Diameter Maintenance and
Extensions (DIME)
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2009

J. Korhonen
TeliaSonera
H. Tschofenig
Nokia Siemens Networks
J. Bournelle
Orange Labs
G. Giaretta
Qualcomm
M. Nakhjiri
Motorola

October 27, 2008

Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction
draft-ietf-dime-mip6-split-13.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 30, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

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 (MSP). This document specifies the interaction between a Mobile IP Home Agent and that Diameter server.

Several different mechanisms for authenticating a Mobile Node are supported. The usage of the Internet Key Exchange v2 (IKEv2) protocol allows different mechanisms, such as the Extensible Authentication Protocol (EAP), certificates and pre-shared secrets to be used. Furthermore, another method makes use of 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

Performing the Mobile IPv6 protocol [1], 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 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 [15]. 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 [16] for the bootstrapping problem in the split scenario [2] and also specifies Diameter support for the Authentication Protocol for Mobile IPv6 [3]. The Diameter support defined in this specification also applies to Dual Stack Mobile IPv6 [17].

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: Asserting or helping with assertion of the correctness of the MN 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 of the HA to provide accounting report to the Diameter infrastructure and thus to support the related Diameter accounting procedures.

Session Management: The management of the mobility services may require the AAA to abort 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 depicts the reference architecture for this document.

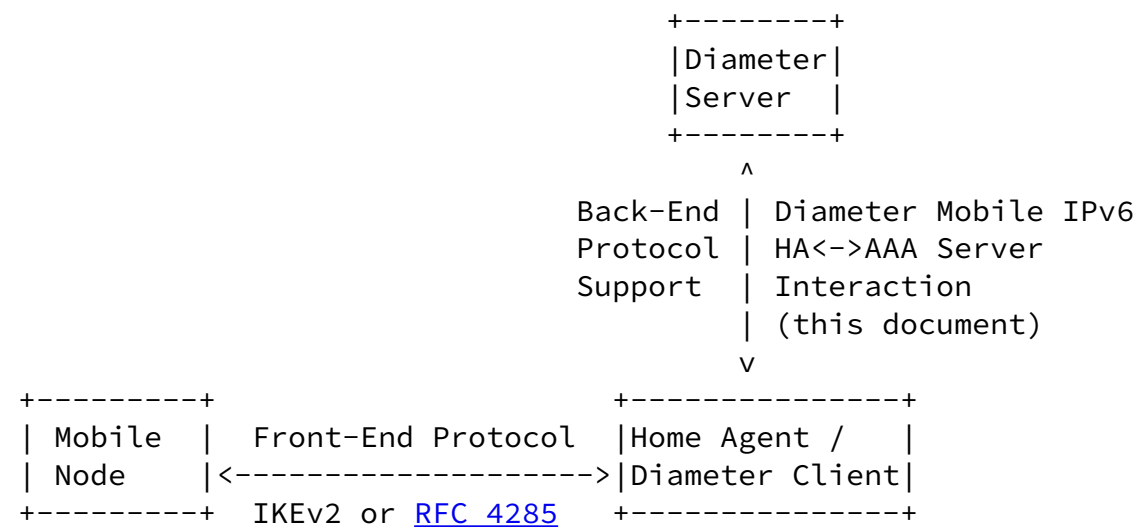

Figure 1: Architecture Overview

Mobile IPv6 signaling between the MN and the HA can be protected using two different mechanisms, namely using IPsec or Authentication Protocol for Mobile IPv6 [3]. For these two approaches several different authentication and key exchange solutions are available. When IPsec is used to protect Mobile IPv6 signaling messages, IKEv2 is used [4]. IKEv2 supports EAP-based initiator authentication, certificates and pre-shared secrets. Alternatively, 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

RFC 3588 [5].

2. Terminology

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 RFC 2119 [6].

The Mobile IPv6 bootstrapping terminology is taken from [15]. Additional terminology is defined below:

Authentication, Authorization, and Accounting (AAA):

AAA protocol based on Diameter [5] with required EAP support [7].

Home AAA (AAAH):

An authentication, authorization and accounting server located in user's home network i.e., in the home realm.

3. Application Identifiers

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 Mobile IPv6 Authentication Protocol.

Mobile IPv6 related accounting generated by the HA uses either MIP6I or MIP6A Application Identifier in the case of coupled accounting model. Diameter Base Accounting Application Identifier (value of 3) is used in the case of split accounting model. Refer Section 4.4 for

more information regarding the accounting models.

4. Protocol Description

4.1. Support for Mobile IPv6 with IKEv2 and EAP

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 [7], 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 RFC 4306 [8]. AVPs specific to Mobile IPv6 bootstrapping are added to the EAP application commands.

Figure 3 shows the message flow involved during the authentication phase when EAP is used.

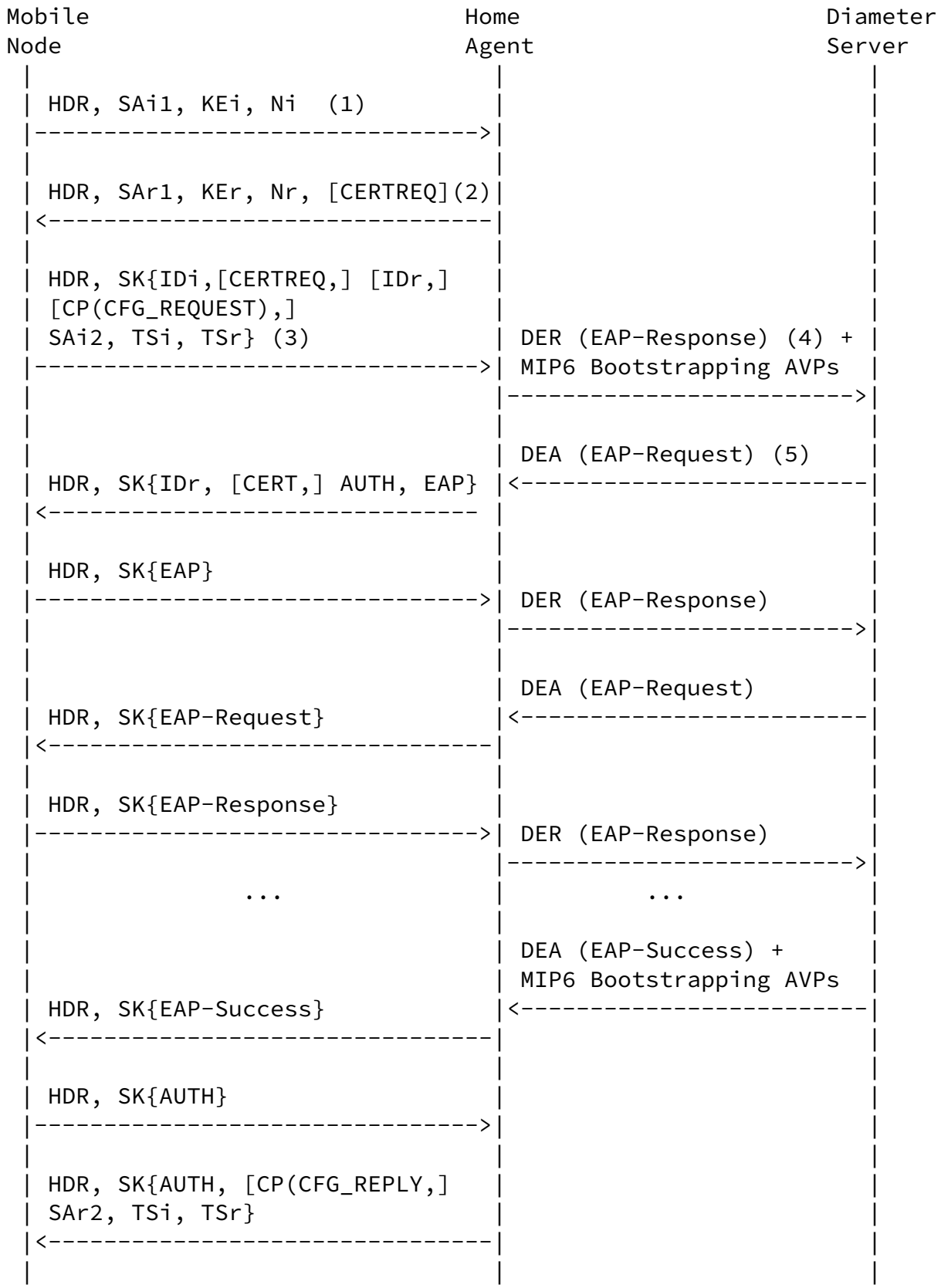

Figure 3: Mobile IPv6 bootstrapping using IKEv2 and EAP

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 [8]).

As part of the authentication process, the MN MAY request a Home-Address, a Home Prefix or suggests one, see [4], 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 acts as a IKEv2 Responder for IPsec VPN access. A problem 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. The MN may provide a hint of the intended service, for example, by using different identities in the IKE_AUTH message for the IPsec VPN service and Mobile IPv6 service. However,

the use of different identities during the IKEv2 negotiation is deployment specific. Another possibility is to make the distinction on the MN subscription basis. In this case the Diameter server can inform the HA during the IKEv2 negotiation whether the MN is provisioned with an IPsec VPN access service or Mobile IPv6 service.

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.

4.2. Support for the Mobile IPv6 Authentication Protocol

Figure 4 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 [3] the MN uses the Mobile Node Identifier Option, specifically the MN-NAI mobility option (as defined in [18]) 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.

In some architectures and network deployments the MN-HA security associations may be established as a result of a successful network access authentication. In such deployments, both MN and Diameter server share the keying material required for computation and validation of the MN-HA Authentication Option, and a Security Parameter Index (SPI) for indexing an appropriate security

association. Upon receiving a BU with a MN-HA Authentication Option, the HA retrieves the keying material required for the computation and validation of the MN-HA Authentication Option from the Diameter server. The Diameter request message sent by the HA must contain enough information (such as SPI, MN-NAI, etc) so that the Diameter server is able to locate the matching MN-HA security association and return correct keying material back to the HA.

This specification assumes that in the case Mobile IPv6 Authentication Protocol is used, the MN-AAA option is included in the BU. Other possible uses of Mobile IPv6 Authentication Protocol are out of scope of this specification and would require a new specification to describe the detailed behavior of the HA-AAAH interface. However, the HA-AAAH interface has been designed in a way that the Mobile IPv6 Authentication Protocol may also be used without the MN-AAA option.

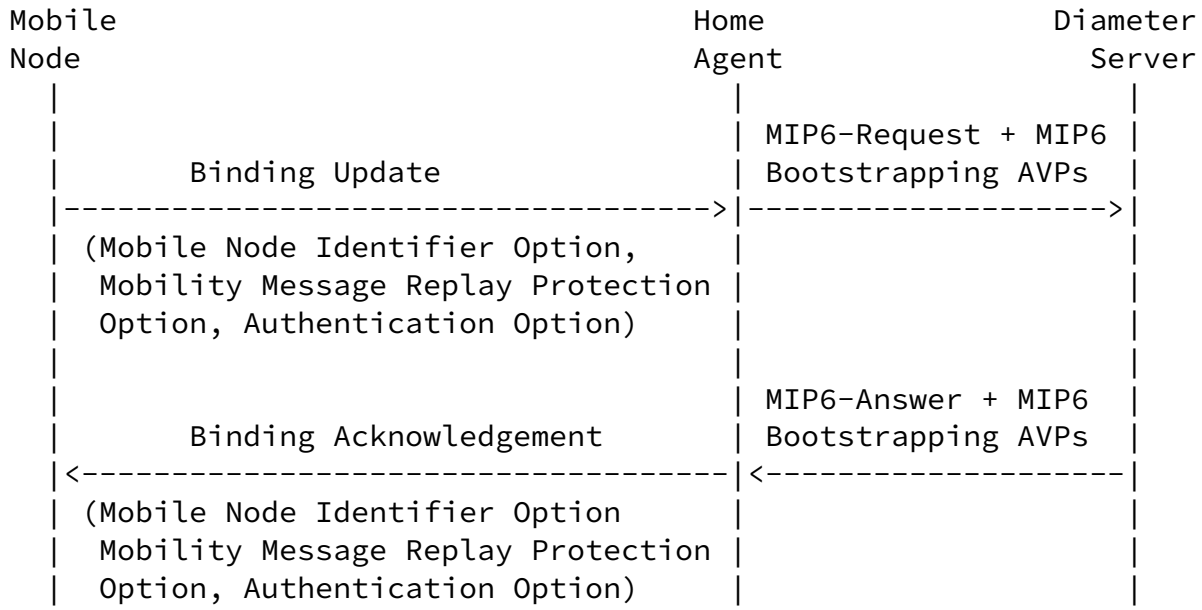

Figure 4: Mobile IPv6 Bootstrapping using the Mobile IPv6 Authentication Protocol

4.3. Mobile IPv6 Session Management

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 [5].

Moreover, the following four commands may be exchanged between the HA and the Diameter server.

4.3.1. Session-Termination-Request

The Session-Termination-Request (STR) message [5] is sent by the HA to inform the Diameter server that an authorized session is being terminated.

4.3.2. Session-Termination-Answer

The Session-Termination-Answer (STA) message [5] is sent by the Diameter server to acknowledge the notification that the session has been terminated.

4.3.3. Abort-Session-Request

The Abort-Session-Request (ASR) message [5] is sent by the Diameter server to terminate the session. This fulfills one of the requirement described in [16].

4.3.4. Abort-Session-Answer

The Abort-Session-Answer (ASA) message [5] is sent by the Home Agent in response to an ASR message.

4.4. Accounting for Mobile IPv6 services

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 [5]. The command codes, exchanged between the HA and Diameter server for accounting purposes, are provided in the following subsections.

The Diameter application design guideline [19] 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 Mobile IPv6 Split or the Mobile IPv6 Auth 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

The Accounting-Request command [5] 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

The Accounting-Answer command [5] is sent by the Diameter server to the HA to acknowledge receiving an Accounting-Request.

5. Command Codes

5.1. Command Code for Mobile IPv6 with IKEv2 and EAP

For the use of Mobile IPv6 with IKEv2 and EAP this document reuses

the Diameter EAP application [7] commands: Diameter-EAP-Request (DER) and Diameter-EAP-Answer (DEA). This specification extends the existing DER and DEA command ABNFs with a number 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.

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 5: Command Codes

5.1.1. Diameter-EAP-Request

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 is set to the value AUTHORIZE_AUTHENTICATE.

5.1.2. Diameter-EAP-Answer

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 ]
                         * [ 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

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

5.2.1. MIP6-Request

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 a replay protection related information, the HA is responsible for the replay protection.

The message format is shown below.

```
<MIP6-Request> ::= < Diameter Header: XXX, 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 he 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

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 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, in addition to the values defined in RFC 3588 [5].

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: XXX, 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 ]
                    [ Origin-State-Id ]
                   * [ Proxy-Info ]
                   * [ Redirect-Host ]
                    [ Redirect-Host-Usage ]
                    [ Redirect-Max-Cache-Time ]
                   * [ Failed-AVP ]
                   * [ AVP ]
```


6. AVPs

To provide support for RFC 4285 [3] and for RFC 4877 [4] the AVPs in the following subsections are needed. RFC 3588, RFC 4004 and RFC 4005 [9] 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	SHLD NOT	MUST NOT	MAY Encr
MIP6-Feature-Vector	TBD	Note 1	Unsigned64	M	P		V	Y
MIP-Mobile-Node-Address	334	RFC4004	Address	M	P		V	Y
MIP6-Agent-Info	TBD	Note 3	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 2	Grouped	M	P		V	Y
QoS-Resources	TBD	Note 2	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 MIP6-Feature-Vector is defined in Section 4.7.4 of [10].

Note 2: The QoS-Capability and QoS-Resource AVPs are defined in Sections 4.1 and 4.3 of [11].

Note 3: The MIP6-Agent-Info is defined in Section 4.5.1 of [10].

				AVP Flag rules				
Attribute Name	AVP Code	Section Defined	Value Type	MUST	MAY	SHLD NOT	MUST NOT	MAY Encr
MIP6-Feature-Vector	TBD	Note 1	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	TBD	Note 3	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	Time	M	P		V	Y
QoS-Capability	TBD	Note 2	Grouped	M	P		M	Y
QoS-Resources	TBD	Note 2	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 MIP6-Feature-Vector is defined in Section 4.7.4 of [10].

Note 2: The QoS-Capability and QoS-Resource AVPs are defined in Sections 4.1 and 4.3 of [11].

Note 3: The MIP6-Agent-Info is defined in Section 4.5.1 of [10].

6.1. User-Name AVP

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

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 [20], if available in the received BU. Future specification may define additional ways to populate the Service-Selection AVP with the required information.

This specification uses the Service-Selection AVP only in the messages sent from the Diameter client to the Diameter Server. However, the AVP is also available to be used in messages sent from the Diameter server to the Diameter client.

6.3. MIP-MN-AAA-SPI AVP

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. 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 MIP6-Auth-Mode AVP is set to value MIP6_AUTH_MN_AAA).

This AVP is re-used from [12].

6.4. MIP-MN-HA-SPI AVP

The MIP-MN-HA-SPI AVP (AVP Code TBD) is of type Unsigned32 and contains an SPI code which can be used with other parameters for identifying the security association required for the validation of the Mobile IPv6 MN-HA Authentication Option.

When included in the MIR message, the Diameter server needs to return a valid MIP-MN-HA-MSA AVP in the corresponding MIA message. Either the MIP-MN-HA-SPI AVP or the MIP-MN-AAA-SPI AVP MUST be present in the MIR message, but not both.

6.5. MIP-Mobile-Node-Address AVP

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 unspecified IPv6 address (0::0) or 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 [12].

6.6. MIP6-Agent-Info AVP

The MIP6-Agent-Info AVP is defined in Section 4.5.1 of [10] 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.

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 [13]). 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

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

6.8. MIP-Authenticator AVP

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. The HA includes this AVP in the MIR message and sets 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).

6.9. MIP-MAC-Mobility-Data AVP

The MIP-MAC-Mobility-Data AVP (AVP Code TBD) is of type OctetString and contains the calculated MAC_Mobility_Data, as defined in [3]. 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).

6.10. MIP-Session-Key AVP

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.

This AVP is re-used from [12].

6.11. MIP-MSA-Lifetime AVP

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) is valid. The associated session key MUST NOT be

used if the lifetime has expired.

This AVP is re-used from [12].

6.12. MIP-MN-HA-MSA AVP

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.

6.13. MIP-Algorithm-Type AVP

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 RFC 4004 that also fulfill current RFC 4285 requirements.

This AVP is re-used from [12].

6.14. MIP-Replay-Mode AVP

The MIP-Replay-Mode AVP (AVP Code 346) is of type Enumerated and contains the replay mode the HA for authenticating the mobile node. The replay modes, defined in RFC 4004 [12], are supported.

This AVP is re-used from [12].

6.15. MIP6-Feature-Vector AVP

The MIP6-Feature-Vector AVP (AVP Code TBD) is of type Unsigned64 and defined in [10]. This document defines a new capability flag bit for signaling the support of Mobile IPv6 split scenario bootstrapping.

MIP6_SPLIT (0x0000000100000000)

When this flag is set by the NAS then it means that the Mobile IPv6 split scenario bootstrapping functionality is supported by the NAS. When this flag is set by the Diameter server then the Mobile IPv6 split scenario bootstrapping is supported by the Diameter server.

6.16. MIP-Timestamp AVP

The MIP-Timestamp AVP (AVP Code TBD) is of type Time and may contain the timestamp value from the Mobility message replay protection option, defined in [3]. 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

The QoS-Capability AVP is defined in [11] and contains a list of supported Quality of Service profiles.

6.18. QoS-Resources AVP

The QoS-Resources AVP is defined in [11] and provides QoS and packet filtering capabilities.

6.19. Chargeable-User-Identity AVP

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 RFC 4372 [14].

6.20. MIP6-Auth-Mode AVP

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. 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 use mode proposed by the HA, then the Diameter server MUST fail the authentication/authorization and set the Result-Code AVP to the value of DIAMETER_ERROR_AUTH_MODE.

6.21. Coupled Accounting Model Accounting AVPs

Diameter Mobile IPv6 application is used in the case of the coupled account model. Diameter Mobile IPv4 application [12] 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

This section defines new Result-Code [5] values that MUST be supported by all Diameter implementations that conform to this specification.

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

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_END_TO_END_MIP6_KEY_ENCRYPTION (Status Code TBD)

This error code is used by the Diameter server to inform the peer that the requested Mobile IPv6 session keys could not be delivered via a security association.

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

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

Command-Code

AVP Name	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	0-1	0
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

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 [5].

	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

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

IANA is requested to allocate a command code values for the following new commands from the Command Code namespace defined in [5]. See Section 5 for the assignment of the namespace in this specification.

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

9.2. AVP Codes

This specification requires IANA to register the following new AVPs from the AVP Code namespace defined in [5].

- 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.

9.3. Result-Code AVP Values

This specification requests IANA to allocate new values to the Result-Code AVP (AVP Code 268) namespace defined in [5]. See Section 7 for the assignment of the namespace in this specification.

Result-Code	Value
DIAMETER_SUCCESS_RELOCATE_HA	TBD
DIAMETER_ERROR_END_TO_END_MIP6_KEY_ENCRYPTION	TBD
DIAMETER_ERROR_MIP6_AUTH_MODE	TBD

9.4. Application Identifier

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 [5].

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

9.5. Namespaces

This specification defines new values to the "Mobility Capability" registry (see [10]) for use with the MIP6-Feature-Vector AVP:

Token	Value	Description
MIP6_SPLIT	0x0000000100000000	RFC TBD

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 values:

Token	Value	Description
MIP6_AUTH_MN_AAA	1	RFC TBD

Allocation of new values follow the example policies described in [21] new values for the MIP6-Auth-Mode AVP will be assigned based on the "Specification Required" policy.

10. Security Considerations

The security considerations for the Diameter interaction required to accomplish the split scenario are described in in [2]. Additionally, the security considerations of the Diameter Base protocol [5], Diameter EAP application [7] 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 intermediate AAA brokers and Diameter agents (such as proxies).

11. Acknowledgements

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.

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

12.1. Normative References

[1] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[2] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[3] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-rfc4285bis-03 (work in progress), July 2008.

[4] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[5] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[7] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[8] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[9] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[10] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", draft-ietf-dime-mip6-integrated-10 (work in progress),

September 2008.

[11] Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., and A. Lior, "Quality of Service Attributes for Diameter", draft-ietf-dime-qos-attributes-07 (work in progress), June 2008.

[12] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, August 2005.

[13] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility

Header Home Agent Switch Message", RFC 5142, January 2008.

[14] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

12.2. Informative References

[15] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[16] 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.

[17] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", draft-ietf-mext-nemo-v4traversal-05 (work in progress), July 2008.

[18] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[19] Fajardo, V., Asveren, T., Tschofenig, H., McGregor, G., and J. Loughney, "Diameter Applications Design Guidelines", draft-ietf-dime-app-design-guide-07 (work in progress), July 2008.

[20] Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6", RFC 5149, February 2008.

[21] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

Jouni Korhonen
TeliaSonera
P.O.Box 970
Sonera FIN-00051
Finland

Email: jouni.nospam@gmail.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Julien Bournelle
Orange Labs
38-40 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

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).