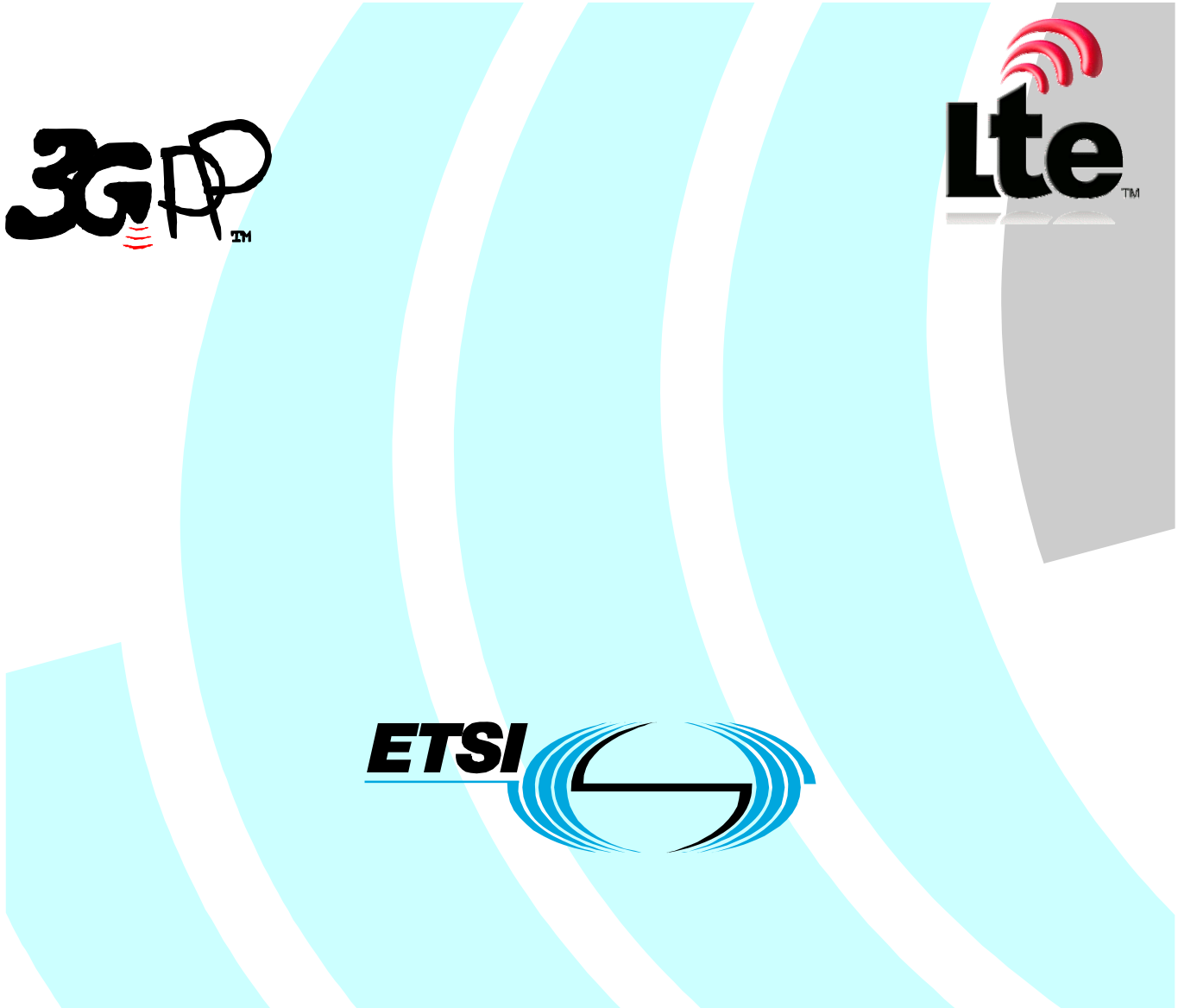
ETSI TS 124 303 V8.2.0 (2009-06)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Mobility management based on Dual-Stack Mobile IPv6;
Stage 3
(3GPP TS 24.303 version 8.2.0 Release 8)



Reference
RTS/TSGC-0124303v820

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

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

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

Foreword

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

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

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

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

The present document specifies the 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] draft-ietf-mext-nemo-v4traversal-09.txt (February 2009): "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)".

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

[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] IETF RFC 2782 (February 2000): "A DNS RR for specifying the location of services (DNS SRV)".

[6] IETF RFC 3775 (June 2004): "Mobility Support in IPv6".

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

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

[9] IETF RFC 3633 (December 2003): "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".

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

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

[12] draft-ietf-mip6-hiopt-15.txt (April 2008): "DHCP Option for Home Information Discovery in MIPv6".

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

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

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

[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] draft-ietf-mext-binding-revocation-05 (March 2009): "Binding Revocation for IPv6 Mobility".

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

[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] 3GPP TS 29.275 "PMIP based Mobility and Tunnelling protocols".

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

[27] draft-ietf-mext-rfc3775bis-02 (October 2008): "Mobility Support in IPv6".

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

[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] draft-ietf-ipsecme-ikev2-redirect-06 (March 2009): "Redirect Mechanism for IKEv2".

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

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 3775 [6]: Home Address, Care-of Address, binding cache, binding cache entry.

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 draft-ietf-mext-nemo-v4traversal [2] and IETF RFC 4877 [4]. Based on 3GPP TS 23.402 [15] 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.

DSMIPv6	Dual-Stack MIPv6
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
GW	Gateway
HA	Home Agent
MIPv6	Mobile IP version 6
UE	User Equipment

4 General

4.1 Mobility management based on Dual-Stack Mobile IPv6

DSMIPv6 is specified in IETF RFC 3775 [6] and draft-ietf-mext-nemo-v4traversal [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, meaning that if multiple PDNs are accessed by the UE, multiple instances of the procedures are needed. The multiple PDN 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.

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 connect to multiple PDNs using multiple DSMIPv6 sessions, one per each PDN the UE is connected to.

NOTE: When UE is associated to multiple PDNs, 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 8) 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 the UE is connected to. This implies that:

- For the initial attach to any PDN, 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 (subclause 5.1.2.2), and the initial binding registration (subclause 5.1.2.4).

- For a handover, the UE shall send a Binding Update for each PDN, following the procedure 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 separately following the procedure described in subclause 5.4.2 for UE initiated detach and following the procedure described in subclause 5.4.3 for HA initiated detach

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 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 draft-ietf-mip6-hiopt [12].

In order to discover the address of the HA the UE shall send an Information-Request message including the Home Network Identifier Option.

In order to connect to a HA for a specific target PDN, the UE shall set the id-type to 1 and include the desired HA-APN in the Home Network Identifier field.

The HA information is provided to the UE within a Home Network Information Option as described in draft-ietf-mip6-hiopt [12]. This option shall include either the available HA addresses (both the IPv6 address and the IPv4 address of the HA, if available) or the HA FQDN. 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.

5.1.2.2 Security association establishment and IPv6 Home Network Prefix assignment

The UE shall support the IKEv2 protocol (see IETF RFC 4306 [14]) for negotiating the IPsec security association to secure DSMIPv6 signalling and shall support EAP over IKEv2 as described in IETF RFC 4306 [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 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 draft-ietf-ipsecme-ikev2-redirect [30].

The UE shall initiate the security association establishment procedure by sending the IKE_SA_INIT request message defined in IETF RFC 4306 [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 draft-ietf-ipsecme-ikev2-redirect [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 [26].

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 reponse 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 may implicitly terminate and remove the states of the IKEv2 security association with the initial HA.

During the IKEv2 exchange, the UE shall request the allocation of an IPv6 home prefix through the Configuration Payload in the IKE_AUTH. 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 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 4306 [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 to request the IPv4 address of the DNS server.

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].

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 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 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. The Home Network prefix may be also statically configured. 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 statically configured or dynamically received in a PCO Information Element.

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 3775 [6] and draft-ietf-mext-nemo-v4traversal [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. The UE shall not register both IPv4 and IPv6 Care-of Address to its HA.

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.

If IPv4 Care-of Address is used for initial binding registration, the UE shall send the Binding Update as follows (see draft-ietf-mext-nemo-v4traversal [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 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 draft-ietf-mext-nemo-v4traversal [2].

When the UE receives the Binding Acknowledgement from the HA, it shall validate it based on the rules described in IETF RFC 3775 [2] and draft-ietf-mext-nemo-v4traversal [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 3775 [2]. If the Binding Acknowledgement contains a value from 129 to 133 as specified in IETF RFC 3775 [2] 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.

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 3775 [6]; IPv4 traffic shall be encapsulated in IPv6 packets as described in draft-ietf-mext-nemo-v4traversal [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 draft-ietf-mext-nemo-v4traversal [2]. Otherwise the UE shall send IPv6 and IPv4 packets encapsulated in IPv4 as specified in draft-ietf-mext-nemo-v4traversal [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 3775 [6] in order to retrieve additional parameters, e.g. Vendor-specific options.

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 4306 [14]) for negotiating the IPsec security association to secure DSMIPv6 signalling and shall support EAP over IKEv2 as described in IETF RFC 4306 [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 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 4306 [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, the HA shall include the same attribute in the CFG_REPLY including zero or more DNS server addresses as specified in IETF RFC 4306 [14]

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 draft-ietf-ipsecme-ikev2-redirect [30]. The HA shall not assign an IPv6 prefix to the UE in the IKE_AUTH exchange. The HA may implicitly terminate and remove the states of the IKEv2 security association with 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 3775 [6] and in draft-ietf-mext-nemo-v4traversal [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 3775 [6] and IETF RFC 3963 [29]. The HA may include the Binding Refresh Advice mobility option following rules defined in IETF RFC 3775 [6] 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 draft-ietf-mext-nemo-v4traversal [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 draft-ietf-mext-nemo-v4traversal [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 draft-ietf-mext-nemo-v4traversal [2].

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 draft-ietf-mext-nemo-v4traversal [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 draft-ietf-mext-nemo-v4traversal [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 3775 [6] and in draft-ietf-mext-nemo-v4traversal [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 3775 [6] and in draft-ietf-mext-nemo-v4traversal [2].

5.1.3.3 Binding Error message

When the HA receives a Binding Update and detects an inappropriate attempt to use the Home Address destination option without an existing binding, or when an unrecognized Mobility Header is received the HA shall send a Binding Error message with appropriate status (value 1 "Unknown binding for Home Address destination option" or value 2 "Unrecognized MH Type value") as specified in IETF draft-ietf-mext-rfc3775bis-02 [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 draft-ietf-mext-nemo-v4traversal [2].

If NAT was detected, the HA shall send the Binding Error encapsulated in UDP and IPv4 based on vanilla UDP encapsulation specified in draft-ietf-mext-nemo-v4traversal [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 which implies a change of the local IP address (e.g. a movement from a 3GPP to a non-3GPP access). 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. 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 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 draft-ietf-mext-nemo-v4traversal [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 3775 [6].

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 [6]. The UE build the Binding Update message as specified in IETF RFC 3775 [6].

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 draft-ietf-mext-nemo-v4traversal [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.

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 3775 [6]. 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.

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 3775 [6] and in draft-ietf-mext-nemo-v4traversal [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 draft-ietf-mip6-nemo-v4traversal [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 draft-ietf-mext-nemo-v4traversal [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 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 I-D draft-ietf-mext-nemo-v4traversal [2] and IETF RFC 3775 [6], 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 draft-ietf-mext-nemo-v4traversal [2].

5.3.2 UE procedures

As specified in IETF RFC 3775 [6], 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 RC 3775 [6], draft-ietf-mext-nemo-v4traversal [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 draft-ietf-mext-nemo-v4traversal [2] sending a re-registration Binding Update containing no IPv4 Home Address option.

5.3.3 HA procedures

When the HA receives a periodic Binding Update message from the UE, it shall validate it as described in IETF RFC 3775 [6], draft-ietf-mext-nemo-v4traversal [2] and in subclause 5.1.3.2.

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. 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 draft-ietf-mext-binding-revocation [19] from the HA, the UE first shall perform the required validity checks on the BRI according to draft-ietf-mext-binding-revocation [19].

If the A (Acknowledge) flag is set in the BRI message, the UE shall send a Binding Revocation Acknowledgement (BRA) as specified in draft-ietf-mext-binding-revocation [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 4306 [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 3775 [6].

The UE shall use the procedures defined in the IKEv2 protocol in IETF RFC 4306 [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 (3GPP TS 29.273 [20]) the HA shall send a Binding Revocation Indication (BRI) message according to draft-ietf-mext-binding-revocation [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 A bit to 1 (Request a Binding Revocation Acknowledgement to be returned), 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 draft-ietf-mext-binding-revocation [19] and shall not include any mobility option. 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 draft-ietf-mext-binding-revocation [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 draft-ietf-mext-binding-revocation [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 draft-ietf-mext-binding-revocation [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 draft-ietf-mext-nemo-v4traversal [2] and IETF RFC 3775 [6].

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 draft-ietf-mext-nemo-v4traversal [2] and IETF RFC 3775 [6].

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

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 3775 [6], draft-ietf-mext-nemo-v4traversal [2] and draft-ietf-mext-binding-revocation [19].

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 3775 [6]
Lifetime	Set to the requested number of time in units of 4 seconds the binding shall remain valid.	IETF RFC 3775 [6]
Home Registration (H)	Set to "1" to indicate receiving node should act as this node"s HA	IETF RFC 3775 [6]
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 3775 [6]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 3775 [6]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 3775 [6]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	draft-ietf-mext-nemo-v4traversal [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]

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'.	draft-ietf-mext-nemo-v4traversal [2]
IPv 4 Care-of Address	C	Set to the IPv4 Care-of address when in an IPv4 Access Network.	draft-ietf-mext-nemo-v4traversal [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 3775 [6]

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 3775 [6]
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 3775 [6], draft-ietf-mext-nemo-v4traversal [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 3775 [6]
Lifetime	Set to the granted number of time units of 4 seconds the binding shall remain valid.	IETF RFC 3775 [6]

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 Home 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".	draft-ietf-mext-nemo-v4traversal [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.	draft-ietf-mext-nemo-v4traversal [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 3775 [6]

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 3775 [6]
Home Address	The home address that was contained in the Home Address destination option	IETF RFC 3775 [6]

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 3775 [6]
Lifetime	Set to the requested number of time units the binding shall remain valid.	IETF RFC 3775 [6]
Home Registration (H)	Set to " 1" to indicate receiving node should act as this node"s HA	IETF RFC 3775 [6]
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 3775 [6]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 3775 [6]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 3775 [6]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	draft-ietf-mext-nemo-v4traversal [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]

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.	draft-ietf-mext-nemo-v4traversal [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	draft-ietf-mext-nemo-v4traversal [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 3775 [6]

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 3775 [6]
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 3775 [6], draft-ietf-mext-nemo-v4traversal [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 3775 [6]
Lifetime	Set to the granted number of time units of 4 seconds the binding shall remain valid.	IETF RFC 3775 [6]

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 Home 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".	draft-ietf-mext-nemo-v4traversal [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.	draft-ietf-mext-nemo-v4traversal [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 3775 [6]

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 3775 [6]
Lifetime	Set to the requested number of time units the binding shall remain valid.	IETF RFC 3775 [6]
Home Registration (H)	Set to "1" to indicate receiving node should act as this node"s HA	IETF RFC 3775 [6]
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 3775 [6]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility.	IETF RFC 3775 [6]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 3775 [6]
Force UDP encapsulation request (F) Flag	Set to "0" to indicate no forced UDP encapsulation	draft-ietf-mext-nemo-v4traversal [2]
Mobile Router Flag (R)	Set to "1" to indicate home network prefix preservation for the UE.	IETF RFC 3963 [29]

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,	draft-ietf-mext-nemo-v4traversal [2]
IPv 4 Care-of Address	C	Set to the IPv4 Care-of address when in an IPv4 Access Network.	draft-ietf-mext-nemo-v4traversal [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 3775 [6]

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 3775 [6]
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 3775 [6], draft-ietf-mext-nemo-v4traversal [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 3775 [6]
Lifetime	Set to the granted number of time units of 4 seconds the binding shall remain valid.	IETF RFC 3775 [6]

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

Mobility Option	Cat.	Mobility Option Description	Reference
IPv4 Home 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".	draft-ietf-mext-nemo-v4traversal [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.	draft-ietf-mext-nemo-v4traversal [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 3775 [6]

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 3775 [6]
Lifetime	Set to a value of "0" indicating that the Binding Cache entry for the UE is to be deleted.	IETF RFC 3775 [6]
Home Registration (H)	Set to "1" to indicate receiving node should act as this node"s HA	IETF RFC 3775 [6]
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 3775 [6]
Key Management Mobility Capability (K)	Set to "1" to indicate IKEv2 SA ability to survive mobility	IETF RFC 3775 [6]
Acknowledge (A)	Set to "1" to request an acknowledgement message.	IETF RFC 3775 [6]
Force UDP encapsulation request (F) Flag	Set to "0 " to indicate no forced UDP encapsulation	draft-ietf-mext-nemo-v4traversal [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.	draft-ietf-mext-nemo-v4traversal [2]
IPv 4 Care-of Address	C	Set to the IPv4 Care-of address when in an IPv4 Access Network.	draft-ietf-mext-nemo-v4traversal [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 3775 [6]

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 3775 [6]
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 3775 [6], draft-ietf-mext-nemo-v4traversal [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 3775 [6]
Lifetime	Set to "0".	IETF RFC 3775 [6]

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
IPv4 Home Address 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.	draft-ietf-mext-nemo-v4traversal [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.	draft-ietf-mext-binding-revocation [19]
Sequence Number	Set to a monotonically increasing value and is used to match with the returned Binding Revocation Acknowledge	draft-ietf-mext-binding-revocation [19]
Revocation Trigger	Set to "1"	draft-ietf-mext-binding-revocation [19]
Proxy Binding (P)	Set to "0"	draft-ietf-mext-binding-revocation [19]
Acknowledge (A)	Set to "1" to request a Binding Revocation Acknowledgement	draft-ietf-mext-binding-revocation [19]
Global (G)	Set to "0"	draft-ietf-mext-binding-revocation [19]
IPv4 HoA Binding Only (V)	Set to "0"	draft-ietf-mext-binding-revocation [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.	Draft-ietf-mext-binding-revocation [19]
Sequence Number	Set to the value received in the corresponding BRI.	draft-ietf-mext-binding-revocation [19]
Status	Indicates the result of the BRI.	draft-ietf-mext-binding-revocation [19]
Proxy Registration Flag (P)	Set to "0" to indicate that the Binding Revocation Acknowledgment is NOT for a proxy MIPv6 binding entry.	draft-ietf-mext-binding-revocation [19]
Global (G)	Set to "0"; the same value as for the BRI.	draft-ietf-mext-binding-revocation [19]
IPv4 HoA Binding Only (V)	Set to "0"	draft-ietf-mext-binding-revocation [19]

A.7 Void

Annex B (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

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
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

History

Document history		
V8.0.0	January 2009	Publication
V8.1.0	March 2009	Publication
V8.2.0	June 2009	Publication