binding cache entry related to the IPv4 Home Address to the UE. If the Binding Update contains no IPv4 Home Address option, the HA shall remove the binding cache entry related to the IPv4 Home Address of the UE if present.

If the Binding Update contains an IPv4 Home Address option with the 0.0.0.0 IPv4 address, the HA shall assign an IPv4 Home Address to the UE, including an IPv4 Address Acknowledgement option in the Binding Acknowledgement message.

The error codes used in the Binding Acknowledgement are the same as specified in subclause 5.1.3.2.

If the Binding Update contains a BID mobility option and (optionally) a Flow summary mobility option, the HA shall process the received Binding Update message and send a Binding Acknowledgement message as described in subclause 5.1.3.2.

If the Key Management Mobility Capability (K) bit is set in the Binding Update and the HA supports the feature, the HA updates its IKEv2 security associations to include the UE's Care-of Address as the peer address and the Binding Acknowledgement is returned with the K bit set.

The HA shall set the R bit to "1" in the Binding Acknowledgement.

5.2.3.3 Handover from a foreign link to a home link

When a UE hands over from a foreign link to its home link, a network based mobility protocol (PMIPv6 or GTP) in the home link creates a binding cache entry for the UE. The DSMIPv6 binding cache entry that was created by the UE on the foreign link shall not be overwritten. The downlink UE packets shall be processed by the HA based on the DSMIPv6 binding cache entry before the DSMIPv6 binding cache entry is removed.

The DSMIPv6 binding cache entry shall be removed when a Binding Update with lifetime field set to "0" is received by the HA from the UE. The HA shall process the message as per IETF RFC 5555 [2] and IETF RFC 6275 [27], removing the associated binding cache entry and sending the Binding Acknowledge message with the Status field set to "0" (Binding Update accepted). If an IPv4 home address was assigned to the UE, the HA shall also remove the binding for the IPv4 home address tied to the IPv6 home address included in the Binding Update.

If the HA decides to remove the DSMIPv6 binding cache entry of the UE, prior to receiving a binding update with lifetime set to "0" from the UE , the HA shall send a Binding Revocation Indication message as specified in subclause 5.4.3.1.

NOTE: As described above, if the HA receives a Binding Update with Lifetime field set to "0", the HA removes the associated binding cache entry, but additionally the HA can store some data of the binding cache entry for a certain time in order to allow the HA to identify a delayed Binding Update registration message arriving at the HA after the Binding Update de-registration.

5.3 Dual Stack Mobile IPv6 Re-Registration

5.3.1 General

The DSMIPv6 Re-Registration procedure can occur at any time when the UE is already registered at the HA. The procedure is initiated by the UE when it wishes to extend the lifetime of an existing registration, e.g. in case the lifetime is expiring. The procedure can also be initiated by the UE when it wishes to request an IPv4 home address or to release the IPv4 binding while maintaining the IPv6 binding. The procedure may also be initiated by the UE as a mechanism to refresh the NAT bindings in order to be reachable from the HA.

NOTE: The usage of BU messages for keepalive purposes can have impacts to the battery life of the UE. The UE can be configured to rate limiting or avoid NAT keepalive as specified in IETF RFC 5555 [2].

5.3.2 UE procedures

As specified in IETF RFC 6275 [27], if the UE wants to extend the validity of an existing binding at the HA, the UE shall send a new Binding Update to the HA before the expiration of the lifetime indicated in the received Binding Acknowledgement, even if it is not changing its primary Care-of Address. This Binding Update is usually referred as periodic Binding Update.

The UE shall follow the rules described in IETF RFC 6275 [27], IETF RFC 5555 [2] and in subclause 5.1.2.4 to send a periodic Binding Update and handle the associated Binding Acknowledgement. As the UE has not performed any handover, the UE shall confirm the already registered Care of Address and shall indicate the desired lifetime value. In a periodic Binding Update the UE may request an IPv4 Home Address.

If a NAT was detected and the UE is not exchanging data traffic, the UE may send a re-registration Binding Update in order to refresh the NAT binding. The Binding Update shall be sent with the interval contained in the Refresh Time field of the NAT detection option received when the NAT was detected. If the Refresh Time field was set to all 1s, the UE shall use the Binding Acknowledge lifetime as reference interval to send NAT keepalives Binding Updates.

The UE may also send a re-registration Binding Update with the purpose of requesting an IPv4 Home Address.

The UE may also send a re-registration Binding Update for the purpose of releasing the IPv4 Home Address previoulsy assigned. For this purpose, the UE shall follow the rules described in IETF RFC 5555 [2] sending a re-registration Binding Update containing no IPv4 Home Address option.

If the UE is an IFOM capable UE configured for IFOM, the UE extends the Binding Update with the following options:

a) the UE shall set the O (Overwrite) flag to "0";

b) the UE shall include a BID identifier mobility option in the Binding Update as specified in IETF RFC 5648 [31];

   - the UE shall set the BID field to the value identifying the Binding it wants to re-register;

   - the UE shall set the BID-PRI field to assign the priority to the BID as indicated in IETF RFC 6089 [32]; and

c) if the UE previously registered in the HA one or more routing filters, the UE shall include a flow summary mobility option as specified in IETF RFC 6089 [32] listing the values of the FIDs identifying the registered routing filter.

5.3.3 HA procedures

When the HA receives a periodic Binding Update message from the UE, it shall validate it as described in subclause 5.1.3.2, in IETF RFC 6275 [27], IETF RFC 5555 [2] and IETF RFC 5648[31].

In processing a periodic Binding Update the HA shall follow the rules described in subclause 5.1.3.2. In addition if the Binding Update does not include the IPv4 home address option the HA shall remove any associated IPv4 binding cache entry and continue to maintain the IPv6 binding.

If the HA accepts the Binding Update message, it shall update the lifetime and sequence number of the existing entry in its binding cache for the Home Address. If the Binding Update contains a BID mobility option, the HA shall process it as specified in IETF RFC 5648 [31] and IETF RFC 6089 [32]. If binding update is accepted, the HA shall insert the BID mobility option into the Binding Acknowledgement message as specified in IETF RFC 5648 [31]. The Care-of Address is not updated as the periodic Binding Update is not used to update the Care-of Address.

5.4 Dual-Stack Mobile IPv6 detach

5.4.1 General

The DSMIPv6 detach is performed by the UE to close the DSMIPv6 session and the respective IKEv2 session or by the network to inform the UE that it does not have access to a specific PDN through DSMIPv6 any longer. After the DSMIPv6 detach procedure, the UE still has IP connectivity provided by the access network.

There are two explicit detach procedures:

- UE-initiated detach procedure: in this case the UE performs a DSMIPv6 de-registration with the HA and closes the IKEv2 session.
- HA-initiated detach procedure: in this case the HA informs the UE that the DSMIPv6 binding is no more valid. The UE shall then perform the network-initiated detach procedure.

5.4.2 UE procedures

5.4.2.1 Network-initiated detach

Upon receiving a Binding Revocation Indication (BRI) message according to IETF RFC 5846 [19] from the HA, the UE first shall perform the required validity checks on the BRI according to IETF RFC 5846 [19].

The UE shall send a Binding Revocation Acknowledgement (BRA) as specified in IETF RFC 5846 [19]. In this message the UE shall set the status field to 'Success' to reflect that it has received the BRI message. The BRA message may be tunnelled in UDP or IPv4 as specified in subclause 5.1.2.4 for Binding Update messages.

The UE then shall remove the entry identified in the BRI as deregistered from its binding update list and shall use the procedures defined in IETF RFC 5996 [14] to remove the IPsec security associations associated with the DSMIPv6 registration as described in subclause 5.4.2.2.

5.4.2.2 UE-initiated detach

To detach from a specific PDN to which it is connected through a DSMIPv6 session, the UE shall send a Binding Update with the Lifetime field set to 0 as specified in IETF RFC 6275 [27].

The UE shall use the procedures defined in the IKEv2 protocol in IETF RFC 5996 [14] to remove the IPsec security associations associated with the DSMIPv6 registration. The UE shall close the security associations associated with the DSMIPv6 registration and instruct the HA to do the same by sending the INFORMATIONAL request message including a DELETE payload. The Protocol ID in the DELETE payload shall be set to "1" (IKE) to indicate that all IPsec ESP security associations that were negotiated within the IKEv2 exchange shall be deleted.

5.4.3 HA procedures

5.4.3.1 Network-initiated detach

As soon as it receives a trigger for network-initiated detach procedure (see 3GPP TS 29.273 [20]) the HA shall send a Binding Revocation Indication (BRI) message according to IETF RFC 5846 [19] to the UE. The message shall contain the Home Address, corresponding to the PDN connection which shall be removed. The HA shall set the P (Proxy

Binding) bit to 0 (Not Proxy MIPv6 binding), G bit (Global) to 0 (only the PDN Connection specified by the HoA is removed) and V bit (IPv4 HoA Binding Only) to 0 (Not to terminate the IPv4 Home Address binding only). The revocation trigger value shall be set to 1 (Unspecified). The HA shall include the UE home address in the Type 2 routing header as per IETF RFC 5846 [19] and shall not include any mobility option. The HA shall not include a BID option in the BRI message. The BRI message may be tunnelled in UDP or IPv4 as specified in subclause 5.1.3.2 for Binding Acknowledgement messages.

The HA shall follow procedures according to IETF RFC 5846 [19] to await the receipt of a Binding Revocation Acknowledgment (BRA) message from the UE. These procedures are based on the timer MINDelayBRIs defined in IETF RFC 5846 [19]. The HA shall not remove the entry from its binding cache before receiving the BRA.

If the HA receives a Binding Update with Lifetime set to 0 after initiating the network-initiated detach procedure, the HA should treat the BU as acknowledgement to the BRI for the purposes of completing the revocation procedures that are defined in IETF RFC 5846 [19]; in this case, the HA shall remove the respective entry in its binding cache, deleting the timer MINDelayBRIs and respond with a Binding Acknowledgement according to IETF RFC 5555 [2] and IETF RFC 6275 [27].

5.4.3.2 UE-initiated detach

When the HA receives a Binding Update with the Lifetime field set to 0, it shall delete any existing entry for the Home Address included in the Binding Update. Then the HA shall send a Binding Acknowledgement as specified in IETF RFC 5555 [2] and IETF RFC 6275 [27].

On receipt of the INFORMATIONAL request message including a DELETE payload indicating that the UE is deleting the IPsec security associations associated with the DSMIPv6 registration, the HA shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the UE.

5.5 Void

5.5A Protection of data traffic

5.5A.1 General

UE and HA can use the IKEv2 CREATE_CHILD_SA exchange procedure to create a child security association to be used to provide integrity protection, confidentiality protection or both, to all data traffic exchanged within the DSMIPv6 tunnel. The procedure can be initiated by the HA or by the UE at any time after the security association between UE and HA has been set up. If both UE and HA independently decide to initiate the child security association establishment, the procedure described in IETF RFC 5996 [14] applies. The profiles for tunnel mode IPsec ESP are defined in 3GPP TS 33.402 [18].

5.5A.2 UE procedures

After establishing the IPsec security association with the HA as described in subclause 5.1.2.2, the UE may initiate the creation of child security association pair to provide integrity protection, confidentiality protection or both. If the UE determines that the trust relationship of the non-3GPP access network is "untrusted" (see 3GPP TS 24.302 [21]), the UE shall not initiate the creation of child security association. If the UE initiates the creation of child security association pair, the UE shall send to the HA a CREATE_CHILD_SA request as described in IETF RFC 4877 [4] and IETF RFC 5996 [14] with the following additions:

a) the content of the Security Association payload is set accordingly for integrity protection, confidentiality protection or both as indicated in IETF RFC 5996 [14] using the IPsec profiles defined in 3GPP TS 33.402 [18]; and

b) the TSi shall contain all the Home Network Prefix assigned to the UE. If prefix delegation is used, the TSi shall also contain all the prefix(es) provided to the UE. If the UE received an IPv4 Home Address, the TSi shall also contain the IPv4 Home Address.

When the UE receives a CREATE_CHILD_SA request from the HA with selectors indicating the DSMIPv6 tunnel traffic, if the UE supports integrity protection, confidentiality protection or both, the UE shall reply with a

CREATE_CHILD_SA response selecting the preferred transform proposed by the HA as specified in IETF RFC 5996 [14].

If the child SA is created successfully, the UE shall start encapsulating all the uplink packets in the DSMIPv6 tunnel in an IPsec ESP tunnel as negotiated with the HA during the CREATE_CHILD_SA procedure.

The UE can stop using integrity protection, confidentiality protection or both, for the DSMIPv6 tunnel traffic. In order to do that, the UE shall delete the respective child security association by sending an INFORMATIONAL request message including the DELETE payload as specified in IETF RFC 5996 [14].

5.5A.3 HA procedures

After establishing the IPsec security association with the UE as described in subclause 5.1.3.1, the HA may initiate the creation of child security association pair to provide integrity protection, confidentiality protection or both. If the HA receives the trust relationship indication as "untrusted" from the 3GPP AAA server during the authentication and authorization procedure or the authorization procedure (see 3GPP TS 29.273 [20]), the HA shall not initiate the creation of child security association procedure. If the trust relationship indication is not received, the initiation of the creation of the child security association is implementation dependent (e.g. based on configuration). If the HA initiates the creation of child security association pair, the HA shall send to the UE a CREATE_CHILD_SA request as described in IETF RFC 4877 [4] and IETF RFC 5996 [14] with the following additions:

a) the content of the Security Association payload is set accordingly for integrity protection, confidentiality protection or both as indicated in IETF RFC 5996 [14] using the IPsec profiles defined in 3GPP TS 33.402 [18]; and

b) the TSi shall contain all the Home Network Prefix assigned to the UE. If prefix delegation is used, the TSi shall also contain all the prefix(es) provided to the UE. If the UE received an IPv4 Home Address, the TSi shall also contain the IPv4 Home Address.

When the HA receives a CREATE_CHILD_SA request from the UE with selectors indicating the DSMIPv6 tunnel traffic, if the HA supports integrity protection, confidentiality protection or both, the HA shall check whether the child security association establishment can be accepted or not. If the HA receives the trust relationship indication set to "untrusted" indication from the 3GPP AAA server (see 3GPP TS 29.273 [20]), the HA shall reject the child security association establishment by using the NOTIFY payload of type "NO_ADDITIONAL_SAS" in the CREATE_CHILD_SA response. If HA does not receive the trust relationship indication, whether to accept or reject the child security association is implementation dependent. Otherwise, the HA shall reply with a CREATE_CHILD_SA response selecting the preferred transform proposed by the HA as specified in IETF RFC 5996 [14].

If the child SA is created successfully, the HA shall start encapsulating, all the uplink packets in the DSMIPv6 tunnel in an IPsec ESP tunnel as negotiated with the UE during the CREATE_CHILD_SA procedure.

The HA can stop using integrity protection, confidentiality protection or both, for the DSMIPv6 tunnel traffic. In order to do that, the HA shall delete the respective child security association by sending an INFORMATIONAL request message including the DELETE payload as specified in IETF RFC 5996 [14].

5.6 Attach to additional access network

5.6.1 General

The operations defined within subclause 5.6 apply to an IFOM capable UE configured for IFOMand a HA supporting IFOM.

The attach to additional access network procedure is performed by a UE supporting IFOM that has already established a PDN connection through an access network and decides to extend the PDN connection to another access network.

There can be two possible scenarios:

- the existing access network is a home link and the added access network is a foreign link; or
- the existing access network is a foreign link and the added access network is a home link.

The attach to additional access network procedure involves performing the following:

- access specific procedure to connect and configure an IP address for the added access network;
- discovery of a HA IP address if the UE has not obtained the IP address of the HA;
- home link detection;
- setting up a security association if there is no security existing association between the UE and HA; and
- exchange of Binding Update and Binding Acknowledgement with the BID mobility option and FID mobility option between the UE and HA.

5.6.2 UE procedures

5.6.2.1 General

For the attach to additional access network procedure, the UE is already attached to either a home link or foreign link and discovers a new link. The UE applies the DSMIPv6 Home Link Detection Function as specified in subclause 5.1.2.3 to determine if the new link will be a home link or a foreign link. If the new link is a home link, the UE follows the procedure as specified in subclause 5.6.2.2. If the new link is a foreign link, the UE follows the procedure as specified in subclause 5.6.2.3.

5.6.2.2 Attach to additional access network acting as home link

The UE shall perform the DSMIPv6 Home Link Detection Function as specified in subclause 5.1.2.3.

In addition, the UE shall perform the initial binding registration and IPv4 Home Address assignment as specified in subclause 5.1.2.4 with the following additional rules:

a) the UE shall send a Binding Update through the home link;

b) the O (Overwrite) flag in the Binding Update shall be set to "0";

c) the UE shall insert a BID mobility option in this Binding Update with:

   - the 'H' flag in the BID mobility option set to "1";
   - the Care-of Address field set to the IPv6 Home Address of the binding; and
   - the BID-PRI field set to assign the priority to the BID as indicated in IETF RFC 6089 [32];

d) if routing filters were previously registered with the HA, the UE shall include a flow summary mobility option as specified in IETF RFC 6089 [32] listing the values of the FIDs identifying the routing filter that were previously registered; and

e) if the UE creates one or more routing rules as specified in subclause 5.1.2.4, for each FID mobility option, the value of the BID field in the Binding Reference suboption identifies the routing address that the UE wants to use to exchange packets matching the routing filter.

When the UE receives the Binding Acknowledgment from the HA, the UE shall process the Binding Acknowledgment as specified in subclause 5.1.2.4.

5.6.2.3 Attach to an additional access acting as foreign link

The UE shall perform the same procedures described in subclause 5.1.2.4. The UE shall send the Binding Update message through the added link. In addition, the UE shall register the binding for the home link by including a BID mobility option in the Binding Update message. The BID mobility option fields for the binding for the home link are those indicated in IETF RFC 5648 [31] for home binding with the following distinctions:

(a) the H flag shall be set to "1";

(b) the Care-of Address field shall be set to the IPv6 HoA of the binding; and

(c) the BID-PRI field shall be set to the assigned priority of the BID as indicated in IETF RFC 6089 [32].

The UE shall process the received Binding Acknowledgement as specified in subclause 5.1.2.4.

5.6.3 HA procedures

5.6.3.1 General

The following subclauses describe the detailed HA procedures for the case when a UE is attaching to an additional access network.

5.6.3.2 Attach to an additional access network acting as home link

When receiving a Binding Update from the UE, the HA performs the same procedure as specified in subclause 5.2.3.2. In addition, the HA shall validate the Binding Update as described in IETF RFC 5648 [31], IETF RFC 6089 [32] and IETF RFC 6088 [33].

5.6.3.3 Attach to additional access acting as foreign link

When receiving a Binding Update from the UE, the HA performs the same procedures described in subclause 5.2.3.2 and in addition the HA shall validate the Binding Update as described in IETF RFC 5648 [31], and IETF RFC 6089 [32] and IETF RFC 6088 [33]. As described in IETF RFC 5648 [31], the HA shall:

- process the IPv6 address contained in the BID option with the H flag set to 0 as the Care-of Address; and
- process the IPv4 address contained in the BID option with the H flag set to 0 in the same way as the HA process the address contained in the IPv4 Care-of Address option in subclause 5.2.3.2.

5.7 Inter-access flow mobility

5.7.1 General

The operations defined within this sub-clause apply to an IFOM capable UE configured for IFOM and to HA supporting IFOM.

The inter-access flow mobility is performed by the UE supporting IFOM that already established a PDN connection and exchanges packets belonging to the PDN connection through multiple access networks. The UE has previously registered one or more routing rules with the HA.

In this procedure, the UE updates the HA by performing any of the following operations:

- assigning one or more routing filters to an access network different from the one those routing filters were previously assigned;
- adding one or more new routing rules to the HA; or
- removing one or more previously registered routing rules from the HA.

The procedure involves the exchange of a Binding Update and a Binding Acknowledgement with BID and FID options between the UE and the HA.

5.7.2 UE procedures

The UE performs the same procedures described in subclause 5.3.2 with the following exceptions:

- the UE shall set the O (Overwrite) flag to 0;
- the UE shall not include any Alternate Care-of Address option in the Binding Update message; and
- the UE shall not include any IPv4 Care-of Address option in the Binding Update message.

In addition, the UE shall extend the Binding Update message with the following options (see IETF RFC 5648 [31], IETF RFC 6089 [32] and IETF RFC 6088 [33]):

a) The UE shall include a BID identifier mobility option:

- the BID field is set to the value identifying the routing address used as IP Source Address of the Binding Update message;
- if the Binding Update message is sent over a home link, the "H" flag is set to 1;
- if the Binding Update message is sent over a foreign link, the "H" flag is set to 0;
- the BID-PRI priority field is set to the priority assigned to the BID as indicated in IETF RFC 6089 [32]; and
- if the routing address is an IPv4 address, a NAT was detected and the UE is not exchanging data traffic, the UE may insert the routing address in the Care-of Address field of the BID mobility option;

b) the UE may create one or more routing rules. For each routing rule that the UE wants to register with the HA, the UE shall include a FID mobility option containing one traffic selector as specified in IETF RFC 6089 [32]. Traffic selectors are defined in IETF RFC 6088 [33]:

- the UE shall set the FID field to an arbitrary value;
- the UE shall set the FID-PRI field to assign the priority to the routing filter as indicated in IETF RFC 6089 [32];
- the UE shall include a Binding Reference suboption as indicated in IETF RFC 6089 [32]. The value assigned to the BID identifies the routing address that the UE wants to use to exchange the packets matching the routing filters; and
- traffic selector suboption shall be set as specified in IETF RFC 6089 [32] and IETF RFC 6088 [33]. The parameters described in the traffic selector suboption represent the routing filter that corresponds to the routing rule that the UE wants to register with the HA;

c) The UE may insert a flow summary mobility option (as described in IETF RFC 6089 [32]).

- If the UE wants to keep some routing rules previously registered unmodified, i.e. no flow handover, the UE lists the values of the FIDs identifying the routing rules that the UE wants to keep unmodified in the flow summary mobility option; and
- If the UE wants to remove one or more previously registered routing rules, the UE does not include in the flow summary mobility option the FIDs identifying the routing rules that the UE wants to remove; and

d) the UE may modify one or more routing rules with the HA. For each routing rule that the UE wants to modify, the UE shall include a FID mobility option as specified in IETF RFC 6089 [32].

- the UE shall set the FID field to the value identifying the routing filter the UE wants to handover;
- the UE shall set the FID-PRI field to assign the priority to the BID as indicated in IETF RFC 6089 [32]; and
- the UE shall include a Binding Reference suboption as indicated in IETF RFC 6089 [32]. The value assigned to the BID identifies the routing address that the UE wants to use to exchange the packets matching the routing filters.

The handling of the received Binding Acknowledgement message is the same as specified in subclause 5.1.2.4. In addition, the UE handles the FID and BID mobility options contained in the received Binding Acknowledgment message as specified in IETF RFC 5648 [31], IETF RFC 6089 [32] and IETF RFC 6088 [33].

5.7.3 HA procedures

When receiving a Binding Update from the UE, the HA performs the same procedures described in subclause 5.3.3 and in addition the HA shall validate the Binding Update as described in IETF RFC 5648 [31], IETF RFC 6089 [32] and IETF RFC 6088 [33].

5.8 UE-initiated removal of an access network from a PDN connection

5.8.1 General

The operations defined within this sub-clause apply to an IFOM capable UE configured for IFOM and to HA supporting IFOM.

The removal of an access network from a PDN connection procedure is initiated by a UE which has a PDN connection through multiple access networks. In this procedure, the UE stops using one of the access network for the PDN connection.

The procedure involves the exchange of a Binding Update and a Binding Acknowledgement between the UE and the HA.

There can be two possible scenarios:

- home link access network is removed and foreign link access network is maintained; or
- foreign link access network is removed and home link access network is maintained.

5.8.2 UE procedures

5.8.2.1 General

The removal of an access network from a PDN connection is performed by a UE attached to multiple access networks. The UE sends a Binding Update message in order to update the HA binding cache removing the entry corresponding to the removed access network. If the removed access network is a home link, the UE follows the procedure as specified in subclause 5.8.2.2. If the removed access network is a foreign link, the UE follows the procedure as specified in subclause 5.8.2.3.

5.8.2.2 Removal of Home link access

If the UE removes the home link from a specific PDN connection, the UE shall perform one of the following operations:

(a) the UE sends a Binding Update with the Lifetime field set to 0 as specified in IETF RFC 5555 [2] and IETF RFC 6275 [27] and with a BID mobility option. The UE populates the BID mobility option as follows (see IETF RFC 5648 [31]):

- the BID identifier field is set to the BID corresponding to the access network the UE wants to remove;
- the H flag is set to 0; and
- the Care-of Address field in the BID mobility option is omitted;

or:

(b) the UE sends a Binding Update message as indicated in subclause 5.1.2.4 with the following additions:

- the Binding Update message shall be exchanged through the maintained access network;
- the BID identifier field is set to the value identifying the maintained access network; and
- the Care-of Address field in the BID mobility option is omitted.

NOTE: The choice of the operation to follow is up to UE implementation.

5.8.2.3 Removal of foreign link from a PDN connection

If the UE removes an access network acting as foreign link from a specific PDN connection and maintains the connection to the PDN through the home link, the UE shall send a Binding Update message with the Lifetime field set

to 0 as specified in subclause 5.4.2.2.If the UE decides to close the security association set up with the HA, the UE shall send the INFORMATIONAL request message including a DELETE payload as specified in subclause 5.4.2.2.

5.8.3 HA procedures

5.8.3.1 General

The following subclauses describe the detailed HA procedures for the case when a UE is removing an access network from a PDN connection.

5.8.3.2 Removal of home link access from a PDN connection

In case of removal of a home link from a PDN connection executed by the UE, the HA shall perform the following operations:

- if the Lifetime field of the received Binding Update is set to 0, the HA processes the received Binding Update message as described in IETF RFC 5555 [2] and IETF RFC 6275 [27] and IETF RFC 5648 [31]; and
- if the Lifetime field of the received Binding Update is not set to 0, the HA shall perform the same procedures described in subclause 5.6.3.3.

5.8.3.3 Removal of foreign link from a PDN connection

When the HA receives a Binding Update with the Lifetime field set to 0, the HA shall perform the same procedures described in subclause 5.4.3.2.

5.9 Network-initiated removal of an access network from a PDN connection

5.9.1 General

The operations defined within this subclause apply to IFOM capable UE configured for IFOM and to HA supporting IFOM.

The removal of an access network from a PDN connection procedure is initiated by the HA for a UE that has an established PDN connection through multiple access networks with the HA. In this procedure, the HA informs the UE that an entry in the binding cache is no more valid over one of the access network for the PDN connection. The UE then performs the network-initiated removal of an access network from a PDN connection procedure.

The procedure involves the exchange of a Binding Revocation Indication (BRI) message and a Binding Revocation Acknowledgement (BRA) between the UE and the HA as specified in IETF RFC 5846 [19].

Once the procedure is completed, the UE uses the maintained access network for the PDN connection.

There can be two possible scenarios:

- home link access network is removed and foreign link access network is maintained; or
- foreign link access network is removed and home link access network is maintained.

5.9.2 UE procedures

5.9.2.1 General

The following subclauses describe the detailed UE procedures for the case when the HA removes an access network from a PDN connection.

5.9.2.2 Removal of home link access from a PDN connection

Upon receiving a BRI message with a BID option, the UE shall perform the procedure as specified in subclause 5.4.2.1 with the following additions:

- the UE shall process the BID mobility option as specified in IETF RFC 5846 [19];
- the UE shall include the received BID mobility option in the BRA as specified in IETF RFC 5846 [19]; and
- the UE shall not close the security associations set up with the HA.

5.9.2.3 Removal of foreign link from a PDN connection

Upon receiving a BRI message without a BID mobility option from the HA, the UE shall process the BRI message as specified in subclause 5.4.2.1. If the UE decides to close the security association set up with the HA, the UE shall send the INFORMATIONAL request message including a DELETE payload as specified in subclause 5.4.2.2.

5.9.3 HA procedures

5.9.3.1 General

The following subclauses describe the detailed HA procedures for the case when the HA removes an access network from a PDN connection.

5.9.3.2 Removal of home link access from a PDN connection

In order to remove the home link access from a PDN connection, the HA shall perform the procedure as specified in subclause 5.4.3.1 with the following additions:

- the HA shall include a BID mobility option of the home link access in the BRI message sent to the UE; and
- the HA shall only remove the home binding of the the PDN connection from the HA binding update cache, when a BRA message with the same BID mobility option is received.

5.9.3.3 Removal of foreign link from a PDN connection

In order to remove the foreign link access network from a PDN connection, the HA shall perform the network initiated detach procedure by sending a BRI message without a BID mobility option as described in subclause 5.4.3.1.

If an INFORMATIONAL request message including a DELETE payload is received, the HA shall perform the procedure as specified in subclause 5.4.3.2.

Annex A (normative): Message Details

A.1 General

Only the message fields and the mobility options used in the DSMIPv6 procedures defined in this TS are present in this annex. Unspecified message fields and mobility options are not used by this specification.

The IP header, the home address destination option, and type 2 routing header option of the DSMIPv6 signalling messages are not included in this annex. They shall be set in the message as defined in the IETF RFC 6275 [27], IETF RFC 5555 [2] and IETF RFC 5846 [19].

Only the message fields and mobility options used for normal cases in this TS are present in this annex.

A.2 Initial Binding Registration

A.2.1 Binding Update

The fields of a BU message for the DSMIPv6 Initial Binding Registration procedure are depicted in Table A.2.1-1.

The Mobility Options in a BU message for the DSMIPv6 Initial Binding Registration procedure are depicted in Table A.2.1-2.

Table A.2.1-1: Fields of a BU message for the DSMIPv6 Initial Binding Registration procedure

Fields	Fields Description	Reference
Sequence Number	Set to a monotonically increasing value.	IETF RFC 6275 [27]
Lifetime	Set to the requested number of time in units of 4 seconds the binding shall remain valid.	IETF RFC 6275 [27]
Home Registration (H)	Set to "1" to indicate receiving node should act as this node's HA	IETF RFC 6275 [27]
Link-local Address Compatibility (L)	The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 6275 [27]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 6275 [27]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]
Overwrite Flag (O)	Set to "1" to indicate replacing all binding cache entries at the HA with the entries listed in the Binding Update.	IETF RFC 5648 [31]

Table A.2.1-2: Mobility Options in a BU message for the DSMIPv6 Initial Binding Registration procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Home Address option	O	Set to the value "0.0.0.0" to request allocation for the UE. The "P" flag is set to '0'. The Prefix Length is set to the requested prefix length of '32'.	IETF RFC 5555 [2]
IPv 4 Care-of Address	C	Set to the IPv4 Care-of address when in an IPv4 Access Network.	IETF RFC 5555 [2]
Alternate Care-of Address	C	Used (in addition to the Source address of the IPv6 packet) to carry the IPv6 care-of address when in an IPv6 access network.	IETF RFC 6275 [27]
Binding Identifier mobility option	O	The BID and BID-PRI are set to an arbitrary value. For registration of a home link, the "H" flag is set to "1" and the value of the CoA field is the Home Address. For registration of a foreign link, the "H" flag is set to "0" and the value of the CoA field is the Care-of Address.	IETF RFC 5648 [31], IETF RFC 6089 [32]
Flow Identification mobility option	O	The FID and FID-PRI are set to an arbitrary value. The Action field is set to indicate the action taken by the receiver of the Binding Update. The sub-option field conveys the Traffic Selector sub-option.	IETF RFC 6089 [32], IETF RFC 6088 [33]
Flow Summary mobility option	O	Contain one or more FIDs present in the binding update list to refresh the respective flow bindings.	IETF RFC 6089 [32]

A.2.2 Binding Acknowledgement

The fields of a BA message for the DSMIPv6 Initial Binding Registration procedure are depicted in Table A.2.2-1.

The Mobility Options in a BA message for the DSMIPv6 Initial Binding Registration procedure are depicted in Table A.2.2-2.

Table A.2.2-1: Fields of a BA message for the DSMIPv6 Initial Binding Registration procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set as per HA ability to support the feature of updating the IKE SA based on Binding Update processing	IETF RFC 6275 [27], IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1"	IETF RFC 3963 [29]
Sequence Number	Set to the value received in the corresponding Binding Update.	IETF RFC 6275 [27]
Lifetime	Set to the granted number of time units of 4 seconds the binding shall remain valid.	IETF RFC 6275 [27]

Table A.2.2-2: Mobility Options in a BA message for the DSMIPv6 Initial Binding Registration procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Address Acknowledgment option	C	If IPv4 Home Address option is present in the corresponding BU, IPv4 Home Address is set to the IPv4 Home Address allocated for the UE. The supporting Status field is set accordingly. Pref-len field is set to "32".	IETF RFC 5555 [2]
NAT Detection Option	C	When present the option contains the F Flag which indicates to the UE that UDP encapsulation is required. Option contains an optionally Refresh Time for the UE to refresh the NAT binding.	IETF RFC 5555 [2]
Binding Refresh Advice	O	Contains a Refresh Interval in units of 4 seconds indicating the remaining time until the UE should send a new home registration to the HA.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE sent a Binding Identifier mobility option in the corresponding BU. The Status field is set accordingly. The BID, BID-PRI and "H" flag are set to the value indicated in the BID mobility option of the received Binding Update.	IETF RFC 5648 [31], IETF RFC 6089 [32]
Flow Identification mobility option	C	The option is present if the UE sent a Flow Identification mobility option in the corresponding BU. The Status field is set accordingly. The FID, FID-PRI, Action field and sub-option field are set to the value indicated in the FID mobility option of the received Binding Update.	IETF RFC 6089 [32], IETF RFC 6088 [33]

A.2.3 Binding Error

The fields of a BE message for the DSMIPv6 Initial Binding Registration procedure are depicted in Table A.2.3-1.

Table A.2.3-1: Fields of a BE message for the DSMIPv6 Initial Binding Registration procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Home Address	The home address that was contained in the Home Address destination option	IETF RFC 6275 [27]

A.3 Re-Registration

A.3.1 Binding Update

The fields of a BU message for the DSMIPv6 Re-Registration procedure are depicted in Table A.3.1-1.

The Mobility Options in a BU message for the DSMIPv6 Re-Registration procedure are depicted in Table A.3.1-2.

Table A.3.1-1: Fields of a BU message for the DSMIPv6 Re-Registration procedure

Fields	Fields Description	Reference
Sequence Number	Set to a monotonically increasing value.	IETF RFC 6275 [27]
Lifetime	Set to the requested number of time units the binding shall remain valid.	IETF RFC 6275 [27]
Home Registration (H)	Set to " 1" to indicate receiving node should act as this node's HA	IETF RFC 6275 [27]
Link-local Address Compatibility (L)	The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 6275 [27]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 6275 [27]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]
Overwrite Flag (O)	Set to "0" to maintain all binding cache entries at the HA previously registered.	IETF RFC 5648 [31]

Table A.3.1-2: Mobility Options in a BU message for the DSMIPv6 Re-Registration procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Home Address option	C	If the UE has previously registered IPv4 home address and wants to keep it, it is included in the option. The "P" flag is not set. The Prefix Length is set to the requested prefix length of 32. If the UE has previously registered IPv4 home address and wants to release it, it is not included in the BU. If the UE has no IPv4 Home address it may set the value "0.0.0.0" to request allocation for the UE. In this case the "P" flag is set to "0". The Prefix Length is set to the requested prefix length of 32.	IETF RFC 5555 [2]
IPv 4 Care-of Address	C	Set to the IPv4 Care-of address (same value as was set in the Initial BU) when in an IPv4 Access Network	IETF RFC 5555 [2]
Alternate Care-of Address	C	Used (in addition to the Source address of the IPv6 packet) to carry the IPv6 care-of address when in an IPv6 access network.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE included a Binding Identifier mobility option in the BU previously sent to the Home Agent. The BID and BID-PRI are set to an arbitrary value. For registration of a home link, the "H" flag is set to "1" and the value of the CoA field is the Home Address. For registration of a foreign link, the "H" flag is set to "0" and the value of the CoA field is the Care-of Address.	IETF RFC 5648 [31], IETF RFC 6089 [32]
Flow Summary mobility option	C	The option is present if the UE included a Flow Summary mobility option or at least one Flow Identification mobility option in the BU previously sent to the Home Agent. Contain one or more FIDs present in the binding update list to refresh the respective flow bindings.	IETF RFC 6089 [32]

A.3.2 Binding Acknowledgement

The fields of a BA message for the DSMIPv6 Re-Registration procedure are depicted in Table A.3.2-1.

The Mobility Options in a BA message for the DSMIPv6 Re-Registration procedure are depicted in Table A.3.2-2.

Table A.3.2-1: Fields of a BA message for the DSMIPv6 Re-Registration procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set as per HA ability to support the feature of updating the IKE SA based on Binding Update processing	IETF RFC 6275 [27], IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1"	IETF RFC 3963 [29]
Sequence Number	Set to the value received in the corresponding Binding Update or the last accepted sequence number in the case of Status 135 ("Sequence Number out of window ").	IETF RFC 6275 [27]
Lifetime	Set to the granted number of time units of 4 seconds the binding shall remain valid.	IETF RFC 6275 [27]

Table A.3.2-2: Mobility Options in a BA message for the DSMIPv6 Re-Registration procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Address Acknowledgment option	C	If IPv4 Home Address option is present in the corresponding BU, IPv4 Home Address is set to the IPv4 Home Address previously allocated for the UE or to a dynamically allocated value if the UE had no previous IPv4 home address and requested one at with the BU. The supporting Status field is set accordingly. Pref-len field is set to "32".	IETF RFC 5555 [2]
NAT Detection Option	C	When present the option contains the F Flag which indicates to the UE that UDP encapsulation is required. Option contains an optionally Refresh Time for the UE to refresh the NAT binding.	IETF RFC 5555 [2]
Binding Refresh Advice	O	Contains a Refresh Interval in units of 4 seconds indicating the remaining time until the UE should send a new home registration to the HA.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE sent a Binding Identifier mobility option in the corresponding BU. The Status field is set accordingly. The BID, BID-PRI and "H" flag are set to the value indicated in the BID mobility option of the received Binding Update.	IETF RFC 5648 [31], IETF RFC 6089 [32]
Flow Identification mobility option	O	The Status field is set accordingly. The FID, FID-PRI, Action field and sub-option field are set to the value indicated in the Flow Summary mobility option of the received Binding Update.	IETF RFC 6089 [32], IETF RFC 6088 [33]

A.4 Handover

A.4.1 Binding Update

The fields of a BU message for the DSMIPv6 Handover procedure are depicted in Table A.4.1-1.

The Mobility Options in a BU message for the DSMIPv6 Handover procedure are depicted in Table A.4.1-2.

Table A.4.1-1: Fields of a BU message for the DSMIPv6 Handover procedure

Fields	Fields Description	Reference
Sequence Number	Set to a monotonically increasing value.	IETF RFC 6275 [27]
Lifetime	Set to the requested number of time units the binding shall remain valid.	IETF RFC 6275 [27]
Home Registration (H)	Set to "1" to indicate receiving node should act as this node's HA	IETF RFC 6275 [27]
Link-local Address Compatibility (L)	The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility.	IETF RFC 6275 [27]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 6275 [27]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]
Overwrite Flag (O)	Set accordingly if the BID mobility option is present in the Binding Update. The purpose is to indicate replacing all binding cache entries at the HA with the entries listed in the Binding Update.	IETF RFC 5648 [31]

Table A.4.1-2: Mobility Options in a BU message for the DSMIPv6 Handover procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Home Address option	C	For dynamic allocation, set to the value "0.0.0.0 " to request allocation for the UE. In this case the "P " flag is set to "0". The Prefix Length is set to the requested prefix length of "32". If the UE already has an IPv4 Home Address and wants to keep on using it, the IPv4 home address is set to the previously allocated value. The "P" flag is not set. The Prefix Length is set to "32". If the UE already has an IPv4 Home Address and wants to release it, the option is not inserted in the BU,	IETF RFC 5555 [2]
IPv 4 Care-of Address	C	Set to the IPv4 Care-of address when in an IPv4 Access Network.	IETF RFC 5555 [2]
Alternate Care-of Address	C	Used (in addition to the Source address of the IPv6 packet) to carry the IPv6 care-of address when in an IPv6 access network.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE included a Binding Identifier mobility option in the BU previously sent to the Home Agent. The BID and BID-PRI are set to an arbitrary value. For registration of a home link, the "H" flag is set to "1" and the value of the CoA field is the Home Address. For registration of a foreign link, the "H" flag is set to "0" and the value of the CoA field is the Care-of Address.	IETF RFC 5648 [31], IETF RFC 6089 [32]
Flow Summary mobility option	C	The option is present if the UE included a Flow Summary mobility option or at least one Flow Identification mobility option in the BU previously sent to the Home Agent. Contain one or more FIDs present in the binding update list to refresh the respective flow bindings.	IETF RFC 6089 [32]

A.4.2 Binding Acknowledgement

The fields of a BA message for the DSMIPv6 Handover procedure are depicted in Table A.4.2-1.

The Mobility Options in a BA message for the DSMIPv6 Handover procedure are depicted in Table A.4.2-2.

Table A.4.2-1: Fields of a BA message for the DSMIPv6 Handover procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set as per HA ability to support the feature of updating the IKE SA based on Binding Update processing	IETF RFC 6275 [27], IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1"	IETF RFC 3963 [29]
Sequence Number	Set to the value received in the corresponding Binding Update or the last accepted sequence number in the case of Status 135 (" Sequence Number out of window").	IETF RFC 6275 [27]
Lifetime	Set to the granted number of time units of 4 seconds the binding shall remain valid.	IETF RFC 6275 [27]

Table A.4.2-2: Mobility Options in a BA message for the DSMIPv6 Handover procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Address Acknowledgment option	C	If IPv4 Home Address option is present in the corresponding BU, IPv4 Home Address is set to the IPv4 Home Address either newly allocated for the UE or previously assigned prior to the Handover. The supporting Status field is set accordingly. The Pref-len is set to "32".	IETF RFC 5555 [2]
NAT Detection Option	C	When present the option contains the F Flag which indicates to the UE that UDP encapsulation is required. Option contains an optionally Refresh Time for the UE to refresh the NAT binding.	IETF RFC 5555 [2]
Binding Refresh Advice	O	Contains a Refresh Interval in units of four seconds indicating the remaining time until the UE should send a new home registration to the HA.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE sent a Binding Identifier mobility option in the corresponding BU. The Status field is set accordingly. The BID, BID-PRI and "H" flag are set to the value indicated in the BID mobility option of the received Binding Update.	IETF RFC 5648 [31], IETF RFC 6089 [32]
Flow Identification mobility option	O	The Status field is set accordingly. The FID, FID-PRI, Action field and sub-option field are set to the value indicated in the Flow Summary mobility option of the received Binding Update.	IETF RFC 6089 [32], IETF RFC 6088 [33]

A.5 UE-initiated Detach

A.5.1 Binding Update

The fields of a BU message for the DSMIPv6 UE-Initiated Detach are depicted in Table A.5.1-1.

The Mobility Options in a BU message for the DSMIPv6 UE-Initiated Detach are depicted in Table A.5.1-2.

Table A.5.1-1: Fields of a BU message for the DSMIPv6 UE-Initiated Detach procedure

Fields	Fields Description	Reference
Sequence Number	Set to a monotonically increasing value.	IETF RFC 6275 [27]
Lifetime	Set to a value of "0" indicating that the Binding Cache entry for the UE is to be deleted.	IETF RFC 6275 [27]
Home Registration (H)	Set to "1" to indicate receiving node should act as this node's HA	IETF RFC 6275 [27]
Link-local Address Compatibility (L)	The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 6275 [27]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 6275 [27]
Force UDP encapsulation request (F) Flag	Set to "0 " to indicate no forced UDP encapsulation	IETF RFC 5555 [2]

Table A.5.1-2: Mobility Options in a BU message for the DSMIPv6 UE-Initiated Detach procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Home Address option	O	Set to the UE's previously registered value. The "P" flag is set to zero. The Prefix Length is set to 32.	IETF RFC 5555 [2]
IPv 4 Care-of Address	C	Set to the IPv4 Care-of address when in an IPv4 Access Network.	IETF RFC 5555 [2]
Alternate Care-of Address	C	Used (in addition to the Source address of the IPv6 packet) to carry the IPv6 care-of address when in an IPv6 access network.	IETF RFC 6275 [27]

A.5.2 Binding Acknowledgement

The fields of a BA message for the DSMIPv6 Initial Binding Registration procedure are depicted in Table A.5.2-1.

The Mobility Options in a BA message for the DSMIPv6 Initial Binding Registration procedure are depicted in Table A.5.2-2.

Table A.5.2-1: Fields of a BA message for the DSMIPv6 UE-Initiated Detach procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set as per HA ability to support the feature of updating the IKE SA based on Binding Update processing	IETF RFC 6275 [27], IETF RFC 5555 [2]
Sequence Number	Set to the value received in the corresponding Binding Update or the last accepted sequence number in the case of Status 135 ("Sequence Number out of window").	IETF RFC 6275 [27]
Lifetime	Set to "0".	IETF RFC 6275 [27]

Table A.5.2-2: Mobility Options in a BA message for the DSMIPv6 UE-Initiated Detach procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4Address Acknowledgment option	C	If present in the BU the IPv4 Home Address is set to the IPv4 Home Address that is now de-registered. The pref-len is set to "32" and the supporting Status field is set accordingly.	IETF RFC 5555 [2]

A.6 Network-initiated detach

A.6.1 Binding Revocation Indication Message

The fields of a Binding Revocation Indication message for the Network-Initiated Detach are depicted in table A.6.1-1.

Table A.6.1-1: Fields of a BRI message for the Network-Initiated Detach procedure

Fields	Fields Description	Reference
B.R. Type	Set to "1" to indicate B.R.I.	IETF RFC 5846 [19]
Sequence Number	Set to a monotonically increasing value and is used to match with the returned Binding Revocation Acknowledge	IETF RFC 5846 [19]
Revocation Trigger	Set to "1"	IETF RFC 5846 [19]
Proxy Binding (P)	Set to "0"	IETF RFC 5846 [19]
Global (G)	Set to "0"	IETF RFC 5846 [19]
IPv4 HoA Binding Only (V)	Set to "0"	IETF RFC 5846 [19]

A.6.2 Binding Revocation Acknowledgement

The fields of a BRA message for the Network-Initiated Detach procedure are depicted in Table A.6.2-1.

Table A.6.2-1: Fields of a BRA message for the Network-Initiated Detach procedure

Fields	Fields Description	Reference
B.R. Type	Set to "2" to indicate B.R.A.	IETF RFC 5846 [19]
Sequence Number	Set to the value received in the corresponding BRI.	IETF RFC 5846 [19]
Status	Indicates the result of the BRI.	IETF RFC 5846 [19]
Proxy Registration Flag (P)	Set to "0" to indicate that the Binding Revocation Acknowledgment is NOT for a proxy MIPv6 binding entry.	IETF RFC 5846 [19]
Global (G)	Set to "0"; the same value as for the BRI.	IETF RFC 5846 [19]
IPv4 HoA Binding Only (V)	Set to "0"	IETF RFC 5846 [19]

A.7 Void

A.8 Attach to an additional access network

A.8.1 Binding Update

The DSMIPv6 attach to additional access network procedure is described in subclause 5.5 and the fields of a BU message used for this procedure are depicted in table A.8.1-1.

The DSMIPv6 attach to additional access network procedure is described in subclause 5.5 and the Mobility Options in a BU message used for this procedure are depicted in table A.8.1-2.

Table A.8.1-1: Fields of a BU message for the DSMIPv6 attach to an additional access network procedure

Fields	Fields Description	Reference
Sequence Number	Set to a monotonically increasing value.	IETF RFC 6275 [27]
Lifetime	Set to the requested number of time in units of 4 seconds to indicate how long the binding will remain valid.	IETF RFC 6275 [27]
Home Registration (H)	Set to "1" to indicate receiving node can act as this node's HA	IETF RFC 6275 [27]
Link-local Address Compatibility (L)	The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 6275 [27]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 6275 [27]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]
Overwrite Flag (O)	If the UE attaches to a foreign link, set to "1" to indicate first registration	IETF RFC 5648 [31]
	If the UE attaches to the home link, set to "0" to maintain all binding cache entries at the HA previously registered.	

Table A.8.1-2: Mobility Options in a BU message for the DSMIPv6 attach to an additional access network procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Home Address option	O	Set to the value "0.0.0.0" to request allocation of an IPv4 Home Address for the UE.	IETF RFC 5555 [2]
		The "P" flag is set to '0'.	
		The Prefix Length is set to the requested prefix length of '32'.	
Binding Identifier mobility option	O	The BID and BID-PRI are set to an arbitrary value.	IETF RFC 5648 [31], IETF RFC 6089 [32]
		For registration of a home link, the "H" flag is set to "1" and the value of the CoA field is the Home Address.	
		For registration of a foreign link, the "H" flag is set to "0" and the value of the CoA field is the Care-of Address.	
Flow Identification mobility option	O	The FID and FID-PRI are set to an arbitrary value.	IETF RFC 6089 [32], IETF RFC 6088 [33]
		The sub-option field conveys the Traffic Selector sub-option.	
Flow Summary mobility option	O	Contain one or more FIDs present in the binding update list to refresh the respective flow bindings.	IETF RFC 6089 [32]

A.8.2 Binding Acknowledgement

The DSMIPv6 attach to additional access network procedure is described in subclause 5.5 and the fields of a BA message used for this procedure are depicted in table A.8.2-1.

The DSMIPv6 attach to additional access network procedure is described in subclause 5.5 and the Mobility Options in a BA message used for this procedure are depicted in table A.8.2-2.

Table A.8.2-1: Fields of a BA message for the DSMIPv6 attach to an additional access network procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set as per HA ability to support the feature of updating the IKE SA based on Binding Update processing	IETF RFC 6275 [27], IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1"	IETF RFC 3963 [29]
Sequence Number	Set to the value received in the corresponding Binding Update.	IETF RFC 6275 [27]
Lifetime	Set to the granted number of time units of 4 seconds to indicate how long the binding will remain valid.	IETF RFC 6275 [27]

Table A.8.2-2: Mobility Options in a BA message for the DSMIPv6 attach to an additional access network procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Address Acknowledgment option	C	If IPv4 Home Address option is present in the corresponding BU, IPv4 Home Address is set to the IPv4 Home Address allocated for the UE.	IETF RFC 5555 [2]
		The supporting Status field is set accordingly.	
		Pref-len field is set to "32".	
NAT Detection Option	C	When present the option contains the F Flag which indicates to the UE that UDP encapsulation is required. Option contains an optionally Refresh Time for the UE to refresh the NAT binding.	IETF RFC 5555 [2]
Binding Refresh Advice	O	Contains a Refresh Interval in units of 4 seconds indicating the remaining time until the UE could send a new home registration to the HA.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE sent a Binding Identifier mobility option in the corresponding BU. The Status field is set accordingly.	IETF RFC 5648 [31], IETF RFC 6089 [32]
		The BID and BID-PRI are set to the value indicated in the BID mobility option of the received Binding Update.	
Flow Identification mobility option	C	The option is present if the UE sent a Flow Identification mobility option in the corresponding BU. The Status field is set accordingly.	IETF RFC 6089 [32], IETF RFC 6088 [33]
		The FID, FID-PRI and sub-option field are set to the value indicated in the FID mobility option of the received Binding Update.	

A.9 Inter-access flow mobility

A.9.1 Binding Update

The DSMIPv6 inter-access flow mobility procedure is described in subclause 5.5 and the fields of a BU message used for this procedure are depicted in table A.9.1-1.

The DSMIPv6 inter-access flow mobility procedure is described in subclause 5.5 and the Mobility Options in a BU message used for this procedure are depicted in table A.9.1-2.

Table A.9.1-1: Fields of a BU message for the DSMIPv6 inter-access flow mobility procedure

Fields	Fields Description	Reference
Sequence Number	Set to a monotonically increasing value.	IETF RFC 6275 [27]
Lifetime	Set to the requested number of time in units of 4 seconds to indicate how long the binding will remain valid.	IETF RFC 6275 [27]
Home Registration (H)	Set to "1" to indicate receiving node can act as this node's HA	IETF RFC 6275 [27]
Link-local Address Compatibility (L)	The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 6275 [27]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 6275 [27]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]
Overwrite Flag (O)	Set to "0" to indicate not replacing all binding cache entries at the HA with the entries listed in the Binding Update	IETF RFC 5648 [31]

Table A.9.1-2: Mobility Options in a BU message for the DSMIPv6 inter-access flow mobility procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Home Address option	O	For dynamic allocation, set to the value "0.0.0.0" to request allocation for the UE.	IETF RFC 5555 [2]
		If the UE already has an IPv4 Home Address and wants to keep on using it, the IPv4 home address is set to the previously allocated value.	
		If the UE already has an IPv4 Home Address and wants to release it, the option is not inserted in the BU.	
		If the UE request allocation of IPv4 Home Address, the "P" flag is set to '0'.	
		If the UE already has an IPv4 Home Address and wants to keep on using it, the "P" flag is not set.	
		The Prefix Length is set to the requested prefix length of '32'.	
Binding Identifier mobility option	O	The BID is set to the value identifying the routing address used as Source IP Address of the Binding Update.	IETF RFC 5648 [31], IETF RFC 6089 [32]
		The BID-PRI is set to the value assigned to the BID.	
		If the Binding Update message is sent on a home link, the "H" flag is set to "1".	
		If the Binding Update message is sent on a foreign link, the "H" flag is set to "0".	
		If the routing address used as IP Source Address of the Binding Update message is an IPv4 address, a NAT was detected and the UE is not exchanging data traffic, the Care-of Address field is set to the routing address.	
Flow Identification mobility option	O	For creating routing rules, the FID and FID-PRI are set to an arbitrary value.	IETF RFC 6089 [32], IETF RFC 6088 [33]
		For modifying routing rules, the FID and FID-PRI are set to the value identifying the routing filter the UE wants to modify.	
		The sub-option field conveys the Traffic Selector sub-option.	
Flow Summary mobility option	O	Contain one or more FIDs present in the binding update list to refresh the respective flow bindings.	IETF RFC 6089 [32]

A.9.2 Binding Acknowledgement

The DSMIPv6 inter-access flow mobility procedure is described in subclause 5.5 and the fields of a BA message used for this procedure are depicted in table A.9.2-1.

The DSMIPv6 inter-access flow mobility procedure is described in subclause 5.5 and the Mobility Options in a BA message used for this procedure are depicted in table A.9.2-2.

Table A.9.2-1: Fields of a BA message for the DSMIPv6 inter-access flow mobility procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set as per HA ability to support the feature of updating the IKE SA based on Binding Update processing	IETF RFC 6275 [27], IETF RFC 5555 [2]
Mobile Router Flag (R)	Set to "1"	IETF RFC 3963 [29]
Sequence Number	Set to the value received in the corresponding Binding Update.	IETF RFC 6275 [27]
Lifetime	Set to the granted number of time units of 4 seconds to indicate how long the binding will remain valid.	IETF RFC 6275 [27]

Table A.9.2-2: Mobility Options in a BA message for the DSMIPv6 inter-access flow mobility procedure

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Address Acknowledgment option	C	If IPv4 Home Address option is present in the corresponding BU, IPv4 Home Address is set to the IPv4 Home Address either newly allocated for the UE or previously assigned prior to the Handover.	IETF RFC 5555 [2]
		The supporting Status field is set accordingly.	
		Pref-len field is set to "32".	
NAT Detection Option	C	When present the option contains the F Flag which indicates to the UE that UDP encapsulation is required. Option contains an optionally Refresh Time for the UE to refresh the NAT binding.	IETF RFC 5555 [2]
Binding Refresh Advice	O	Contains a Refresh Interval in units of 4 seconds indicating the remaining time until the UE could send a new home registration to the HA.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE sent a Binding Identifier mobility option in the corresponding BU. The Status field is set accordingly.	IETF RFC 5648 [31], IETF RFC 6089 [32]
		The BID and BID-PRI are set to the value indicated in the BID mobility option of the received Binding Update.	
Flow Identification mobility option	C	The option is present if the UE sent a Flow Identification mobility option in the corresponding BU. The Status field is set accordingly.	IETF RFC 5648 [31], IETF RFC 6089 [32]
		The FID, FID-PRI and sub-option field are set to the value indicated in the FID mobility option of the received Binding Update.	

A.10 UE-initiated removal of an access network from a PDN connection

A.10.1 Binding Update

The UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.8 and the fields of a BU message used for this procedure are depicted in table A.10.1-1.

The UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.8 and the Mobility Options in a BU message used for this procedure are depicted in table A.10.1-2.

Table A.10.1-1: Fields of a BU message for the UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Fields	Fields Description	Reference
Sequence Number	Set to a monotonically increasing value.	IETF RFC 6275 [27]
Lifetime	If the Binding Update is to de-register binding of the access network, the Lifetime is set to a value of "0".	IETF RFC 6275 [27]
	If the Binding Update is to register the maintained access network, the Lifetime is set to the requested number of time in units of 4 seconds to indicate how long the binding will remain valid.	
Home Registration (H)	Set to "1" to indicate receiving node can act as this node's HA	IETF RFC 6275 [27]
Link-local Address Compatibility (L)	The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 6275 [27]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 6275 [27]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	IETF RFC 5555 [2]
Mobile Router Flag (R)	If the Binding Update is to register the maintained access network, the Mobile Router Flag (R) is set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]
Overwrite Flag (O)	Set to any value if the lifetime field of the Binding Update is set to 0	IETF RFC 5648 [31]
	Set to "1" if the lifetime field of the Binding Update is set to any value different from 0	

Table A.10.1-2: Mobility Options in a BU message for the UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Mobility Option	Cat.	Mobility Option Description	Reference
Binding Identifier mobility option	O	For a Binding Update with Lifetime set to "0", the BID and BID-PRI are set to the corresponding entry that the UE wants to remove.	IETF RFC 5648 [31], IETF RFC 6089 [32]
		For a Binding Update with Lifetime not set to "0", the BID and BID-PRI are set to the corresponding entry that the UE wants to maintain.	

A.10.2 Binding Acknowledgement

The UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.8 and the fields of a BA message used for this procedure are depicted in table A.10.2-1.

The UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.8 and the Mobility Options in a BA message used for this procedure are depicted in table A.10.2-2.

Table A.10.2-1: Fields of a BA message for the UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Fields	Fields Description	Reference
Status	Set to indicate the result.	IETF RFC 6275 [27]
Key Management Mobility Capability (K)	Set as per HA ability to support the feature of updating the IKE SA based on Binding Update processing	IETF RFC 6275 [27], IETF RFC 5555 [2]
Mobile Router Flag (R)	If the Binding Update is to register the maintained access network, the Mobile Router Flag (R) is set to "1"	IETF RFC 3963 [29]
Sequence Number	Set to the value received in the corresponding Binding Update or the last accepted sequence number in the case of Status 135 ("Sequence Number out of window").	IETF RFC 6275 [27]
Lifetime	If the Binding Update is to de-register binding of the access network, the Lifetime is set to a value of "0".	IETF RFC 6275 [27]
	If the Binding Update is to register the maintained access network, the Lifetime is set to the granted number of time in units of 4 seconds to indicate how long the binding will remain valid.	

Table A.10.2-2: Mobility Options in a BA message for the UE-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Mobility Option	Cat.	Mobility Option Description	Reference
NAT Detection Option	C	When present the option contains the F Flag which indicates to the UE that UDP encapsulation is required. Option contains an optionally Refresh Time for the UE to refresh the NAT binding.	IETF RFC 5555 [2]
Binding Refresh Advice	O	Contains a Refresh Interval in units of 4 seconds indicating the remaining time until the UE could send a new home registration to the HA.	IETF RFC 6275 [27]
Binding Identifier mobility option	C	The option is present if the UE sent a Binding Identifier mobility option in the corresponding BU. The Status field is set accordingly.	IETF RFC 5648 [31], IETF RFC 6089 [32]
		For a Binding Update with Lifetime not set to "0", the BID and BID-PRI are set to the value indicated in the BID mobility option of the received Binding Update.	

A.11 Network-initiated removal of an access network from a PDN connection

A.11.1 Binding Revocation Indication Message

The network-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.9 and the fields of a BRI message used for this procedure are depicted in table A.11.1-1.

The network-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.9 and the Mobility Options in a BRI message used for this procedure are depicted in table A.11.1-2.

Table A.11.1-1: Fields of a BRI message for the network-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Fields	Fields Description	Reference
B.R. Type	Set to "1" to indicate BRI.	IETF RFC 5846 [19]
Sequence Number	Set to a monotonically increasing value and is used to match with the returned Binding Revocation Acknowledge	IETF RFC 5846 [19]
Revocation Trigger	Set to "1"	IETF RFC 5846 [19]
Proxy Binding (P)	Set to "0"	IETF RFC 5846 [19]
Global (G)	Set to "0"	IETF RFC 5846 [19]
IPv4 HoA Binding Only (V)	Set to "0"	IETF RFC 5846 [19]

Table A.11.1-2: Mobility Options in a BRI message for the network-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Mobility Option	Cat.	Mobility Option Description	Reference
Binding Identifier mobility option	O	The BID and BID-PRI are set to the corresponding entry that the UE wants to remove.	IETF RFC 5648 [31], IETF RFC 6089 [32]

A.11.2 Binding Revocation Acknowledgement

The network-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.9 and the fields of a BRA message used for this procedure are depicted in table A.11.2-1.

The network-initiated DSMIPv6 removal of an access network from a PDN connection procedure is described in subclause 5.9 and the Mobility Options in a BRA message used for this procedure are depicted in table A.11.2-2.

Table A.11.2-1: Fields of a BRA message for the network-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Fields	Fields Description	Reference
B.R. Type	Set to "2" to indicate BRA.	IETF RFC 5846 [19]
Sequence Number	Set to the value received in the corresponding BRI.	IETF RFC 5846 [19]
Status	Indicates the result of the BRI.	IETF RFC 5846 [19]
Proxy Registration Flag (P)	Set to "0" to indicate that the Binding Revocation Acknowledgment is NOT for a proxy MIPv6 binding entry.	IETF RFC 5846 [19]
Global (G)	Set to "0"; the same value as for the BRI.	IETF RFC 5846 [19]
IPv4 HoA Binding Only (V)	Set to "0"	IETF RFC 5846 [19]

Table A.11.2-2: Mobility Options in a BRA message for the network-initiated DSMIPv6 removal of an access network from a PDN connection procedure

Mobility Option	Cat.	Mobility Option Description	Reference
Binding Identifier mobility option	C	This option may be included to indicate the specific BID that failded the revocation procedure. The BID and BID-PRI are set to the value indicated in the BID mobility option of the received Binding Revocation Indication.	IETF RFC 5648 [31], IETF RFC 6089 [32]

Annex B (normative): Extensions specific to the present document

B.1 PDN Identifier notify payload

The format of the PDN Identifier notify payload is shown in figure B-1-1.

The PDN Identifier notify payload type is 40960. The length of the PDN Identifier notify payload is 21 octets. The IPv6 Home Network Prefix contains the IPv6 prefix of a PDN connection. The Prefix Length field indicates the length of the prefix contained in IPv6 Home Network Prefix field.

The other fields are defined by IETF RFC 5996 [14].

Bits 7 6 5 4 3 2 1 0	Octets
Protocol ID	1
SPI Size	2
Notify Message Type	3-4
IPv6 Home Network Prefix	5 – 20
Prefix Length	21

Figure B.1-1: PDN Identifier notify payload format

NOTE: As the notify payload notifies information relating an IKE_SA, SPI Size field is set to 0 and there is no Security Parameter Index field.

B.2 IFOM Capability notify payload

The format of the IFOM Capability notify payload is shown in figure B.2-1.

The IFOM Capability notify payload type is 16428. The length of the IFOM Capability notify payload is 4 octets. The IFOM Capability notify payload is used to indicate the IFOM capability.

The other fields are defined by IETF RFC 5996 [14].

Bits 7 6 5 4 3 2 1 0	Octets
Protocol ID	1
SPI Size	2
Notify Message Type	3-4

Figure B.2-1: IFOM Capability notify payload format

NOTE: As the notify payload notifies information relating to an IKE_SA, SPI Size field is set to 0 and there is no Security Parameter Index field.

Annex C (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
01-2008					Version 0.0.0 Editor's internal draft		0.0.0
02-2008	CT1 #51				Includes the following contributions agreed in CT1 #51: C1-080436, C1-080437	0.0.0	0.1.0
02-2008	CT1 #51bis				Includes the following contributions agreed in CT1 #51bis: C1-080770, C1-080776, C1-080791.	0.1.0	0.2.0
02-2008	Email-review				Editorial/style corrections in the clean version	0.2.0	0.2.1
04-2008	CT1 #52				Includes the following contributions agreed in CT1 #52: C1-080954, C1-080959, C1-080960, C1-081213, C1-081232, C1-081398, C1-081399, C1-081400, C1-081401, C1-081402, C1-081419	0.2.1	0.3.0
04-2008	Email-review				Editorial/style corrections in the clean version	0.3.0	0.3.1
05-2008	CT1 #53				Includes the following contributions agreed in CT1 #53: C1-081590, C1-081594, C1-081693, C1-082079, C1-082080, C1-082082, C1-082083, C1-082084, C1-082063	0.3.1	0.4.0
05-2008	Email-review				Editorial clean-up	0.4.0	0.4.1
05-2008					Version 1.0.0 to be presented to CT-40 created by MCC	0.4.1	1.0.0
07-2008	CT1 #54				Includes the following contributions agreed in CT1 #54: C1-082122, C1-082364, C1-082368, C1-082693, C1-082694, C1-082698, C1-082699, C1-082700 and C1-082808	1.0.0	1.1.0
08-2008	CT1 #55				Includes the following contributions agreed in CT1 #55: C1-082827, C1-082828, C1-082989, C1-083003, C1-083004, C1-083486, C1-083488, C1-083524 and C1-083601	1.1.0	1.2.0
10-2008	CT1 #55bis				Includes the following contributions agreed in CT1 #55bis: C1-083858, C1-083861, C1-084384, C1-084454, C1-084455, C1-084457, C1-084458, C1-084460, C1-084461, C1-084553, C1-084563, C1-084564, C1-084565	1.2.0	1.3.0
11-2008	CT1 #56				Includes the following contributions agreed in CT1 #56: C1-084692, C1-084693, C1-085379, C1-085517	1.3.0	1.4.0
11-2008	E-mail review				Editorial clean-up	1.4.0	1.4.1
11-2008	E-mail review				Editorial clean-up	1.4.1	1.4.2
11-2008	E-mail review				Editorial clean-up	1.4.2	1.4.3
11-2008					Version 2.0.0 created for presentation to CT#42 for approval	1.4.3	2.0.0
12-2008					Version 8.0.0 created after approval in CT#42	2.0.0	8.0.0
03-2009	CT-43	CP-090126	0001	1	Binding Update Optimization	8.0.0	8.1.0
03-2009	CT-43	CP-090126	0003		BRI error correction	8.0.0	8.1.0
03-2009	CT-43	CP-090129	0005	1	Missing HA Initiated Multiple PDN Detach	8.0.0	8.1.0
03-2009	CT-43	CP-090129	0007		IPv4 HoA release	8.0.0	8.1.0
03-2009	CT-43	CP-090125	0008	1	Align with latest version of internet draft	8.0.0	8.1.0
03-2009	CT-43				Editorial cleanup by MCC	8.0.0	8.1.0
06-2009	CT-44	CP-090413	0004	3	Discovery of the Home Agent address	8.1.0	8.2.0
06-2009	CT-44	CP-090413	0011	1	HA discovery via DHCPv6	8.1.0	8.2.0
06-2009	CT-44	CP-090413	0012		Nemo Binding Acknowledgement Status value clarification	8.1.0	8.2.0
06-2009	CT-44	CP-090413	0013		Alternate Care-of Address correction	8.1.0	8.2.0
06-2009	CT-44	CP-090413	0014		TLV Header Format flag references	8.1.0	8.2.0
06-2009	CT-44	CP-090413	0016		Update to the Binding Revocation Indication Message	8.1.0	8.2.0
06-2009	CT-44	CP-090413	0017		Clarification of routing header usage	8.1.0	8.2.0
06-2009	CT-44	CP-090324	0018	3	HA reallocation procedure and Home Address request	8.1.0	8.2.0
09-2009	CT-45	CP-090655	0019		DNS lookup at HA discovery based on DHCPv6	8.2.0	8.3.0
09-2009	CT-45	CP-090655	0021	1	Clarification of IPv4 Home Address request	8.2.0	8.3.0
09-2009	CT-45	CP-090655	0023	1	Update of TS after DS-MIPv6 RFC availability	8.2.0	8.3.0
09-2009	CT-45	CP-090655	0024	1	Remove the static HNP configured in LTE capable UE	8.2.0	8.3.0
09-2009	CT-45	CP-090655	0025		IPv4 address acknowledgement option type	8.2.0	8.3.0
09-2009	CT-45	CP-090655	0027		Deletion of SA to the initial HA during HA reallocation procedure	8.2.0	8.3.0
12-2009	CT-46	CP-090901	0028		RFC5555 missing reference	8.3.0	8.4.0
12-2009	CT-46	CP-090901	0030		A bit in BRI message	8.3.0	8.4.0
12-2009	CT-46	CP-090901	0031	1	UE procedures at BRI reception	8.3.0	8.4.0
12-2009	CT-46	CP-090901	0029	2	Clarification of Binding Error message	8.4.0	9.0.0
03-2010	CT-47	CP-100107	0035	1	Multiple PDN connections	9.0.0	9.1.0
03-2010	CT-47	CP-100107	0037	1	PDN connections	9.0.0	9.1.0

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
03-2010	CT-47	CP-100107	0039		Reference to redirect RFC	9.0.0	9.1.0
06-2010	CT-48	CP-100339	0042		Reference Updates	9.1.0	9.2.0
06-2010	CT-48	CP-100339	0044	2	Usage of PDN prefix information with multiple PDNs to the same APN	9.1.0	9.2.0
09-2010	CT-49	CP-100485	0048	3	Usage of PDN Identifier notify payload	9.2.0	9.3.0
09-2010	CT-49	CP-100513	0049	4	IFOM Reference and Definitions	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0050	6	UE behaviour with multiple PDN connection for IFOM	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0053	3	Attach to additional access - general	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0054	5	Dual Stack Mobile IPv6 inter-access flow mobility	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0055	2	Attach to additional access acting as home link – UE behaviour	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0056	2	Attach to additional access acting as visted link – UE behaviour	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0057	2	Attach to additional access acting as home link – HA behaviour	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0058	1	Attach to additional access acting as visited link - HA behavior	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0059	2	Access removal - general	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0060		Home link access removal - UE behavior	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0061	2	Visited link access removal - UE behavior	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0062		Removal of an access acting as home link – HA procedures	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0063	2	Visited link access removal - HA behavior	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0064	1	IFOM initial attachment	9.3.0	10.0.0
09-2010	CT-49	CP-100513	0065	1	Message format for IP flow mobility	9.3.0	10.0.0
09-2010	CT-49	CP-100520	0066	2	Support of IPv6 Prefix Delegation on S2c	9.3.0	10.0.0
09-2010	CT-49	CP-100518	0067	1	Usage of IP version for Care-of Address selection	9.3.0	10.0.0
12-2010	CT-50	CP-100754	0069	2	IFOM Attach to additional access procedure	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0070	2	IFOM flow mobility procedure	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0071	1	IFOM Remove a link - general	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0075	3	Additional message format for IP flow mobility	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0077	1	Clarification on Dual Stack Mobile IPv6 re-registration	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0078	3	Network-initiated detach in multiple Care-of addresses use case	10.0.0	10.1.0
12-2010	CT-50	CP-100763	0079	1	Delegated Prefix in HA	10.0.0	10.1.0
12-2010	CT-50	CP-100763	0080	1	UE behaviour of DHCPv6 prefix delegation	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0082	2	Clarification on IFOM capability	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0083	1	Corrections and clarifications on IFOM procedures	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0084	5	Access removal from PDN	10.0.0	10.1.0
12-2010	CT-50	CP-100763	0087		Assigned HNP in BA message	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0088	1	IFOM Capability Discovery	10.0.0	10.1.0
12-2010	CT-50	CP-100754	0089	2	Error conditions for IFOM	10.0.0	10.1.0
03-2011	CT-51	CP-110185	0093	1	IFOM capability discovery through ISRP	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0094	3	IFOM condition for binding acknowledge	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0095		IFOM error condition	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0096	1	IFOM correction on attach to additional access procedure	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0098	1	Network-initiated removal of an access	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0100	3	Revision to Network-initiated Removal of Foreign Link from a PDN Connection	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0101		Modification of UE-initiated Removal of an Access Network from a PDN Connection	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0102	1	Correction to pointer to TS 24.302 for IFOM procedure	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0103		IFOM extensions for handover	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0104		IFOM capability discovery – PCO usage correction	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0105		Correction on 'O' flag	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0106	1	Protocol type definition for IFOM capability IKE-v2 payload	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0107	2	Routing of packets for IFOM	10.1.0	10.2.0
03-2011	CT-51	CP-110185	0108		Removal of editor's note	10.1.0	10.2.0
03-2011	CT-51	CP-110197	0109	2	S2c data integrity protection	10.1.0	10.2.0
06-2011	CT-52	CP-110478	0110	1	References to RFC	10.2.0	10.3.0
09-2011	CT-53	CP-110682	0111	1	S2c data integrity protection over trusted non-3GPP access	10.3.0	10.4.0
09-2011	CT-53	CP-110660	0115	2	Correction of Home Agent discovery via DHCPv6	10.3.0	10.4.0
09-2011	CT-53	CP-110682	0117	1	Correction to S2c data integrity protection – UE procedures	10.3.0	10.4.0
09-2011	CT-53	CP-110690	0112	1	Correction of security related reference	10.4.0	11.0.0
09-2011	CT-53	CP-110690	0116	1	Rejection of IKEv2 SA request	10.4.0	11.0.0
09-2011	CT-53	CP-110690	0120	1	Correction to references	10.4.0	11.0.0
12-2011	CT-54	CP-110874	0121	2	Correction to S2c data integrity protection – HA procedures	11.0.0	11.1.0
06-2012	CT-56	CP-120300	0123		IETF reference update	11.1.0	11.2.0

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
06-2012	CT-56	CP-120293	0125	4	Correction to HA discovery based on DHCPv6	11.1.0	11.2.0
06-2012	CT-56	CP-120309	0126	1	Generalize handover procedure to include also Care-of Address change independent of handover	11.1.0	11.2.0
06-2012	CT-56	CP-120309	0127	1	Corrections with references	11.1.0	11.2.0
06-2013	CT-60	CP-130237	0129	1	Specification of IFOM Capability notify payload type	11.2.0	11.3.0
09-2014	CT-65				Upgrade to Rel-12	11.3.0	12.0.0
12-2015	CT-70				Upgrade to Rel-13	12.0.0	13.0.0

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-03	CT-75					Upgrade to Rel-14	14.0.0
2018-06	SA-80	-	-	-	-	Update to Rel-15 version (MCC)	15.0.0
2020-07	SA-88e	-	-	-	-	Update to Rel-16 version (MCC)	**16.0.0**

History

Document history		
V16.0.0	September 2020	Publication