Diameter Maintenance and	J. Korhonen, Ed.	
Extensions (DIME)	H. Tschofenig	
Internet-Draft	Nokia Siemens Networks	
Intended status: Standards Track	J. Bournelle	
Expires: October 30, 2009	Orange Labs	
	G. Giaretta	
	Qualcomm	
	M. Nakhjiri	
	Motorola	
	April 28, 2009	

TOC

Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction
draft-ietf-dime-mip6-split-17.txt

Status of this Memo

Copyright Notice

Abstract

Mobile IPv6 deployments may want to bootstrap their operations dynamically based on an interaction between the Home Agent and the Diameter server of the Mobile Service Provider. This document specifies the interaction between a Mobile IP Home Agent and a Diameter server. This document defines the Home Agent to the Diameter server communication when the mobile node authenticates using the Internet Key Exchange v2 protocol with the Extensible Authentication Protocol or using the Mobile IPv6 Authentication Protocol. In addition to authentication and authorization, the configuration of Mobile IPv6 specific parameters and accounting is specified in this document.

Table of Contents

---

1. Introduction

TOC

Performing the Mobile IPv6 protocol [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.), requires the Mobile Node (MN) to own a Home Address (HoA) and to have an assigned Home Agent (HA) to the MN. The MN needs to register with the HA in order to enable its reachability and mobility, when away from its home link. The registration process itself may require an establishment of IPsec security associations (SA) and cryptographic material between the MN and the HA. Alternatively, the registration process may be secured using a mobility message authentication option, which enables IPv6 mobility in a MN without having to establish an IPsec SA with its HA. Providing the collection of home address, HA address and keying material is generally referred to as the Mobile IPv6 bootstrapping problem [RFC4640] (Patel, A. and G. Giaretta, “Problem Statement for

bootstrapping Mobile IPv6 (MIPv6)," September 2006.). The purpose of this specification is to provide Diameter support for the interaction between the HA and the Authentication, Authorization, and Accounting (AAA) server. This specification satisfies the requirements defined in [I-D.ietf-mext-aaa-ha-goals] (Giaretta, G., Guardini, I., Demaria, E., Bournelle, J., and R. Lopez, "AAA Goals for Mobile IPv6," May 2008.) for the bootstrapping problem in the split scenario [RFC5026] (Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario," October 2007.) and also specifies Diameter support for the Authentication Protocol for Mobile IPv6 [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6," January 2006.). The Diameter support defined in this specification also applies to Dual Stack Mobile IPv6 [I-D.ietf-mext-nemo-v4traversal] (Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers," April 2009.). From a Mobility Service Provider (MSP) perspective, it is important to verify that the MN is authenticated and authorized to utilize Mobile IPv6 service, and is accounted for those. Only when the MN is authenticated and authorized, the MSP allows the bootstrapping of Mobile IPv6 parameters. Thus, prior to processing the Mobile IPv6 registrations, the HA participates in the authentication of the MN to verify the MN's identity. The HA also participates in the Mobile IPv6 authorization process involving the Diameter infrastructure. The HA, due to its role in traffic forwarding, may also perform accounting for the Mobile IPv6 service provided to the MN.
This document enables the following functionality:

Authentication: Verifying the MN's identity. As a Diameter client supporting the new Diameter Mobile IPv6 application, the HA may need to support more than one authentication type depending on the environment. Although the authentication is performed by the AAA server there is an impact for the HA as different set of command codes are needed for the respective authentication procedures.

Authorization: The HA must verify that the user is authorized to the Mobile IPv6 service using the assistance of the MSP Diameter servers. This is accomplished through the use of new Diameter applications specifically designed for performing Mobile IPv6 authorization decisions. This document defines required AAA procedures and requires the HA to support them and to participate in this authorization signaling.

Accounting: For accounting purposes and capacity planning, it is required that the HA provides accounting reports to the Diameter infrastructure and thus to support the related Diameter

accounting procedures.

Session Management: The management of the mobility services may require the Diameter server or the HA to terminate the Mobile IPv6 service before the binding expires. This document defines procedures for the AAA based session management.

Figure 1 (Architecture Overview) depicts the reference architecture for this document.

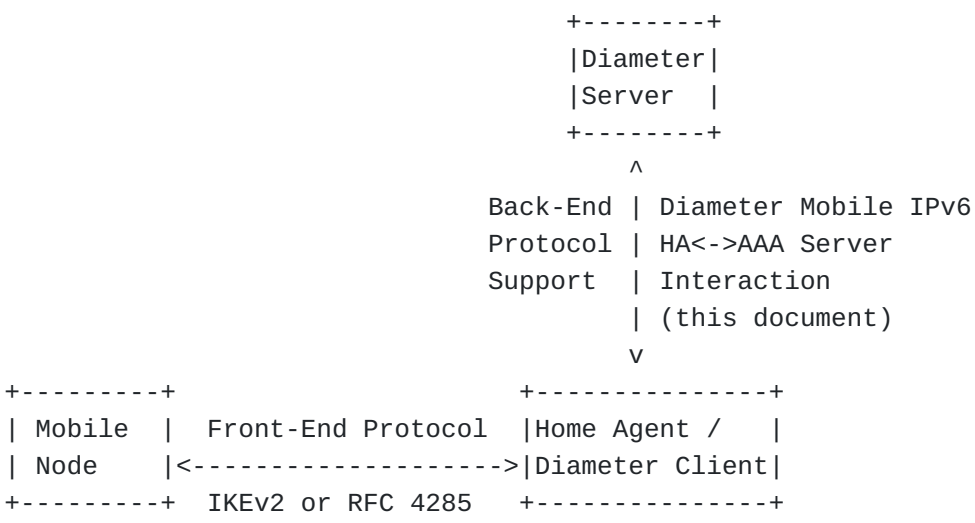

Figure 1: Architecture Overview

Mobile IPv6 signaling between the MN and the HA can be protected using two different mechanisms, namely using IPsec or the Authentication Protocol for Mobile IPv6 [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6," January 2006.). For these two approaches several different authentication and key exchange solutions are available. When IPsec is used to protect Mobile IPv6 signaling messages, Internet Key Exchange v2 (IKEv2) is used [RFC4877] (Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," April 2007.) for the setup of the IPsec SAs. IKEv2 supports Extensible Authentication Protocol (EAP) based initiator authentication, certificates and pre-shared secrets. Alternatively, the Authentication Protocol for Mobile IPv6 uses a mechanism that is very similar to the one used for protecting Mobile IPv4 signaling messages.
The ability to use different credentials and methods to authenticate the MN has an impact on the AAA interactions between the HA (acting as a Diameter client) and the Diameter Server. This specification is only limited to the following MN authentication methods:

*IKEv2 usage with EAP

*Mobile IPv6 Authentication Protocol

New authentication mechanisms may be added later by separate specifications.
For accounting of Mobile IPv6 services provided to the MN, this specification uses the Diameter Base Protocol accounting defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.).

---

2. Terminology

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
The Mobile IPv6 bootstrapping terminology is taken from [RFC4640] (Patel, A. and G. Giaretta, “Problem Statement for bootstrapping Mobile IPv6 (MIPv6),” September 2006.). Additional terminology is defined below:

Authentication, Authorization, and Accounting (AAA):
AAA protocol based on Diameter [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.) with required EAP support [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, “Diameter Extensible Authentication Protocol (EAP) Application,” August 2005.).

Home AAA (AAAH):
An authentication, authorization and accounting server located in user's home network i.e., in the home realm.

---

3. Application Identifiers

TOC

This specification defines two new Diameter applications and their respective Application Identifiers:

```
Diameter Mobile IPv6 IKE   (MIP6I)  TBD by IANA
Diameter Mobile IPv6 Auth  (MIP6A)  TBD by IANA
```

The MIP6I Application Identifier is used when the MN is authenticated and authorized using IKEv2. The MIP6A Application Identifier is used when the MN is authenticated and authorized using the Mobile IPv6 Authentication Protocol.
Mobile IPv6 related accounting information generated by the HA uses either the MIP6I or the MIP6A Application Identifier in the case of coupled accounting model. The Diameter Base Accounting Application Identifier (value of 3) is used in case of the split accounting model. Refer to Section 4.4 (Accounting for Mobile IPv6 services) for more information regarding the accounting models.

---

4. Protocol Description

TOC

4.1. Support for Mobile IPv6 with IKEv2 and EAP

TOC

The use of IKEv2 with EAP between the MN and the HA allows the AAA to authenticate the MN. When EAP is used with IKEv2, the Diameter EAP application logic and procedures, as defined in [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.), are re-used. EAP methods that do not establish a shared key SHOULD NOT be used, as they are subject to a number of man-in-the-middle attacks as stated in Section 2.16 and Section 5 of [RFC4306] (Kaufman, C., "Internet Key Exchange (IKEv2) Protocol," December 2005.). AVPs specific to Mobile IPv6 bootstrapping are added to the EAP application commands.
Figure 2 (Mobile IPv6 bootstrapping using IKEv2 and EAP) shows the message flow involved during the authentication phase when EAP is used. The communication between the mobile node and the home agent use the conventions defined in [RFC4306] (Kaufman, C., "Internet Key Exchange (IKEv2) Protocol," December 2005.). Similarly, the communication between the home agent and the Diameter server use the conventions defined in [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.).

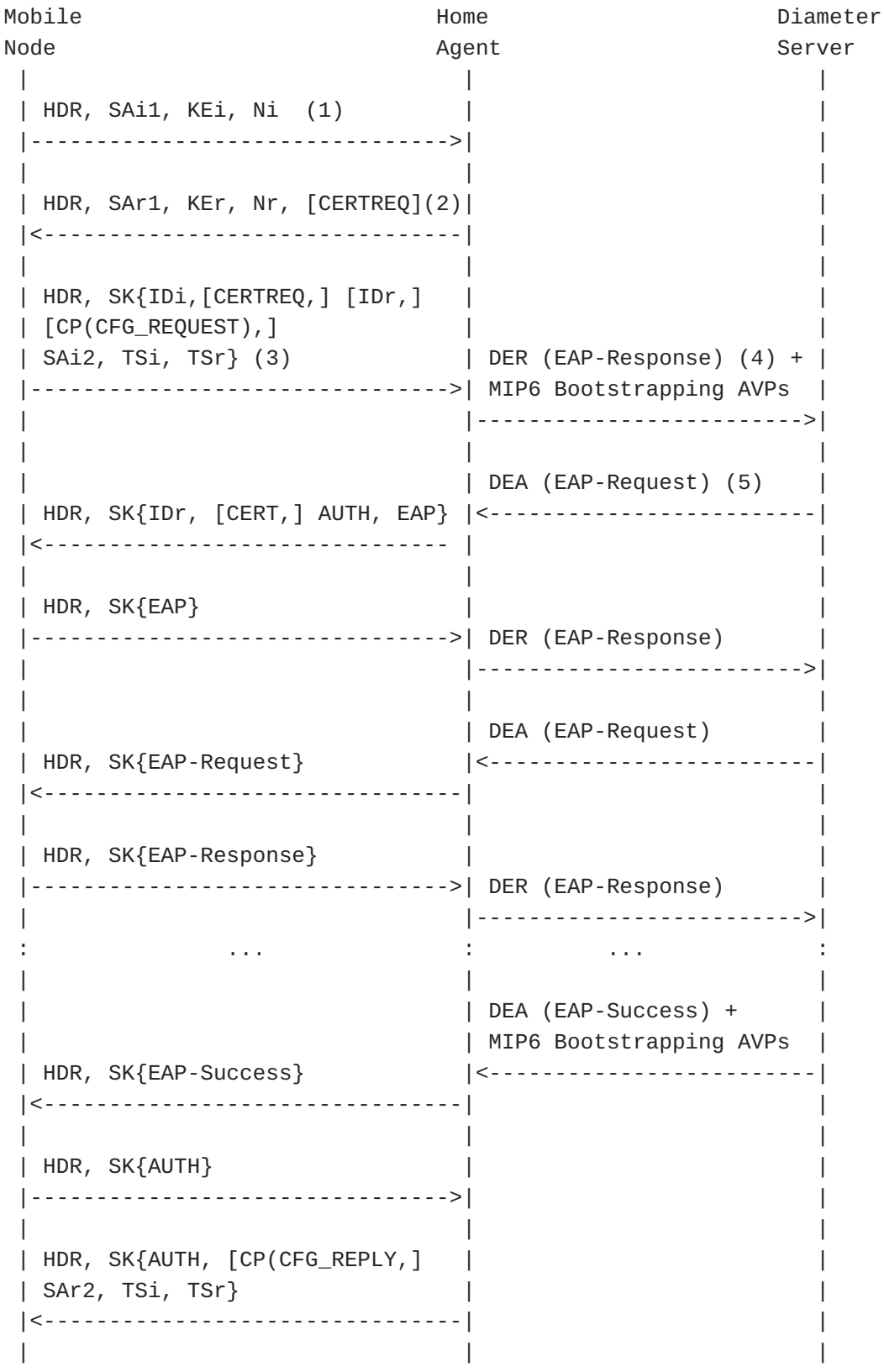

Figure 2: Mobile IPv6 bootstrapping using IKEv2 and EAP

The MN and the HA start the interaction with an IKE_SA_INIT exchange. In this phase cryptographic algorithms are negotiated, nonces and Diffie-Hellman parameters are exchanged. Message (3) starts the IKE_AUTH phase. This second phase authenticates the previous messages, exchanges identities and certificates and establishes the first CHILD_SA. It is used to mutually authenticate the MN (acting as an IKEv2 Initiator) and the HA (acting as an IKEv2 Responder). The identity of the user/MN is provided in the IDi field. The MN indicates its willingness to be authenticated via EAP by omitting the AUTH field in message (3) (see Section 2.16 of [RFC4306] (Kaufman, C., “Internet Key Exchange (IKEv2) Protocol,” December 2005.)).

As part of the authentication process, the MN MAY request a Home-Address, a Home Prefix or suggests one, see [RFC4877] (Devarapalli, V. and F. Dupont, “Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture,” April 2007.), using a CFG_REQUEST payload in the message (3).

The HA extracts the IDi field from the message (3) and sends a Diameter-EAP-Request (DER) message (4) towards the authenticating Diameter server. The EAP-Payload AVP contains a EAP-Response/Identity with the identity extracted from the IDi field.

This message is routed to the MN's Diameter server/EAP server. The Diameter server selects the EAP method and replies with the Diameter-EAP-Answer (DEA) Message. Depending on the type of EAP method chosen, a number of DER and DEA messages carry the method specific exchanges between the MN and the Diameter server/EAP server.

At the end of the EAP authentication phase, the Diameter server indicates the result of the authentication in the Result-Code AVP and provides the corresponding EAP packet (EAP Success or EAP Failure). The last IKEv2 message sent by the HA contains the Home Address or the Home Prefix. In the latter case, a CREATE_CHILD_SA exchange is necessary to setup IPsec SAs for Mobile IPv6 signaling.

In some deployment scenarios, the HA may also act as an IKEv2 Responder for a conventional IPsec VPN access. The challenge in this case is that the IKEv2 responder may not know if IKEv2 is used for Mobile IPv6 service or for IPsec VPN access service. A network operator needs to be aware of this limitation. One solution already supported by IKEv2 is to use different responder identities when operating as a conventional IPsec VPN gateway or as a HA. The MN can then indicate the preferred responder type using the appropriate IDr payload in the IKE_AUTH message.

Eventually, when the HA receives a Binding Update (BU), the HA authenticates and authorizes the MN. It is RECOMMENDED that the HA sends an accounting request message every time it receives a BU.

TOC

4.2. Support for the Mobile IPv6 Authentication Protocol

Figure 3 (Mobile IPv6 Bootstrapping using the Mobile IPv6 Authentication Protocol) shows the message sequence between the MN, the HA and the Diameter server during the registration when Mobile IPv6 Authentication Protocol is used. A BU and a Binding Acknowledgement (BA) messages are used in the binding registration process.
Receiving a BU at the HA initiates a MIP6-Request to be sent to the Diameter server. The Diameter server in turn responds with a MIP6-Answer. The HA may assign a Home Address to the MN and provide it to the Diameter server in the MIP-Mobile-Node-Address AVP.
According to [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, “Authentication Protocol for Mobile IPv6,” January 2006.) the MN uses the Mobile Node Identifier Option, specifically the MN-NAI mobility option (as defined in [RFC4283] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, “Mobile Node Identifier Option for Mobile IPv6 (MIPv6),” November 2005.)) to identify itself. The HA MUST copy the MN-NAI mobility option value to the User-Name AVP in the subsequent request messages.
The procedure described in this specification for the Mobile IPv6 Authentication Protocol is only needed for the initially received BU for which the HA does not have an existing security association. When the HA receives subsequent BUs, they are processed locally in the HA. It is RECOMMENDED that the HA sends an accounting request message every time it receives a Binding Update. However, the HA MAY re-authorize the MN with the Diameter server at any time depending on the deployment and the local policy.
This specification assumes that in the case Mobile IPv6 Authentication Protocol is used, the MN-AAA option is included in the BU as defined in [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, “Authentication Protocol for Mobile IPv6,” January 2006.) and the Diameter server computes required session keys after having successfully authenticated the MN. The computation of the session keys is out of scope of this specification. Other possible ways of using Mobile IPv6 Authentication Protocol are also out of scope of this specification and would require a new specification to describe the detailed behavior of the HA-AAAH interface and corresponding session key derivation.

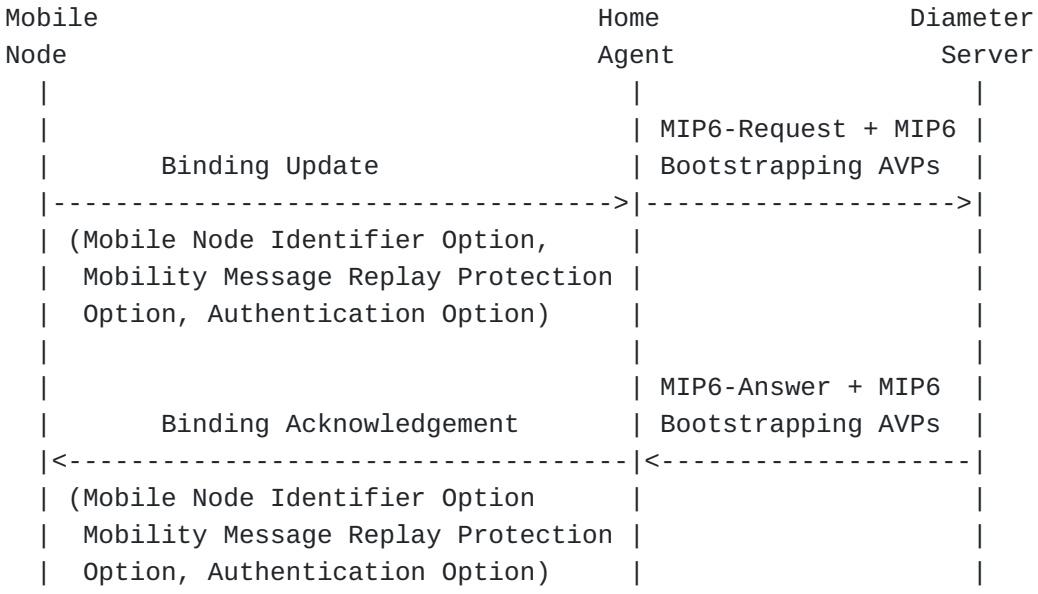

Figure 3: Mobile IPv6 Bootstrapping using the Mobile IPv6 Authentication Protocol

4.3. Mobile IPv6 Session Management

TOC

The Diameter server may maintain state or may be stateless. This is indicated in the Auth-Session-State AVP (or its absence). The HA MUST support the Authorization Session State Machine defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.).
This specification makes an assumption that each SA created between the MN and the HA as a result of a successful IKEv2 negotiation or a Mobile IPv6 Authentication Protocol exchange correspond to one Diameter session. In IKEv2 case we specifically mean the created IKE SA.

4.3.1. Session-Termination-Request

TOC

The Session-Termination-Request (STR) message [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) is sent by the HA to inform the Diameter server that an authorized session is being terminated. This means that the HA MUST terminate the corresponding Mobile IPv6 binding and also terminate the corresponding SA.

4.3.2. Session-Termination-Answer

TOC

The Session-Termination-Answer (STA) message [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) is sent by the Diameter server to acknowledge the notification that the session has been terminated.

4.3.3. Abort-Session-Request

TOC

The Abort-Session-Request (ASR) message [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) is sent by the Diameter server to the HA to terminate the authorized session. This fulfills one of the requirement described in [I-D.ietf-mext-aaa-ha-goals] (Giaretta, G., Guardini, I., Demaria, E., Bournelle, J., and R. Lopez, "AAA Goals for Mobile IPv6," May 2008.). When the HA receives the ASR message, it MUST terminate the corresponding SA. Subsequently, the HA MUST take further actions to terminate the corresponding Mobile IPv6 binding.

4.3.4. Abort-Session-Answer

TOC

The Abort-Session-Answer (ASA) message [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) is sent by the Home Agent in response to an ASR message.

4.4. Accounting for Mobile IPv6 services

TOC

The HA MUST be able act as a Diameter client collecting accounting records needed for service control and charging. The HA MUST support the accounting procedures (specifically the command codes mentioned below) and the Accounting Session State Machine as defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.). The command codes, exchanged between the HA and Diameter server for accounting purposes, are provided in the following subsections.
The Diameter application design guideline [I-D.ietf-dime-app-design-guide] (Fajardo, V., Tschofenig, H., and L.

Morand, “Diameter Applications Design Guidelines,” March 2010.) defines two separate models for accounting:

> **Split accounting model:**
>
> According to this model, the accounting messages use the Diameter Base Accounting Application Identifier (value of 3). Since accounting is treated as an independent application, accounting commands may be routed separately from the rest of application messages and thus the accounting messages generally end up in a central accounting server. Since Diameter Mobile IPv6 application does not define its own unique accounting commands, this is the preferred choice, since it permits use of centralized accounting for several applications.
>
> **Coupled accounting model:**
>
> In this model, the accounting messages will use either the MIP6I or the MIP6A Application Identifiers. This means that accounting messages will be routed like any other Mobile IPv6 application messages. This requires the Diameter server in charge of Mobile IPv6 application to handle the accounting records (e.g., sends them to a proper accounting server).

As mentioned above, the preferred choice is to use the split accounting model and thus to choose Diameter Base Accounting Application Identifier (value of 3) for accounting messages.

4.4.1. Accounting-Request

TOC

The Accounting-Request command [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.) is sent by the HA to the Diameter server to exchange accounting information regarding the MN with the Diameter server.

4.4.2. Accounting-Answer

TOC

The Accounting-Answer command [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.) is sent by the Diameter server to the HA to acknowledge an Accounting-Request.

---

5. Command Codes

TOC

5.1. Command Code for Mobile IPv6 with IKEv2 and EAP

TOC

For the use of Mobile IPv6 with IKEv2 and EAP this document reuses the Diameter EAP application [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.) commands: Diameter-EAP-Request (DER) and Diameter-EAP-Answer (DEA). This specification extends the existing DER and DEA command ABNFs with a number of AVPs to support Mobile IPv6 split scenario bootstrapping. Other than new additional AVPs and the corresponding additions to the command ABNFs, the Diameter EAP application command ABNFs remain unchanged. The ABNF language is defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.).

Command-Name	Abbrev.	Code	Reference	Application
Diameter-EAP-Request	DER	268	RFC 4072	Diameter Mobile IPv6 IKE
Diameter-EAP-Answer	DEA	268	RFC 4072	Diameter Mobile IPv6 IKE

Figure 4: Command Codes

5.1.1. Diameter-EAP-Request

TOC

The Diameter-EAP-Request (DER) message, indicated by the Command-Code field set to 268 and the 'R' bit set in the Command Flags field, is sent by the HA to the Diameter server to initiate a Mobile IPv6 service authentication and authorization procedure. The Application-ID field of the Diameter Header MUST be set to the Diameter Mobile IPv6 IKE Application ID (value of TDB).

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
                           < Session-Id >
                           { Auth-Application-Id }
                           { Origin-Host }
                           { Origin-Realm }
                           { Destination-Realm }
                           { Auth-Request-Type }
                           [ Destination-Host ]
                           [ NAS-Identifier ]
                           [ NAS-IP-Address ]
                           [ NAS-IPv6-Address ]
                           [ NAS-Port-Type ]
                           [ User-Name ]
                           ...
                           { EAP-Payload }
                           ...
                           [ MIP6-Feature-Vector ]
                           [ MIP6-Agent-Info ]
                          *2[ MIP-Mobile-Node-Address ]
                           [ Chargeable-User-Identity ]
                           [ Service-Selection ]
                           [ QoS-Capability ]
                          * [ QoS-Resources ]
                           ...
                          * [ AVP ]
```

Mobile IPv6 bootstrapping AVPs are only included in the first DER message send by the HA. The subsequent DER messages required by the EAP-method do not need to include any Mobile IPv6 bootstrapping AVPs. The MN is both authenticated and authorized for the mobility service during the EAP authentication. Thus, the Auth-Request-Type AVP MUST be set to the value AUTHORIZE_AUTHENTICATE.

5.1.2. Diameter-EAP-Answer

TOC

The Diameter-EAP-Answer (DEA) message, indicated by the Command-Code field set to 268 and 'R' bit cleared in the Command Flags field, is sent in response to the Diameter-EAP-Request message (DER). The Application-Id field in the Diameter message header MUST be set to the Diameter Mobile IPv6 IKE Application-Id (value of TBD). If the Mobile IPv6 authentication procedure was successful then the response MAY include any set of bootstrapping AVPs.

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
                          < Session-Id >
                          { Auth-Application-Id }
                          { Auth-Request-Type }
                          { Result-Code }
                          { Origin-Host }
                          { Origin-Realm }
                          [ User-Name ]
                          [ EAP-Payload ]
                          [ EAP-Reissued-Payload ]
                          [ EAP-Master-Session-Key ]
                          [ EAP-Key-Name ]
                          [ Multi-Round-Time ]
                          ...
                         *2[ MIP-Mobile-Node-Address ]
                          [ MIP6-Feature-Vector ]
                          [ MIP6-Agent-Info ]
                          [ Service-Selection ]
                         * [ QoS-Resources ]
                          [ Chargeable-User-Identity ]
                          ...
                         * [ AVP ]
```

If the EAP-based authentication and the authorization for the mobility service succeeds, then the Mobile IPv6 bootstrapping AVPs are included in the last DEA message that also carries the EAP-Success EAP payload. The other DEA messages required by the used EAP-method do not include any Mobile IPv6 bootstrapping AVPs.

5.2. Command Codes for Mobile IPv6 Authentication Protocol Support

TOC

This section defines the commands that are used for support with the Mobile IPv6 Authentication Protocol.
There are multiple ways of deploying and utilizing Mobile IPv6 Authentication Protocol, especially regarding the associated AAA interactions. In order to support multiple deployment models this specification defines the MIP6-Auth-Mode AVP that in the request message tells the mode that the HA supports. This specification defines a method that requires the use of the MN-AAA option with the Mobile IPv6 Authentication Protocol.

Command-Name	Abbrev.	Code	Reference	Application
MIP6-Request	MIR	TBD	5.3.1	Diameter Mobile IPv6 Auth
MIP6-Answer	MIA	TBD	5.3.2	Diameter Mobile IPv6 Auth

Command Codes

5.2.1. MIP6-Request

TOC

The MIP6-Request (MIR), indicated by the Command-Code field set to TBD and the 'R' bit set in the Command Flags field, is sent by the HA, acting as a Diameter client, in order to request the authentication and authorization of a MN.
Although the HA provides the Diameter server with replay protection related information, the HA is responsible for the replay protection.
The message format is shown below.

```
<MIP6-Request> ::= < Diameter Header: TBD, REQ, PXY >
                   < Session-ID >
                   { Auth-Application-Id }
                   { User-Name }
                   { Destination-Realm }
                   { Origin-Host }
                   { Origin-Realm }
                   { Auth-Request-Type }
                   [ Destination-Host ]
                   [ Origin-State-Id ]
                   [ NAS-Identifier ]
                   [ NAS-IP-Address ]
                   [ NAS-IPv6-Address ]
                   [ NAS-Port-Type ]
                   [ Called-Station-Id ]
                   [ Calling-Station-Id ]
                   [ MIP6-Feature-Vector ]
                   { MIP6-Auth-Mode }
                   [ MIP-MN-AAA-SPI ]
                   [ MIP-MN-HA-SPI ]
                 1*2{ MIP-Mobile-Node-Address }
                   { MIP6-Agent-Info }
                   { MIP-Careof-Address }
                   [ MIP-Authenticator ]
                   [ MIP-MAC-Mobility-Data ]
                   [ MIP-Timestamp ]
                   [ QoS-Capability ]
                  * [ QoS-Resources ]
                   [ Chargeable-User-Identity ]
                   [ Service-Selection ]
                   [ Authorization-Lifetime ]
                   [ Auth-Session-State ]
                  * [ Proxy-Info ]
                  * [ Route-Record ]
                  * [ AVP ]
```

If the MN is both authenticated and authorized for the mobility service, then the Auth-Request-Type AVP is set to the value AUTHORIZE_AUTHENTICATE. This is the case when the MIP6-Auth-Mode is set to the value MIP6_AUTH_MN_AAA.

5.2.2. MIP6-Answer

TOC

The MIP6-Answer (MIA) message, indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by

the Diameter server in response to the MIP6-Request message. The User-Name AVP MAY be included in the MIA if it is present in the MIR. The Result-Code AVP MAY contain one of the values defined in Section 7 (Result-Code AVP Values), in addition to the values defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.).
An MIA message with the Result-Code AVP set to DIAMETER_SUCCESS MUST include the MIP-Mobile-Node-Address AVP.
The message format is shown below.

```
     <MIP6-Answer> ::= < Diameter Header: TBD, PXY >
                       < Session-Id >
                       { Auth-Application-Id }
                       { Result-Code }
                       { Origin-Host }
                       { Origin-Realm }
                       { Auth-Request-Type }
                       [ User-Name ]
                       [ Authorization-Lifetime ]
                       [ Auth-Session-State ]
                       [ Error-Message ]
                       [ Error-Reporting-Host ]
                       [ Re-Auth-Request-Type ]
                       [ MIP6-Feature-Vector ]
                       [ MIP-Agent-Info ]
                      *2[ MIP-Mobile-Node-Address ]
                       [ MIP-MN-HA-MSA ]
                      * [ QoS-Resources ]
                       [ Chargeable-User-Identity ]
                       [ Service-Selection ]
                       [ Origin-State-Id ]
                      * [ Proxy-Info ]
                      * [ Redirect-Host ]
                       [ Redirect-Host-Usage ]
                       [ Redirect-Max-Cache-Time ]
                      * [ Failed-AVP ]
                      * [ AVP ]
```

---

6. AVPs

TOC

To provide support for [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6," January 2006.) and for [RFC4877] (Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," April 2007.) the AVPs in the following subsections are needed.

[RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.), [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, “Diameter Mobile IPv4 Application,” August 2005.) and [RFC4005] (Calhoun, P., Zorn, G., Spence, D., and D. Mitton, “Diameter Network Access Server Application,” August 2005.) defined AVPs are reused whenever possible without changing the existing semantics of those AVPs.

Attribute Name	AVP Code	Defined in	Value Type	AVP Flag rules: MUST	MAY	SHOULD NOT	MUST NOT	MAY Encr
MIP6-Feature-Vector	124	RFC5447	Unsigned64	M	P		V	Y
MIP-Mobile-Node-Address	334	RFC4004	Address	M	P		V	Y
MIP6-Agent-Info	486	RFC5447	Grouped	M	P		V	Y
User-Name	1	RFC3588	UTF8String	M	P		V	Y
Service-Selection	TBD	6.2	UTF8String	M	P		V	Y
QoS-Capability	TBD	Note 1	Grouped	M	P		V	Y
QoS-Resources	TBD	Note 1	Grouped	M	P		V	Y
MIP-MN-HA-MSA	TBD	6.12	Grouped	M	P		V	Y
Chargeable-User-Identity	89	6.19	OctetString	M	P		V	Y

AVPs for Mobile IPv6 IKE Application

Note 1: The QoS-Capability and the QoS-Resource AVPs are defined in Sections 4.1 and 4.3 of [I-D.ietf-dime-qos-attributes] (Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., and A. Lior, “Traffic Classification and Quality of Service Attributes for Diameter,” December 2009.).

				AVP Flag rules				
Attribute Name	AVP Code	Section Defined	Value Type	MUST	MAY	SHOULD NOT	MUST NOT	MAY Encr
MIP6-Feature-Vector	124	RFC5447	Unsigned64	M	P		V	Y
User-Name	1	RFC3588	UTF8String	M	P		V	Y
Service-Selection	TBD	6.2	UTF8String	M	P		V	Y
MIP-MN-AAA-SPI	341	RFC4004	Unsigned32	M	P		V	Y
MIP-MN-HA-SPI	TBD	6.4	Unsigned32	M	P		V	Y
MIP-Mobile-Node-Address	333	RFC4004	Address	M	P		V	Y
MIP6-Agent-Info	486	RFC5447	Grouped	M	P		V	Y
MIP-Careof-Address	TBD	6.7	Address	M	P		V	Y
MIP-Authenticator	TBD	6.8	OctetString	M	P		V	Y
MIP-MAC-Mobility-Data	TBD	6.9	OctetString	M	P		V	Y
MIP-Session-Key	343	6.10	OctetString	M	P		V	Y
MIP-MSA-Lifetime	367	RFC4004	Unsigned32	M	P		V	Y
MIP-MN-HA-MSA	TBD	6.12	Grouped	M	P		V	Y
MIP-Algorithm-Type	345	6.13	Enumerated	M	P		V	Y
MIP-Replay-Mode	346	6.14	Enumerated	M	P		V	Y
MIP-Timestamp	TBD	6.16	OctetString	M	P		V	Y
QoS-Capability	TBD	Note 1	Grouped	M	P		V	Y

QoS-Resources	TBD	Note 1	Grouped	M	P		V	Y
Chargeable-User-Identity	89	6.19	OctetString	M	P		V	Y
MIP6-Auth-Mode	TBD	6.20	Enumerated	M	P		V	Y
Rest of the AVPs in the MIR & MIA excluding *[AVP]		RFC3588 RFC4005		M	P		V	Y

AVPs for the Mobile IPv6 Auth Application

Note 1: The QoS-Capability and the QoS-Resource AVPs are defined in Sections 4.1 and 4.3 of [I-D.ietf-dime-qos-attributes] (Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., and A. Lior, "Traffic Classification and Quality of Service Attributes for Diameter," December 2009.).

6.1. User-Name AVP

TOC

The User-Name AVP (AVP Code 1) is of type UTF8String and contains an NAI extracted from the MN-NAI mobility option included in the received BU message. Alternatively, the NAI can be extracted from the IKEv2 IDi payload included in the IKE_AUTH message sent by the IKE initiator.

6.2. Service-Selection AVP

TOC

The Service-Selection AVP (AVP Code TBD) is of type UTF8String and contains the name of the service or the external network that the mobility service should be associated with. In the scope of this specification the value can extracted from the IKEv2 IDr payload, if available in the IKE_AUTH message sent by the IKE initiator. Alternatively, if the Mobile IPv6 Authentication Protocol is used, then the Service-Selection AVP contains the string extracted from the Service Selection Mobility Option [RFC5149] (Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6," February 2008.), if available in the received BU. Future specification may define additional ways to populate the Service-Selection AVP with the required information.

The AVP is also available to be used in messages sent from the Diameter server to the Diameter client. For example, if the request message did not contain the Service-Selection AVP but the MN was assigned with a default service, the Diameter server MAY return the name of the assigned default service to the HA.
If the Service-Selection AVP is present in both the request and the reply messages, it SHOULD contain the same service name. If the services differ, the HA MAY treat that as authorization failure.

6.3. MIP-MN-AAA-SPI AVP

TOC

The MIP-MN-AAA-SPI AVP (AVP Code 341) is of type Unsigned32 and contains an SPI code extracted from the Mobility Message Authentication Option included in the received BU message. This AVP is re-used from [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, “Diameter Mobile IPv4 Application,” August 2005.).
When the MIP6-Auth-Mode AVP is set to value MIP6_AUTH_MN_AAA, this AVP MUST be present in the MIR message.

6.4. MIP-MN-HA-SPI AVP

TOC

The MIP-MN-HA-SPI AVP (AVP Code TBD) is of type Unsigned32 and contains an SPI value that can be used with other parameters for identifying the security association required for the validation of the Mobile IPv6 MN-HA Authentication Option.
When the MIP6-Auth-Mode AVP is set to value MIP6_AUTH_MN_AAA, and the Diameter server returns a valid MIP-MN-HA-MSA AVP in the MIA message, this AVP MUST be present inside the MIP-MN-HA-MSA AVP.

6.5. MIP-Mobile-Node-Address AVP

TOC

The MIP-Mobile-Node-Address AVP (AVP Code 333) is of type Address and contains the HA assigned IPv6 or IPv4 Home Address of the Mobile Node. If the MIP-Mobile-Node-Address AVP contains the unspecified IPv6 address (0::0) or the all zeroes IPv4 address (0.0.0.0) in a request message, then the HA expects the Diameter server to assign the Home Address in a subsequent answer message. If the Diameter server assigns only an IPv6 Home Network Prefix to the Mobile Node the lower 64 bits of the MIP-Mobile-Node-Address AVP provided address MUST be set to zero.

This AVP is re-used from [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, “Diameter Mobile IPv4 Application,” August 2005.).

6.6. MIP6-Agent-Info AVP

TOC

The MIP6-Agent-Info AVP (AVP Code 486) is defined in Section 4.2.1 of [RFC5447] (Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, “Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction,” February 2009.) and contains the IPv6 or the IPv4 address information of the HA. The HA address in a request message is the same as in the received BU message that triggered the authentication and authorization procedure towards the Diameter server. One use case is e.g., to inform the Diameter server of the dynamically assigned HA.
If the MIP6-Agent-Info AVP is present in an answer message and the Result-Code AVP is set to DIAMETER_SUCCESS_RELOCATE_HA, then the Diameter server is indicating to the HA that it MUST initiate a HA switch procedure towards the MN (e.g., using the procedure defined in [RFC5142] (Haley, B., Devarapalli, V., Deng, H., and J. Kempf, “Mobility Header Home Agent Switch Message,” January 2008.)). If the Result-Code AVP is set to any other value, then the HA SHOULD initiate the HA switch procedure towards the MN. The address information of the assigned HA is defined in the MIP6-Agent-Info AVP.

6.7. MIP-Careof-Address AVP

TOC

The MIP-Careof-Address AVP (AVP Code TBD) is of type Address and contains the IPv6 or the IPv4 Care-of Address of the Mobile Node. The HA extracts this IP address from the received BU message.

6.8. MIP-Authenticator AVP

TOC

The MIP-Authenticator AVP (AVP Code TBD) is of type OctetString and contains the Authenticator Data from the received BU message. The HA extracts this data from the MN-AAA Mobility Message Authentication Option included in the received BU message.
When the MIP6-Auth-Mode AVP is set to value MIP6_AUTH_MN_AAA, this AVP MUST be present in the MIR message.

6.9. MIP-MAC-Mobility-Data AVP

TOC

The MIP-MAC-Mobility-Data AVP (AVP Code TBD) is of type OctetString and contains the MAC_Mobility_Data calculated by the HA as defined in [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6," January 2006.) for the MN-AAA Mobility Message Authentication Option.
When the MIP6-Auth-Mode AVP is set to value MIP6_AUTH_MN_AAA, this AVP MUST be present in the MIR message.

6.10. MIP-Session-Key AVP

TOC

The MIP-Session-Key AVP (AVP Code 343) is of type OctetString and contains the MN-HA shared secret (i.e., the session key) for the associated Mobile IPv6 MH-HA authentication option. When the Diameter server computes the session key it is placed in this AVP. How the Diameter server computes the session key is not defined in this specification. The Session key derivation is deployment specific and needs to be defines in a respective deployment specific system specification.
This AVP is re-used from [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," August 2005.).

6.11. MIP-MSA-Lifetime AVP

TOC

The MIP-MSA-Lifetime AVP (AVP Code 367) is of type Unsigned32 and represents the period of time (in seconds) for which the session key (see Section 6.10 (MIP-Session-Key AVP)) is valid. The associated session key MUST NOT be used if the lifetime has expired.
This AVP is re-used from [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," August 2005.).

6.12. MIP-MN-HA-MSA AVP

TOC

The MIP-MN-HA-MSA AVP (AVP Code TBD) is of type Grouped and contains the session related information for use with the Mobile IPv6 Authentication Protocol.

```
MIP-MN-HA-MSA ::= < AVP Header: TBD >
                  { MIP-Session-Key }
                  { MIP-MSA-Lifetime }
                  [ MIP-MN-HA-SPI ]
                  [ MIP-Algorithm-Type ]
                  [ MIP-Replay-Mode ]
                * [ AVP ]
```

The MIP-MN-HA-SPI sub-AVP within the MIP-MN-HA-MSA grouped AVP identifies the security association required for the validation of the Mobile IPv6 MN-HA Authentication Option. The absence of the MIP-Replay-Mode AVP MUST be treated as no replay protection was selected.

6.13. MIP-Algorithm-Type AVP

TOC

The MIP-Algorithm-Type AVP (AVP Code 345) is of type Enumerated and contains Algorithm identifier for the associated Mobile IPv6 MN-HA Authentication Option. The Diameter server selects the algorithm type. Existing algorithm types are defined in [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," August 2005.) that also fulfill current RFC 4285 requirements. This AVP is re-used from [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," August 2005.).
When the MIP6-Auth-Mode AVP is set to value MIP6_AUTH_MN_AAA, and the Diameter server returns a valid MIP-MN-HA-MSA AVP in the MIA message, this AVP MUST be present inside the MIP-MN-HA-MSA AVP.

6.14. MIP-Replay-Mode AVP

TOC

The MIP-Replay-Mode AVP (AVP Code 346) is of type Enumerated and contains the replay mode the HA for authenticating the mobile node. Out of all possible replay modes defined in [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," August 2005.), the following are supported by this specification:

1 None
2 Timestamp

This AVP is re-used from [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," August 2005.).

6.15. MIP6-Feature-Vector AVP

TOC

The MIP6-Feature-Vector AVP (AVP Code 124) is defined in [RFC5447] (Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction," February 2009.). However, this specification does not define any Mobile IPv6 split scenario bootstrapping specific capability flag.

6.16. MIP-Timestamp AVP

TOC

The MIP-Timestamp AVP (AVP Code TBD) is of type OctetString and contains eight octets timestamp value (i.e. 64 bits timestamp) from the Mobility message replay protection option, defined in [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6," January 2006.). The HA extracts this value from the received BU message, if available. The HA includes this AVP in the MIR message when the MN-AAA Mobility Message Authentication Option is available in the received BU and the Diameter server is expected to return the key material required for the calculation and validation of the Mobile IPv6 MN-HA Authentication Option (and the MIP6-Auth-Mode AVP is set to value MIP6_AUTH_MN_AAA).

6.17. QoS-Capability AVP

TOC

The QoS-Capability AVP is defined in [I-D.ietf-dime-qos-attributes] (Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., and A. Lior, "Traffic Classification and Quality of Service Attributes for Diameter," December 2009.) and contains a list of supported Quality of Service profiles.

6.18. QoS-Resources AVP

TOC

The QoS-Resources AVP is defined in [I-D.ietf-dime-qos-attributes] (Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., and A.

Lior, “Traffic Classification and Quality of Service Attributes for Diameter,” December 2009.) and provides QoS and packet filtering capabilities.

6.19. Chargeable-User-Identity AVP

TOC

The Chargeable-User-Identity AVP (AVP code 89) is of type OctetString and contains an unique temporary handle of the user. The Chargeable-User-Identity is defined in [RFC4372] (Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, “Chargeable User Identity,” January 2006.).

6.20. MIP6-Auth-Mode AVP

TOC

The MIP6-Auth-Mode (AVP Code TBD) is of type Enumerated and contains information of the used Mobile IPv6 Authentication Protocol mode. This specification defines only one value MIP6_AUTH_MN_AAA and the corresponding AAA interactions when MN-AAA security association is used to authenticate the Binding Update as described in [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, “Authentication Protocol for Mobile IPv6,” January 2006.). When the MIP6-Auth_Mode AVP is set to the value of MIP6_AUTH_MN_AAA, the Auth-Request-Type AVP MUST be set to the value of AUTHORIZE_AUTHENTICATE. If the Diameter server does not support the Mobile IPv6 Authentication Protocol usage mode proposed by the HA, then the Diameter server MUST fail the authentication/authorization and MUST set the Result-Code AVP to the value of DIAMETER_ERROR_AUTH_MODE.

6.21. Accounting AVPs

TOC

Diameter Mobile IPv6 applications, either MIP6I or MIP6A, are used in the case of the coupled account model. Diameter Mobile IPv4 application [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, “Diameter Mobile IPv4 Application,” August 2005.) accounting AVPs are reused in this document. The following AVPs SHOULD be included in the accounting request message:

- Accounting-Input-Octets: Number of octets in IP packets received from the mobile node.
- Accounting-Output-Octets: Number of octets in IP packets sent by the mobile node

- Accounting-Input-Packets: Number of IP packets received from the mobile node.
- Accounting-Output-Packets: Number of IP packets sent by the mobile node.
- Acct-Multi-Session-Id: Used to link together multiple related accounting sessions, where each session would have a unique Session-Id, but the same Acct-Multi-Session-Id AVP.
- Acct-Session-Time: Indicates the length of the current session in seconds.
- MIP6-Feature-Vector: The supported features for this mobility service session.
- MIP-Mobile-Node-Address: The Home Address of the mobile node.
- MIP-Agent-Info: The current home agent of the mobile node.
- Chargeable-User-Identity: The unique temporary identity of the user. This AVP MUST be included if it is available in the home agent.
- Service-Selection: Currently selected mobility service.
- QoS-Resources: Assigned QoS resources for the mobile node.
- QoS-Capability: The QoS capability related to the assigned QoS-Resources.
- MIP-Careof-Address: The current Care-of Address of the mobile node.

---

7. Result-Code AVP Values

TOC

This section defines new Result-Code [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.) values that MUST be supported by all Diameter implementations that conform to this specification.

TOC

7.1. Success

Errors that fall within the Success category are used to inform a peer that a request has been successfully completed.

DIAMETER_SUCCESS_RELOCATE_HA (Status Code TBD)
This result code is used by the Diameter server to inform the HA that the MN MUST be switched to another HA.

7.2. Permanent Failures

TOC

Errors that fall within the permanent failures category are used to inform the peer that the request failed and SHOULD NOT be attempted again.

DIAMETER_ERROR_MIP6_AUTH_MODE (Status Code TBD)
This error code is used by the Diameter server to inform the peer that the requested Mobile IPv6 Authentication Protocol usage mode is not supported.

---

8. AVP Occurrence Tables

TOC

The following tables present the AVPs defined in this document and their occurrences in Diameter messages. Note that AVPs that can only be present within a Grouped AVP are not represented in this table.
The table uses the following symbols:

0:
The AVP MUST NOT be present in the message.

0+:
Zero or more instances of the AVP MAY be present in the message.

0-1:
Zero or one instance of the AVP MAY be present in the message.

1:
One instance of the AVP MUST be present in the message.

8.1. DER, DEA, MIR and MIA AVP/Command-Code Table

TOC

AVP Name	Command-Code			
	DER	DEA	MIR	MIA
MIP6-Feature-Vector	0-1	0-1	0-1	0-1
MIP-Mobile-Node-Address	1-2	0-2	1-2	0-2
MIP-MN-AAA-SPI	0	0	0-1	0
MIP-MN-HA-SPI	0	0	0-1	0
MIP6-Agent-Info	1	0-1	1	0-1
MIP-Careof-Address	0	0	0-1	0
MIP-Authenticator	0	0	0-1	0
MIP-MAC-Mobility-Data	0	0	0-1	0
MIP-MSA-Lifetime	0	0	0	1
MIP-MN-HA-MSA	0	0	0	0-1
MIP-Timestamp	0	0	0-1	0-1
User-Name	0-1	0-1	1	0-1
Service-Selection	0-1	0-1	0-1	0-1
QoS-Resources	0+	0+	0+	0+
QoS-Capability	0-1	0	0-1	0
Chargeable-User-Identity	0-1	0-1	0-1	0-1
MIP6-Auth-Mode	0	0	1	0

8.2. Coupled Accounting Model AVP Table

TOC

The table in this section is used to represent which AVPs defined in this document are to be present in the Accounting messages, as defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.).

	Command-Code	
Attribute Name	ACR	ACA
Accounting-Input-Octets	0-1	0-1
Accounting-Input-Packets	0-1	0-1
Accounting-Output-Octets	0-1	0-1
Accounting-Output-Packets	0-1	0-1
Acct-Multi-Session-Id	0-1	0-1
Acct-Session-Time	0-1	0-1
MIP6-Feature-Vector	0-1	0-1
MIP6-Agent-Info	0-1	0-1
MIP-Mobile-Node-Address	0-2	0-2
Event-Timestamp	0-1	0
MIP-Careof-Address	0-1	0
Service-Selection	0-1	0
QoS-Capability	0+	0+
QoS-Resources	0+	0+
Chargeable-User-Identity	0-1	0

---

9. IANA Considerations

TOC

This section contains the namespaces that have either been created in this specification or had their values assigned to existing namespaces managed by IANA.

9.1. Command Codes

TOC

IANA is requested to allocate a command code value for the following new commands from the Command Code namespace defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.). See Section 5 (Command Codes) for the assignment of the namespace in this specification.

Command Code		Value
MIP6-Request	(MIR)	TBD
MIP6-Answer	(MIA)	TBD

9.2. AVP Codes

TOC

This specification requires IANA to register the following new AVPs from the AVP Code namespace defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.).

*MIP-Careof-Address

*MIP-Authenticator

*MIP-MAC-Mobility-Data

*MIP-Timestamp

*MIP-MN-HA-SPI

*MIP-MN-HA-MSA

*Service-Selection

*MIP6-Auth-Mode

The AVPs are defined in Section 6 (AVPs).

9.3. Result-Code AVP Values

TOC

This specification requests IANA to allocate new values to the Result-Code AVP (AVP Code 268) namespace defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," September 2003.). See Section 7 (Result-Code AVP Values) for the assignment of the namespace in this specification.

Result-Code	Value
DIAMETER_SUCCESS_RELOCATE_HA	TBD
DIAMETER_ERROR_MIP6_AUTH_MODE	TBD

9.4. Application Identifier

TOC

This specification requires IANA to allocate two new values "Diameter Mobile IPv6 IKE" and "Diameter Mobile IPv6 Auth" from the Application Identifier namespace defined in [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.).

Application Identifier		Value
Diameter Mobile IPv6 IKE	(MIP6I)	TBD
Diameter Mobile IPv6 Auth	(MIP6A)	TBD

9.5. Namespaces

TOC

IANA is requested to create a new registry "MIP6 Authentication Mode" registry for use with the enumerated MIP6-Auth-Mode AVP. The registry will initially contain the following value:

Token	Value	Description
MIP6_AUTH_MN_AAA	1	RFC TBD

Allocation of new values follow the example policies described in [RFC5226] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.) new values for the MIP6-Auth-Mode AVP will be assigned based on the "Specification Required" policy. The value 0 (zero) is reserved and the maximum value is 4294967295 (i.e. 2^32-1).

---

10. Security Considerations

TOC

The security considerations for the Diameter interaction required to accomplish the split scenario are described in [RFC5026] (Giaretta, G., Kempf, J., and V. Devarapalli, “Mobile IPv6 Bootstrapping in Split Scenario,” October 2007.). Additionally, the security considerations of the Diameter Base protocol [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.), Diameter EAP application [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, “Diameter Extensible Authentication Protocol (EAP) Application,” August 2005.) are applicable to this document.

The Diameter messages may be transported between the HA and the Diameter server via one or more AAA brokers or Diameter agents. In this case the HA to the Diameter server AAA communication rely on the security properties of the intermediating AAA inter-connection networks, AAA brokers and Diameter agents (such as proxies).
In case of the Authentication Protocol for Mobile IPv6 [RFC4285] (Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6," January 2006.), this specification expects that the Diameter server derives the MN-HA Security Association and returns the associated session key (i.e. the MN-HA shared session key) to the HA. However, this specification does not define nor other IETF specification defines how the Diameter server actually derives required keys. The details of the key derivation depends on the deployment where this specification is used and therefore the security properties of the system depend on how this is done.

---

11. Acknowledgements

TOC

The authors would like to thank Jari Arkko, Tolga Asversen, Pasi Eronen, Santiago Zapata Hernandez, Anders Kristensen, Avi Lior, John Loughney, Ahmad Muhanna, Behcet Sarikaya, Basavaraj Patil, Vijay Devarapalli, Lionel Morand, Domagoj Premec, Semyon Mizikovsky and Yoshihiro Ohba for all the useful discussions. Ahmad Muhanna provided a detailed review of the document in August 2007. Pasi Eronen provided detailed comments and text proposals during the IESG review that helped to improved this document greatly.
We would also like to thank our Area Director, Dan Romascanu, for his support.
Hannes Tschofenig would like to thank the European Commission support in the co-funding of the ENABLE project, where this work is partly being developed.
Julien Bournelle would like to thank GET/INT since he began this work while he was under their employ.
Madjid Nakhjiri would like to thank Huawei USA as most of his contributions to this draft were possible while he was under their employ.

---

12. References

TOC

12.1. Normative References

TOC

[I-D.ietf-dime-qos-attributes]	Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., and A. Lior, "Traffic Classification and Quality of Service Attributes for Diameter," draft-ietf-dime-qos-attributes-15 (work in progress), December 2009 (TXT).
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3588]	Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," RFC 3588, September 2003 (TXT).
[RFC3775]	Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004 (TXT).
[RFC4004]	Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," RFC 4004, August 2005 (TXT).
[RFC4005]	Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application," RFC 4005, August 2005 (TXT).
[RFC4072]	Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," RFC 4072, August 2005 (TXT).
[RFC4283]	Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)," RFC 4283, November 2005 (TXT).
[RFC4285]	Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6," RFC 4285, January 2006 (TXT).
[RFC4306]	Kaufman, C., "Internet Key Exchange (IKEv2) Protocol," RFC 4306, December 2005 (TXT).
[RFC4372]	Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity," RFC 4372, January 2006 (TXT).
[RFC4877]	Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," RFC 4877, April 2007 (TXT).
[RFC5026]	Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario," RFC 5026, October 2007 (TXT).
[RFC5142]	Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message," RFC 5142, January 2008 (TXT).
[RFC5149]	Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6," RFC 5149, February 2008 (TXT).

[RFC5447]	Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction," RFC 5447, February 2009 (TXT).

12.2. Informative References

TOC

[I-D.ietf-dime-app-design-guide]	Fajardo, V., Tschofenig, H., and L. Morand, "Diameter Applications Design Guidelines," draft-ietf-dime-app-design-guide-11 (work in progress), March 2010 (TXT).
[I-D.ietf-mext-aaa-ha-goals]	Giaretta, G., Guardini, I., Demaria, E., Bournelle, J., and R. Lopez, "AAA Goals for Mobile IPv6," draft-ietf-mext-aaa-ha-goals-01 (work in progress), May 2008 (TXT).
[I-D.ietf-mext-nemo-v4traversal]	Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers," draft-ietf-mext-nemo-v4traversal-10 (work in progress), April 2009 (TXT).
[RFC4640]	Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)," RFC 4640, September 2006 (TXT).
[RFC5226]	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," BCP 26, RFC 5226, May 2008 (TXT).

Authors' Addresses

TOC

	Jouni Korhonen (editor)
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo FIN-02600
	Finland
Email:	jouni.nospam@gmail.com
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo FIN-02600
	Finland
Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at

	Julien Bournelle
	Orange Labs
	38-4O rue du general Leclerc
	Issy-Les-Moulineaux 92794
	France
Email:	julien.bournelle@orange-ftgroup.com
	Gerardo Giaretta
	Qualcomm
	5775 MoreHouse Dr
	San Diego, CA 92121
	USA
Email:	gerardo.giaretta@gmail.com
	Madjid Nakhjiri
	Motorola
	USA
Email:	madjid.nakhjiri@motorola.com