Internet Engineering Task Force (IETF)
Request for Comments: 5778
Category: Standards Track
ISSN: 2070-1721

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

February 2010

Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction

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.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5778.

Table of Contents

1. Introduction

Performing the Mobile IPv6 protocol [RFC3775] requires the mobile node (MN) to own a home address 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 (SAs) 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 an 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]. 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 [RFC5637] for the bootstrapping problem in the split scenario [RFC5026] and also specifies Diameter support for the Authentication Protocol for Mobile IPv6 [RFC4285]. The Diameter support defined in this specification also applies to Dual Stack Mobile IPv6 [RFC5555].

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 does the MSP allow 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: The MN's identity needs to be verified. 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 sets 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 supports 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 depicts the reference architecture for this document.

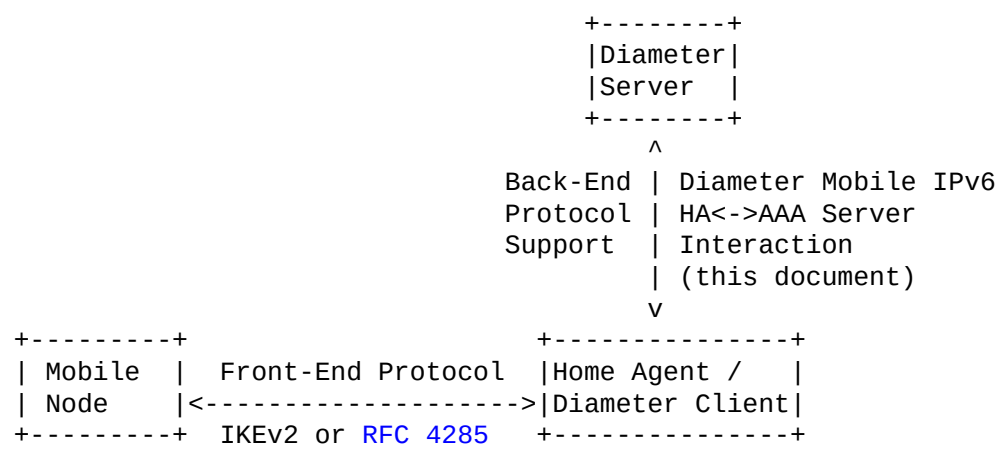

Figure 1: Architecture Overview

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]. 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] for the setup of the IPsec SAs. IKEv2 supports EAP-based (Extensible Authentication Protocol) 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].

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 [RFC2119].

The Mobile IPv6 bootstrapping terminology is taken from [RFC4640]. Additional terminology is defined below:

Authentication, Authorization, and Accounting (AAA):

> AAA protocol based on Diameter [RFC3588] with required EAP support [RFC4072].

Home AAA (AAAH):

> An authentication, authorization, and accounting server located in the 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)  7
Diameter Mobile IPv6 Auth  (MIP6A)  8
```

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 the coupled accounting model. The Diameter Base Accounting Application Identifier (value of 3) is used in the case of the split accounting model. Refer to 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 [RFC4072], 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]. Attribute-value pairs (AVPs) specific to Mobile IPv6 bootstrapping are added to the EAP application commands.

Figure 2 shows the message flow involved during the authentication phase when EAP is used. The communication between the mobile node and the home agent uses the conventions defined in [RFC4306]. Similarly, the communication between the home agent and the Diameter server uses the conventions defined in [RFC4072].

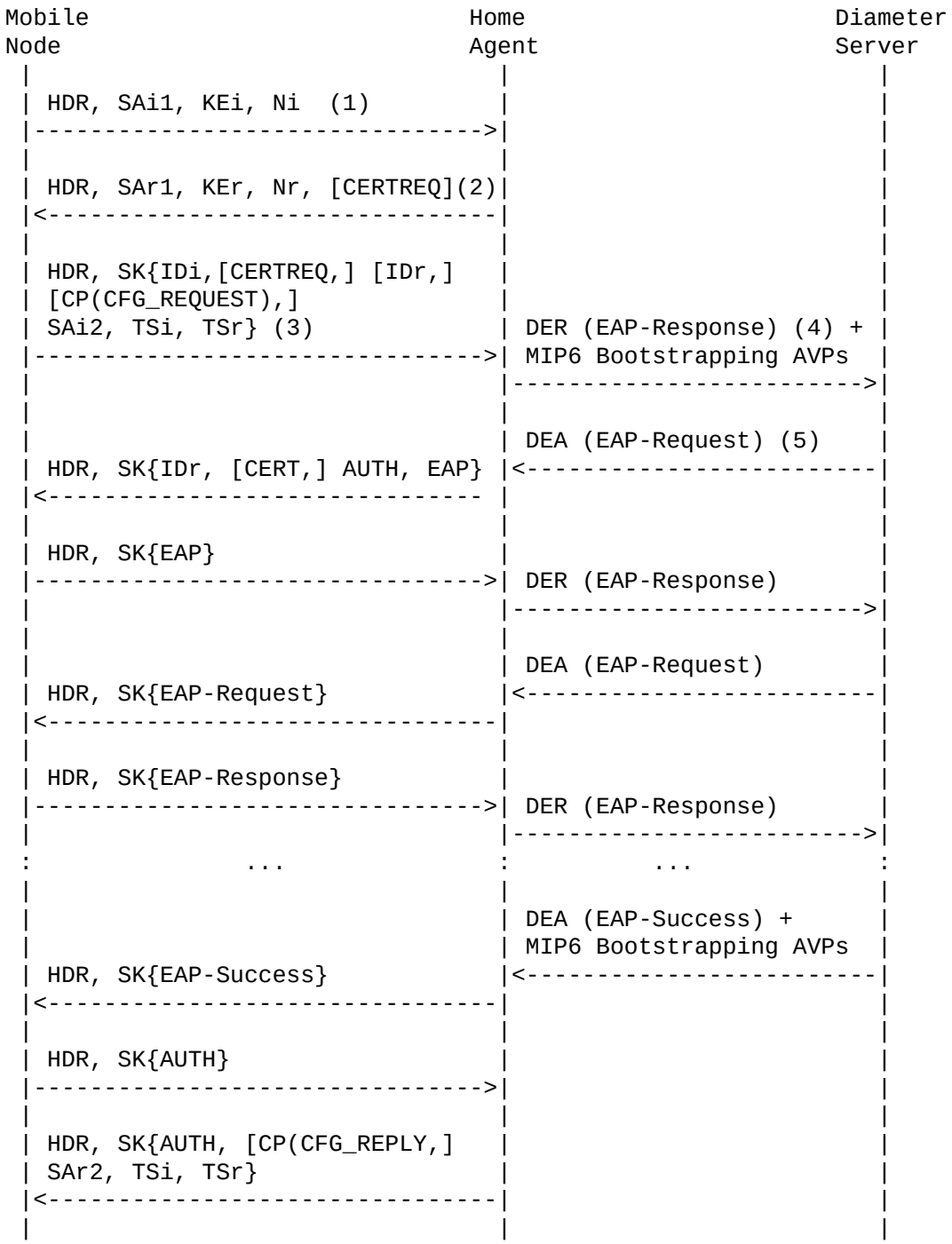

Figure 2: Mobile IPv6 Bootstrapping Using IKEv2 and EAP

The MN and the HA start the interaction with an IKE_SA_INIT exchange.

In this phase, cryptographic algorithms are negotiated, and 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]).

As part of the authentication process, the MN MAY request a home address or a home prefix or suggest one (see [RFC4877]), 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 set up 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 an 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.

4.2. Support for the Mobile IPv6 Authentication Protocol

Figure 3 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], the MN uses the Mobile Node Identifier Option, specifically the MN-NAI mobility option (as defined in [RFC4283]) 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 where Mobile IPv6 Authentication Protocol is used, the MN-AAA option is included in the BU as defined in [RFC4285] 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 the 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.

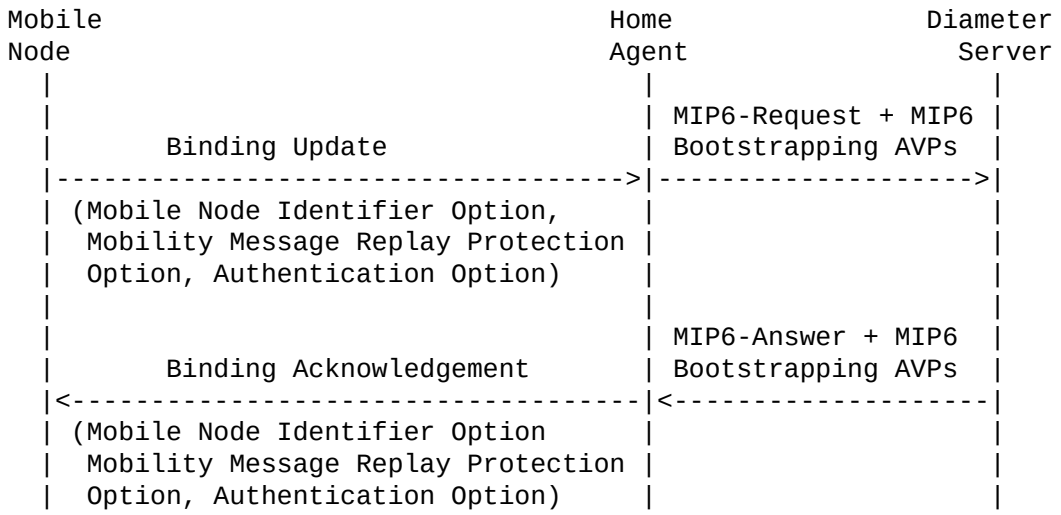

Figure 3: Mobile IPv6 Bootstrapping Using the Mobile IPv6 Authentication Protocol

4.3. Mobile IPv6 Session Management

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].

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 corresponds to one Diameter session. In the IKEv2 case, we specifically mean the created IKE SA.

4.3.1. Session-Termination-Request

The Session-Termination-Request (STR) message [RFC3588] 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

The Session-Termination-Answer (STA) message [RFC3588] 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 [RFC3588] is sent by the Diameter server to the HA to terminate the authorized session. This fulfills one of the requirement described in [RFC5637]. 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

The Abort-Session-Answer (ASA) message [RFC3588] 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 [RFC3588]. The command codes, exchanged between the HA and Diameter server for accounting purposes, are provided in the following subsections.

The Diameter application design guideline [DIME-APP] 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 the 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

The Accounting-Request command [RFC3588] 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 [RFC3588] is sent by the Diameter server to the HA to acknowledge 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 [RFC4072] 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].

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

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 7). The grouped AVP has the following modified ABNF (as defined in [RFC3588]):

```
<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

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 (DER) message. The Application-Id field in the Diameter message header MUST be set to the Diameter Mobile IPv6 IKE Application-Id (value of 7). 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

This section defines the commands that are used for support with the Mobile IPv6 Authentication Protocol.

There are multiple ways of deploying and utilizing the 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	325	5.3.1	Diameter Mobile IPv6 Auth
MIP6-Answer	MIA	325	5.3.2	Diameter Mobile IPv6 Auth

Command Codes

5.2.1. MIP6-Request

The MIP6-Request (MIR), indicated by the Command-Code field set to 325 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 an 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: 325, 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

The MIP6-Answer (MIA) message, indicated by the Command-Code field set to 325 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, in addition to the values defined in [RFC3588].

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: 325, 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

To provide support for [RFC4285] and for [RFC4877], the AVPs in the following subsections are needed. [RFC3588], [RFC4004], and [RFC4005] 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	RFC 5447	Unsigned64	M	P		V	Y
MIP-Mobile-Node-Address	333	RFC 4004	Address	M	P		V	Y
MIP6-Agent-Info	486	RFC 5447	Grouped	M	P		V	Y
User-Name	1	RFC 3588	UTF8String	M	P		V	Y
Service-Selection	493	6.2	UTF8String	M	P		V	Y
QoS-Capability	578	Note 1	Grouped	M	P		V	Y
QoS-Resources	508	Note 1	Grouped	M	P		V	Y
MIP-MN-HA-MSA	492	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 [RFC5777].

Attribute Name	AVP Code	Section Defined	Value Type	AVP Flag Rules: MUST	MAY	SHOULD NOT	MUST NOT	MAY Encr
MIP6-Feature-Vector	124	RFC 5447	Unsigned64	M	P		V	Y
User-Name	1	RFC 3588	UTF8String	M	P		V	Y
Service-Selection	493	6.2	UTF8String	M	P		V	Y

MIP-MN-AAA-SPI	341	RFC 4004	Unsigned32	M	P		V	Y
MIP-MN-HA-SPI	491	6.4	Unsigned32	M	P		V	Y
MIP-Mobile-Node-Address	333	RFC 4004	Address	M	P		V	Y
MIP6-Agent-Info	486	RFC 5447	Grouped	M	P		V	Y
MIP-Careof-Address	487	6.7	Address	M	P		V	Y
MIP-Authenticator	488	6.8	OctetString	M	P		V	Y
MIP-MAC-Mobility-Data	489	6.9	OctetString	M	P		V	Y
MIP-Session-Key	343	6.10	OctetString	M	P		V	Y
MIP-MSA-Lifetime	367	RFC 4004	Unsigned32	M	P		V	Y
MIP-MN-HA-MSA	492	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	490	6.16	OctetString	M	P		V	Y
QoS-Capability	578	Note 1	Grouped	M	P		V	Y
QoS-Resources	508	Note 1	Grouped	M	P		V	Y
Chargeable-User-Identity	89	6.19	OctetString	M	P		V	Y
MIP6-Auth-Mode	494	6.20	Enumerated	M	P		V	Y
Rest of the AVPs in the MIR & MIA excluding *[AVP]		RFC 3588 RFC 4005		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 [RFC5777].

6.1. User-Name AVP

The User-Name AVP (AVP Code 1) is of type UTF8String and contains a Network Access Identifier (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 493) is of type UTF8String and contains the name of the service or the external network with which the mobility service should be associated. In the scope of this specification, the value can be 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], if available in the received BU. Future specifications 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

The MIP-MN-AAA-SPI AVP (AVP Code 341) is of type Unsigned32 and contains a Security Parameter Index (SPI) code extracted from the Mobility Message Authentication Option included in the received BU message. This AVP is reused from [RFC4004].

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

The MIP-MN-HA-SPI AVP (AVP Code 491) 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

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 reused from [RFC4004].

6.6. MIP6-Agent-Info AVP

The MIP6-Agent-Info AVP (AVP Code 486) is defined in Section 4.2.1 of [RFC5447] 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 an HA switch procedure towards the MN (e.g., using the procedure defined in [RFC5142]). 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 487) 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

The MIP-Authenticator AVP (AVP Code 488) 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

The MIP-MAC-Mobility-Data AVP (AVP Code 489) is of type OctetString and contains the MAC_Mobility_Data calculated by the HA as defined in [RFC4285] 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

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 MN-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 defined in a respective deployment-specific system specification.

This AVP is reused from [RFC4004].

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 reused from [RFC4004].

6.12. MIP-MN-HA-MSA AVP

The MIP-MN-HA-MSA AVP (AVP Code 492) is of type Grouped and contains the session-related information for use with the Mobile IPv6 Authentication Protocol.

```
MIP-MN-HA-MSA ::= < AVP Header: 492 >
                  { 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

The MIP-Algorithm-Type AVP (AVP Code 345) is of type Enumerated and contains the 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] that also fulfill current RFC 4285 requirements. This AVP is reused from [RFC4004].

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

The MIP-Replay-Mode AVP (AVP Code 346) is of type Enumerated and contains the replay mode of the HA for authenticating the mobile node. Out of all possible replay modes defined in [RFC4004], the following are supported by this specification:

```
1   None
2   Timestamp
```

This AVP is reused from [RFC4004].

6.15. MIP6-Feature-Vector AVP

The MIP6-Feature-Vector AVP (AVP Code 124) is defined in [RFC5447]. However, this specification does not define any Mobile IPv6 split scenario bootstrapping specific capability flag.

6.16. MIP-Timestamp AVP

The MIP-Timestamp AVP (AVP Code 490) is of type OctetString and contains an 8-octet timestamp value (i.e., 64-bit timestamp) from the Mobility message replay protection option, defined in [RFC4285]. 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 [RFC5777] and contains a list of supported Quality of Service profiles.

6.18. QoS-Resources AVP

The QoS-Resources AVP is defined in [RFC5777] 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 a unique temporary handle of the user. The Chargeable-User-Identity is defined in [RFC4372].

6.20. MIP6-Auth-Mode AVP

The MIP6-Auth-Mode (AVP Code 494) 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]. 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

Diameter Mobile IPv6 applications, either MIP6I or MIP6A, are used in the case of the coupled account model. Diameter Mobile IPv4 application [RFC4004] 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 Quality-of-Service (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 [RFC3588] 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 2009)

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_MIP6_AUTH_MODE (Status Code 5041)

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 tables use 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	0-1	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

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].

Attribute Name	Command-Code ACR	Command-Code 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 has allocated a command code value for the following new command from the Command Code namespace defined in [RFC3588]. See Section 5 for the assignment of the namespace in this specification.

Command Code	Value
MIP6-Request/Answer (MIR/MIA)	325

9.2. AVP Codes

IANA has registered the following new AVPs from the AVP Code namespace defined in [RFC3588].

- 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

IANA has allocated new values to the Result-Code AVP (AVP Code 268) namespace defined in [RFC3588]. See Section 7 for the assignment of the namespace in this specification.

Result-Code	Value
DIAMETER_SUCCESS_RELOCATE_HA	2009
DIAMETER_ERROR_MIP6_AUTH_MODE	5041

9.4. Application Identifier

IANA has allocated two new values "Diameter Mobile IPv6 IKE" and "Diameter Mobile IPv6 Auth" from the Application Identifier namespace defined in [RFC3588].

Application Identifier	Value
Diameter Mobile IPv6 IKE (MIP6I)	7
Diameter Mobile IPv6 Auth (MIP6A)	8

9.5. Namespaces

IANA has created a new registry, "MIP6 Authentication Mode Registry", for use with the enumerated MIP6-Auth-Mode AVP. The registry initially contains the following value:

Token	Value	Description
MIP6_AUTH_MN_AAA	1	RFC 5778

Allocation of new values follow the example policies described in [RFC5226]. 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

The security considerations for the Diameter interaction required to accomplish the split scenario are described in [RFC5026]. Additionally, the security considerations of the Diameter base protocol [RFC3588], and Diameter EAP application [RFC4072] 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 relies on the security properties of the intermediating AAA inter-connection networks, AAA brokers, and Diameter agents (such as proxies).

In the case of the Authentication Protocol for Mobile IPv6 [RFC4285], 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 do other IETF specifications define 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

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 document were possible while he was under their employ.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4004] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, August 2005.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4372] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5142] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.

[RFC5149] Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6", RFC 5149, February 2008.

[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.

[RFC5777] Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., Ed., and A. Lior, "Traffic Classification and Quality of Service (QoS) Attributes for Diameter", RFC 5777, February 2010.

12.2. Informative References

[DIME-APP] Fajardo, V., Asveren, T., Tschofenig, H., McGregor, G., and J. Loughney, "Diameter Applications Design Guidelines", Work in Progress, July 2009.

[RFC4640] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[RFC5637] Giaretta, G., Guardini, I., Demaria, E., Bournelle, J., and R. Lopez, "Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6", RFC 5637, September 2009.

Authors' Addresses

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