

**Diameter MIPv6 Application for the Integrated Scenario**  
**draft-tschofenig-dime-mip6-integrated-00.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 August 31, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

A Mobile IPv6 node requires a home agent address, a home address, and IPsec security association with its home agent before it can start utilizing Mobile IPv6 service. [RFC 3775](#) requires that some or all of these parameters are statically configured. Ongoing work aims to make this information dynamically available to the mobile node. An important aspect of the Mobile IPv6 bootstrapping solution is to support interworking with existing authentication, authorization and accounting infrastructure. This document defines a Diameter

application to facilitate Mobile IPv6 bootstrapping for the integrated scenario.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Terminology and Abbreviations . . . . .</a>	<a href="#">4</a>
<a href="#">3.</a>	<a href="#">Overview . . . . .</a>	<a href="#">5</a>
<a href="#">4.</a>	<a href="#">Command Codes and AVPs . . . . .</a>	<a href="#">7</a>
<a href="#">4.1.</a>	<a href="#">Command Codes . . . . .</a>	<a href="#">7</a>
<a href="#">4.2.</a>	<a href="#">Advertising Application Support . . . . .</a>	<a href="#">7</a>
<a href="#">4.3.</a>	<a href="#">MIPv6-Bootstrapping-Request (MBR) . . . . .</a>	<a href="#">8</a>
<a href="#">4.4.</a>	<a href="#">MIPv6-Bootstrapping-Answer (MBA) . . . . .</a>	<a href="#">8</a>
<a href="#">4.5.</a>	<a href="#">MIPv6-Home-Agent-Request (MHR) . . . . .</a>	<a href="#">9</a>
<a href="#">4.6.</a>	<a href="#">MIPv6-Home-Agent-Answer (MHA) . . . . .</a>	<a href="#">9</a>
<a href="#">4.7.</a>	<a href="#">AVPs . . . . .</a>	<a href="#">10</a>
<a href="#">4.7.1.</a>	<a href="#">Home Agent Address AVP . . . . .</a>	<a href="#">10</a>
<a href="#">4.7.2.</a>	<a href="#">Home Agent FQDN AVP . . . . .</a>	<a href="#">10</a>
<a href="#">4.7.3.</a>	<a href="#">Home Link Prefix AVP . . . . .</a>	<a href="#">10</a>
<a href="#">4.7.4.</a>	<a href="#">Home Address AVP . . . . .</a>	<a href="#">10</a>
<a href="#">4.7.5.</a>	<a href="#">DNS Update Mobility Option Attribute . . . . .</a>	<a href="#">10</a>
<a href="#">4.7.6.</a>	<a href="#">MIPv6 Bootstrapping Feature Attribute . . . . .</a>	<a href="#">11</a>
<a href="#">4.7.7.</a>	<a href="#">MIPv6 Security Association Parameters . . . . .</a>	<a href="#">11</a>
<a href="#">5.</a>	<a href="#">Example Exchanges . . . . .</a>	<a href="#">12</a>
<a href="#">6.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">13</a>
<a href="#">7.</a>	<a href="#">Acknowledgements . . . . .</a>	<a href="#">14</a>
<a href="#">8.</a>	<a href="#">Contributors . . . . .</a>	<a href="#">15</a>
<a href="#">9.</a>	<a href="#">Open Issues . . . . .</a>	<a href="#">16</a>
<a href="#">10.</a>	<a href="#">References . . . . .</a>	<a href="#">17</a>
<a href="#">10.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">17</a>
<a href="#">10.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">17</a>
	<a href="#">Author's Address . . . . .</a>	<a href="#">19</a>
	<a href="#">Intellectual Property and Copyright Statements . . . . .</a>	<a href="#">20</a>



## **1. Introduction**

Mobile IPv6 specification [[1](#)] requires a Mobile Node (MN) to perform registration with a Home Agent with information about its current point of attachment (Care-of Address). The Home Agent creates and maintains binding between the MN's Home Address and the MN's Care-of Address.

In order to register with a Home Agent, the MN needs to know some information such as, the Home Link prefix, the Home Agent Address, the Home Address, the Home Link prefix Length and security related information in order to later secure the Binding Update.

The aforementioned set of information may be statically provisioned in the MN. However, static provisioning of this information has its drawbacks. It increases provisioning and network maintenance burden for the operator. Moreover, static provisioning does not allow load balancing, failover, opportunistic home link assignment etc. For example, the user may be accessing the network from a location that may be geographically far away from the preconfigured home link; the administrative burden to configure the MN's with the respective addresses is large and the ability to react on environmental changes is minimal. In these situations static provisioning may not be desirable.

Dynamic assignment of Mobile IPv6 home registration information is a desirable feature for ease of deployment and network maintenance. For this purpose, the Diameter infrastructure, which is used for access authentication, can be leveraged to assign some or all of the necessary parameters. The Diameter server in the Access Service Provider (ASP) or in the Mobility Service Provider's (MSP) network may return these parameters to the AAA client. The AAA client might either be the NAS, in case of the integrated scenario, or the home agent, in case of the split scenario. The terms integrated and split are described in the terminology section and were introduced in [[2](#)].



## **2. Terminology and Abbreviations**

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [3].

General mobility terminology can be found in [4]. The following additional terms, as defined in [2], are used in this document:

Access Service Authorizer (ASA):

A network operator that authenticates a mobile node and establishes the mobile node's authorization to receive Internet service.

Access Service Provider (ASP):

A network operator that provides direct IP packet forwarding to and from the mobile node.

Mobility Service Authorizer (MSA):

A service provider that authorizes Mobile IPv6 service.

Mobility Service Provider (MSP):

A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile node must be authenticated and authorized to obtain the Mobile IPv6 service.

Split scenario:

A scenario where the mobility service and the network access service are authorized by different entities.

Integrated Scenario:

A scenario where the mobility service and the network access service are authorized by the same entity.



In the typical Mobile IPv6 access scenario as shown above, the MN attaches in a Access Service Provider's network. During this network attachment procedure, the NAS/Diameter client interacts with the mobile node. As shown in Figure 1, the authentication and authorization happens via a Diameter infrastructure.





At the time of authorizing the user for IPv6 access, the Diameter server in the MSA detects that the user is authorized for Mobile IPv6 access. Based on the MSA's policy, the Diameter server may allocate several parameters to the MN for use during the subsequent Mobile IPv6 protocol interaction with the home agent.

Depending on the details of the solution interaction with the DHCPv6 server may be required, as described in [\[5\]](#).

#### **4. Command Codes and AVPs**

This section defines command codes and AVPs for usage of Diameter for bootstrapping MIPv6 in the split scenario.

##### **4.1. Command Codes**

This document introduces four new command codes:

- o MIPv6-Bootstrapping-Request (MBR) (Code TBD)
- o MIPv6-Bootstrapping-Answer (MBA) (Code TBD)
- o MIPv6-Home-Agent-Request (MHR) (Code TBD)
- o MIPv6-Home-Agent-Answer (MHA) (Code TBD)

In addition, the following Diameter Base protocol messages are used with this application:

Command-Name	Abbrev.	Code	Reference
Accounting-Request	ACR	271	<a href="#">RFC 3588</a>
Accounting-Request	ACR	271	<a href="#">RFC 3588</a>
Accounting-Answer	ACA	271	<a href="#">RFC 3588</a>
Re-Auth-Request	RAR	258	<a href="#">RFC 3588</a>
Re-Auth-Answer	RAA	258	<a href="#">RFC 3588</a>
Abort-Session-Request	ASR	274	<a href="#">RFC 3588</a>
Abort-Session-Answer	ASA	274	<a href="#">RFC 3588</a>
Session-Term-Request	STR	275	<a href="#">RFC 3588</a>
Session-Term-Answer	STA	275	<a href="#">RFC 3588</a>

##### **4.2. Advertising Application Support**

Diameter nodes conforming to this specification MAY advertise support by including the value of (TBD) in the Auth-Application-Id or the Acct-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command [[6](#)].

The value of TBD MUST be used as the Application-Id in all MBR/MBA and MHR/MHA commands.

The value of zero (0) SHOULD be used as the Application-Id in all STR/STA, ACR/ACA, ASR/ASA, and RAR/RAA commands, because these commands are defined in the Diameter base protocol and no additional mandatory AVPs for those commands are defined in this document.



#### **4.3. MIPv6-Bootstrapping-Request (MBR)**

The MIPv6-Bootstrapping-Request message (MBR) indicated by the Command- Code field (see Section 3 of [6]) set to TBD and 'R' bit set in the Command Flags field is used by Diameter clients to request home agent assignment, to authorize for mobility service usage and optionally to indicate the support of local home agent assignment.

The MBR message MAY carry the DNS Update Mobility Option and the MIPv6 Bootstrapping Feature attribute.

The message format, presented in ABNF form [7], is defined as follows:

```
<MIPv6-Bootstrapping-Request> ::= < Diameter Header: XXX, REQ, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    [ Destination-Host ]
    [ User-Name ]
    [ DNS Update Mobility Option ]
    [ MIPv6 Bootstrapping Feature ]
    * [ AVP ]
```

#### **4.4. MIPv6-Bootstrapping-Answer (MBA)**

The MIPv6-Bootstrapping-Answer (MBA) message, indicated by the Command- Code field set to TBD and 'R' bit cleared in the Command Flags field is sent in response to the MIPv6-Bootstrapping-Request message (MBR). If the mobility service is successfully authorized and the Diameter server was able to fulfill the bootstrapping request (if needed) then the response MAY include the DNS Update Mobility Option, Home Address, Home Link Prefix, Home Agent FQDN and the Home Agent Address AVP.

The message format is defined as follows:



```
<MIPv6-Bootstrapping-Answer> ::= < Diameter Header: XXX, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [ DNS Update Mobility Option ]
    [ Home Address ]
    [ Home Link Prefix ]
    [ Home Agent FQDN ]
    [ Home Agent Address ]
    * [ AVP ]
```

#### **4.5. MIPv6-Home-Agent-Request (MHR)**

The MIPv6-Home-Agent-Request (MHR) message, indicated by the Command-Code field set to TDB and 'R' bit set in the Command Flags field is used by Diameter entity (acting as a Diameter client) to interact with the home agent. (acting as a Diameter server).

The message MUST carry the MIPv6 Security Association Parameters. Additionally, the Diameter client might provide the Home Address and the Home Link Prefix to the Diameter server.

The message format is defined as follows:

```
<MIPv6-Home-Agent-Request> ::= < Diameter Header: XXX, REQ, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    [ Destination-Host ]
    [ Home Address ]
    [ Home Link Prefix ]
    [ MIPv6 Security Association ]
    * [ AVP ]
```

#### **4.6. MIPv6-Home-Agent-Answer (MHA)**

The MIPv6-Home-Agent-Answer (MHA) message, indicated by the Command-Code field set to TBD and 'R' bit cleared in the Command Flags field is sent in response to the MIPv6-Home-Agent-Request (MHR) message for confirmation of the result of MIPv6 HA bootstrapping. This message MAY contain the Home Link Prefix and the Home Address.





The message format is defined as follows:

```
<MIPv6-Home-Agent-Answer (MHA)> ::= < Diameter Header: XXX, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Result-Code }
    [ Home Address ]
    [ Home Link Prefix ]
    * [ AVP ]
```

#### **4.7. AVPs**

##### **4.7.1. Home Agent Address AVP**

The Diameter server MAY decide to assign a Home Agent to the MN that is in close proximity to the point of attachment (e.g., determined by the NAS-ID). There may be other reasons for dynamically assigning Home Agents to the MN, for example to share the traffic load. The AVP also contains the prefix length so that the MN can easily infer the Home Link prefix from the Home Agent address.

##### **4.7.2. Home Agent FQDN AVP**

The Diameter server MAY assign an FQDN of the home address to the MN. The mobile node can perform DNS query with the FQDN to derive the home agent address.

##### **4.7.3. Home Link Prefix AVP**

For the same reason as the HA assignment, the Diameter server MAY assign a Home Link that is in close proximity to the point of attachment (NAS-ID). The MN can perform [\[1\]](#) specific procedures to discover other information for Mobile IPv6 registration.

##### **4.7.4. Home Address AVP**

The Diameter server MAY assign a Home Address to the MN. This allows the network operator to support mobile devices that are not configured with static addresses. The attribute also contains the prefix length so that the MN can easily infer the Home Link prefix from the Home Agent address.

##### **4.7.5. DNS Update Mobility Option Attribute**

By using this payload the Diameter client instructs the Diameter



server to perform a dynamic DNS update. When this payload is included in the reverse direction, i.e., from the Diameter server to the Diameter client, it informs about the status of the dynamic DNS update. When the payload is sent from the Diameter client to the Diameter server then the response MUST include the DNS Update Mobility Option AVP.

#### **4.7.6. MIPv6 Bootstrapping Feature Attribute**

By using this payload the Diameter client indicates to the Diameter server certain capabilities and features. For example, the Diameter client might want to indicate that local Home Agent assignment can be provided.

Local-Home-Agent-Assignment:

This flag is set to 1 when the Diameter client knows that a local home agent can be provided for the mobile node. Whether a local home agent can be provided depends on the functionality offered by the visited network and configured to the Diameter client.

#### **4.7.7. MIPv6 Security Association Parameters**

This payload is used by the Diameter entity to provision keying material in a push fashion to the home agent. This AVP includes keying material, lifetime and key name information. Security parameter bootstrapping can be provided for IKEv2 [8], IKEv1 or for the MIPv6-AUTH protocol.

[Editor's Note: A future version of this document will provide detailed AVP formats.]



## 5. Example Exchanges

The following section shows a basic message flow with dynamic Home Agent assignment in the user's home network. The MBR / MBA message exchange illustrates the communication between the Diameter client and the Diameter server to initiate the bootstrapping procedure. The interaction between the Home Diameter server and the Home Agent (for HA bootstrapping in the home network) is depicted with the MHR / MHA exchange.

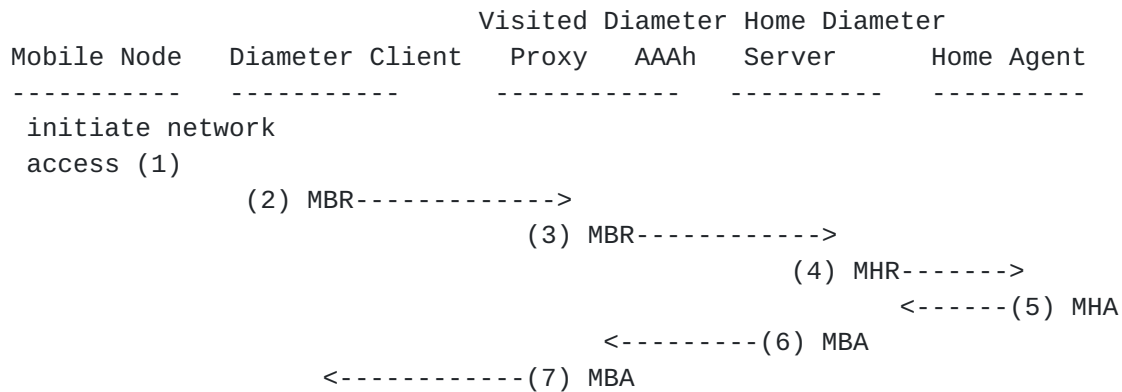


Figure 7: Basic Bootstrapping Scenario

[Editor's Note: A future version of this document will provide additional examples.]



## **6. Security Considerations**

The security considerations for the Diameter interaction required to accomplish the integrated scenario are described in [5] . Additionally, the security considerations of the Diameter base protocol [6], Diameter NASREQ [11] / Diameter EAP [12] (with respect to network access authentication and the transport of keying material) are applicable to this document.

## **7. Acknowledgements**

This document is heavily based on the ongoing work for RADIUS MIPv6 interaction. Hence, credits go to Kuntal Chowdhury and Avi Lior for their work with [draft-chowdhury-mip6-radius-00.txt](#). Furthermore, the author would like to thank the authors of [draft-le-aaa-diameter-mobileipv6-04.txt](#) (Franck Le, Basavaraj Patil, Charles E. Perkins, Stefano Faccin) for their work in context of MIPv6 Diameter interworking. Their work influenced this document.

Parts of this document are a byproduct of the ENABLE Project, partially funded by the European Commission under its Sixth Framework Programme. It is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ENABLE Project or the European Commission.





## **8. Contributors**

Add your name here.

## **9. Open Issues**

A number of open issues have been identified during the work on this document. This document is incomplete since the AAA interaction for MIPv6 bootstrapping is still at an early stage. The following aspects require further discussion:

- o The details of the Diameter bootstrapping with respect to security.
- o AVP formats are not yet provided and a table of occurrence is missing.
- o The IANA consideration section is empty.
- o Diameter Client/Server Behavior needs to be specified explicitly.
- o More examples are useful.
- o Alignment with the ongoing RADIUS MIPv6 bootstrapping needs to be ensured.



## **10. References**

### **10.1. Normative References**

- [1] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [2] Giarretta, G. and A. Patel, "Problem Statement for bootstrapping Mobile IPv6", [draft-ietf-mip6-bootstrap-ps-04](#) (work in progress), February 2006.
- [3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.
- [4] Manner, J. and M. Kojo, "Mobility Related Terminology", [RFC 3753](#), June 2004.
- [5] Chowdhury, K. and A. Yegin, "MIPv6-bootstrapping via DHCPv6 for the Integrated Scenario", [draft-ietf-mip6-bootstrapping-integrated-dhc-00](#) (work in progress), October 2005.
- [6] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", [RFC 3588](#), September 2003.
- [7] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), November 1997.
- [8] Dupont, F. and V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec", [draft-ietf-mip6-ikev2-ipsec-04](#) (work in progress), October 2005.
- [9] Giarretta, G., "Goals for AAA-HA interface", [draft-ietf-mip6-aaa-ha-goals-01](#) (work in progress), January 2006.

### **10.2. Informative References**

- [10] Tschofenig, H., "Mobile IPv6 Bootstrapping using Diameter", [draft-tschofenig-mip6-aaa-ha-diameter-01](#) (work in progress), October 2005.
- [11] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", [RFC 4005](#), August 2005.
- [12] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", [RFC 4072](#), August 2005.



- [13] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", [draft-ietf-mip6-bootstrapping-split-01](#) (work in progress), October 2005.
- [14] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", [RFC 2136](#), April 1997.
- [15] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.

Author's Address

Hannes Tschofenig  
Siemens  
Otto-Hahn-Ring 6  
Munich, Bavaria 81739  
Germany

Email: [Hannes.Tschofenig@siemens.com](mailto:Hannes.Tschofenig@siemens.com)

URI: <http://www.tschofenig.com>



## Intellectual Property Statement

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](mailto:ietf-ipr@ietf.org).

## Disclaimer of Validity

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 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.

## Copyright Statement

Copyright (C) The Internet Society (2006). 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.

## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

