

MIPSHOP Working Group  
Internet-Draft  
Expires: March 25, 2007

W. Haddad  
S. Krishnan  
Ericsson Research  
September 21, 2006

Authenticating FMIPv6 Handovers  
draft-haddad-mipshop-fmipv6-auth-02

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/lid-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 March 25, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document specifies a scheme to secure the handover signaling in FMIPv6 using one way hash chains. The values generated in a one way hash chain will be used one at a time during each handoff to authenticate the signaling messages.

Internet-Draft

FMIPv6 Authentication

September 2006

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Conventions used in this document . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Glossary . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Protocol Operation . . . . .	<a href="#">6</a>
<a href="#">5.</a>	New Options . . . . .	<a href="#">9</a>
<a href="#">5.1.</a>	Hash Handoff Option (HHO) . . . . .	<a href="#">9</a>
<a href="#">5.2.</a>	Hash Extension Option (HEO) . . . . .	<a href="#">9</a>
<a href="#">5.3.</a>	Handoff Vector Option (HVO) . . . . .	<a href="#">10</a>
<a href="#">5.4.</a>	Handoff Option (HO) . . . . .	<a href="#">11</a>
<a href="#">5.5.</a>	Hash Chain Option (HCO) . . . . .	<a href="#">11</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">13</a>
<a href="#">7.</a>	References . . . . .	<a href="#">13</a>
	Authors' Addresses . . . . .	<a href="#">14</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">15</a>

## 1. Introduction

FMIPv6 protocol (described in [[RFC4068](#)]) specifies a fast handoff procedure for IPv6 mobile nodes, which is based on tunneling data packets between the mobile node's previous and new access routers (ARs). The FMIPv6 protocol specification does not provide a method to establish a handoff key to secure the FMIPv6 signaling messages between the MN and the AR. Current proposed schemes require generation of a handoff key at each handover in order to secure the handoff signaling.

This draft suggests a mechanism based on the one-way hash chain technique to authenticate the handoff signaling messages without the burden of generating one "handoff key" by using public keys, per handoff procedure. Values generated in a OWHC will be used one at a time during each handoff to authenticate the signaling messages.

## 2. Conventions used in this document

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](#)].

### [3.](#) Glossary

#### One Way Hash Chain (OWHC)

A one way chain ( $V_0 \dots V_n$ ) is a collection of values such that each value  $V_i$  (except the last value  $V_n$ ) is a one-way function of the next value  $V_{i+1}$ . In particular, we have  $V_i = H(V_{i+1})$ , for  $i$  belonging to  $[0, n[$ . For clarity purpose and to avoid confusion, we'll use in the rest of this document the notation  $V[i]$  instead of  $V_i$ , which means  $V[i+1]$  points to  $V_{i+1} \dots$

#### Fast Binding Update (FBU)

A message from the MN instructing its PAR to redirect its traffic towards the nAR.

#### Previous Access Router (pAR)

The MN's default router prior to its handover.

#### New Access Router (nAR)

The MN's default router subsequent to its handover.

## Fast Binding Acknowledgment (FBA)

A message from the pAR in response to an FBU.

## [4.](#) Protocol Operation

In order to avoid using heavy cryptographic operations and redundant signaling messages to generate a handoff key each time the MN switches to a new AR, the MN should be able to use simpler mechanisms such as OWHC technique in order to authenticate the FBU message sent to its pAR. On the other side, the network access infrastructure should also provide the MN enough assurance that the FBA message is coming from the same AR, which received the FBU message.

Furthermore, it is important to mention that a fast growing class of mobile devices tend to have very limited battery and processing power. Thus the available energy must be meticulously controlled and consumed, i.e., not to be wasted on exchanging unnecessary redundant signaling messages nor on computing unnecessary RSA signatures.

Consequently, care should be taken to rely whenever possible on low processing power operations and to minimize the amount of signaling messages sent from the MN.

The suggested protocol allows an FMIPv6 enabled MN to generate a OWHC (e.g., 20 values) prior to triggering the first fast handoff procedure (i.e., sending an FBU message following the receipt of a PrRtAdv message from its AR). The length of each value of the OWHC SHOULD be equal to 128 bits and SHOULD be used together with another parameter to generate each nCoA interface identifier (IID).

In order to minimize using expensive processing power operations, the MN SHOULD use the SEND procedure only at the beginning, i.e., when switching for the first time to another AR. In this case, the MN sends a RtSol message signed with CGA to its current AR, prior to triggering a fast handoff procedure. The RtSol message SHOULD carry the tip of the MN's OWHC in a new option called the "hash handoff" option (HHO).

Upon receiving a RtSol message carrying an HHO, the AR SHOULD reply by sending confidentially a 64-bit unique parameter called "Handoff Vector" (HV). For this purpose, the AR MUST encrypt the HV with the MN's CGA public key and inserts it in a unicast RtAdv message before sending it to the MN. The AR SHOULD also store the sender's current IPv6 address, the associated OWHC value and the corresponding HV in its mobile cache entries (MCE) for a limited lifetime.

Note that an additional optimization would mainly target the use of CGA technology and would consist on using the Optimized SEND protocol (described in [[OptiSEND](#)]).

In order to respect the MN's privacy, the HV will be used to hide any correlation between the MN's nCoA and the previous CoA (pCoA). This

is achieved by using a simple computation involving the HV and the MN's CoAs.

In addition, upon receiving a valid FBU message from the MN, the AR SHOULD hash the current HV value then forward the first 64-bit value of the resulting hash, i.e., new HV, to the MN's nAR. The new HV (nHV) is inserted in a new option carried by the Handoff Initiate (HI) message. Note that we assume that all links between ARs are secure and the network access infrastructure can be trusted.

When the MN performs a fast handoff procedure (other than the first one), it starts by autoconfiguring a new CoA. For this purpose, it has to compute the nCoA IID. This is done in the following way:

$$\text{nCoA (IID)} = \text{First} [64, \text{OWHC}(\text{NV})) \text{ XOR First}(64, \text{nHV})]$$

The rule to generate the nHV is the following:

$$\text{nHV} = \text{First}[64, \text{SHA1}((\text{n}-1)\text{HV})]$$

Where:

- OWHC(NV) is the next 128-bit undisclosed value from the MN's OWHC.
- First(x,y) is a function which extracts the first "x" bits from "y".
- nHV is the new HV value received by the MN's nAR and (n-1) is the previous value used by the MN's pAR to check the validity of the FBU message.

After generating the nCoA's IID, the MN generates another 64-bit value from XORing the remaining 64-bit of the OWHC(NV) with nHV. The resulting value is called "Hash Extension" (HE) value and is sent in a new option carried by the FBU message. The last step is to authenticate the FBU message with the 128-bit OWHC(NV) and insert the result in the BAD.

Procedures to exchange FBU/FBA messages between the MN and ARs are described in the following:

Upon receiving an FBU message, the AR (i.e., the pAR which has generated the HV) checks its MCE for an entry containing the MN's pCoA. If the MN's pCoA is found, then the pAR decodes the nCoA IID by using its nHV then it decodes the HE value and concatenates the result with the nCoA's IID. The next step consists on hashing the concatenation of the two decoded values and comparing the first 128 bits of the resulting hash to the 128-bit OWHC disclosed value stored in the MN's corresponding entry.

If the two values are equal, then the pAR proceeds to check the authenticity of the BU message and sends an FBA message to the MN.

The FBA message MUST be authenticated with the same key, i.e.,

OWHC(NV), in order for the MN to check if the FBA message has been sent by the same entity which has received the MN's corresponding HV and the FBU message.

Note that the 128-bit OWHC value SHOULD be forwarded by the pAR to the nAR in the HI message. For this purpose, a new option called "Hash Chain" Option (HCO) is defined to carry the OWHC value in the HI message.

When the nAR gets an HI message carrying an HV, it SHOULD store it together with the MN's nCoA in its cache memory for future use. As mentioned earlier, after using SEND protocol with the first AR, any subsequent AR visited by the MN MUST NOT use the same HV value used by the previous one. The same requirement applies also to the MN, which has to hash again its current HV value before using it to compute the nCoA IID.

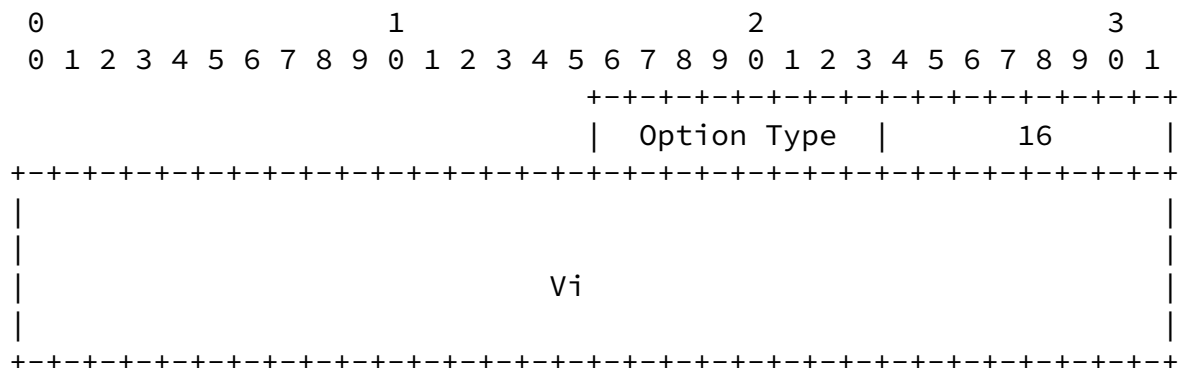
## 5. New Options

This proposal defines 5 new options described in the following:

### 5.1. Hash Handoff Option (HHO)

This option is used to carry a 128-bit value, which is the tip of the MN's OWHC. The HHO is carried by the RtSol message sent by the MN to its current AR.

The format of the option is the following:



Option Type

<To Be Assigned By IANA>

Option Length

16

Option Data

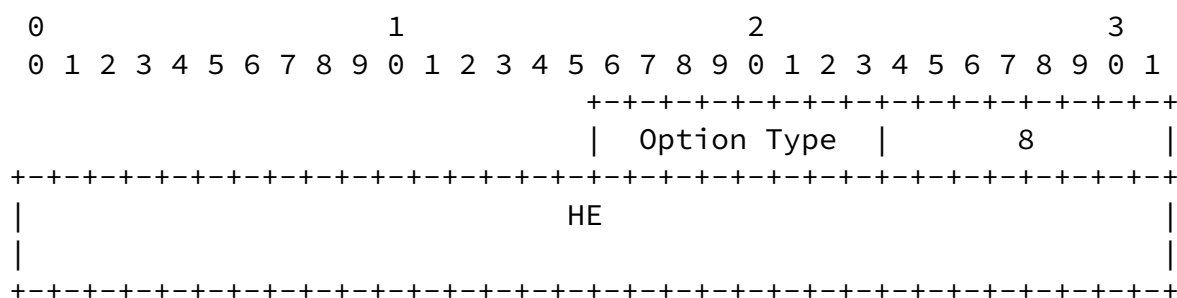
This contains the value at the tip of the hash chain.

### 5.2. Hash Extension Option (HEO)

This option is used to carry the 64-bit value, which is generated from XORing the leftmost 64 bits extracted from the 128-bit OWHC(NV) with the first 64 bits resulting from hashing HV (or re-hashing). The HEO is carried by the FBU message sent by the MN to the pAR.

The format of the option is the following:

September 2006



<To Be Assigned By IANA>

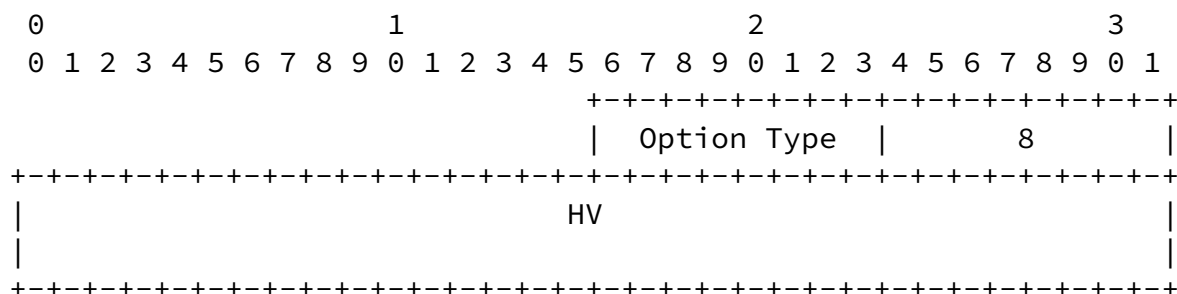
8

Contains the 64-bit HE, which is used by the MN to provide the pAR the ability to discover the entire OWHC(NV), i.e., the new shared secret, in order to check the authenticity of the FBU message and to authenticate the FBA message.

### 5.3. Handoff Vector Option (HVO)

This option is carried by the RtAdv message sent by the AR after receiving a RtSol message carrying an HHO. The HVO is used to carry the 64-bit handoff vector.

The format of the option is the following:



Option	Type
	<To Be Assigned By IANA>

Option Length  
8.

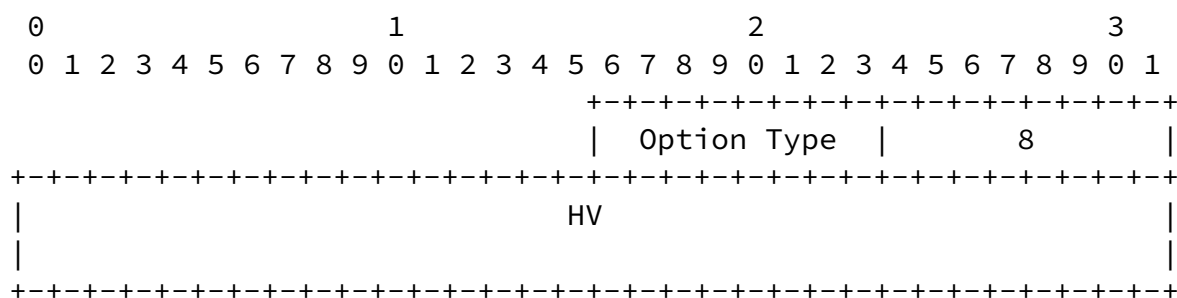
Option Data  
Contains the 64-bit HV, which is the used by the MN to prevent correlation between its different CoAs generated from the same OWHC,

and by the AR to decode the MN's CoA(s) and the HE value prior to hashing the combination and checking the validity of the FBU message. Note that the HV value is hashed by the MN at each handoff and by each nAR before storing it in the corresponding MCE.

#### 5.4. Handoff Option (H0)

This option is carried by the HI message sent by the pAR to the nAR upon receiving a valid FBU message. The HO carries the 64-bit HV in order to allow the nAR to check the validity of the FBU message sent by the MN to its nAR.

The format of the option is the following:



Option	Type
	<To Be Assigned By IANA>

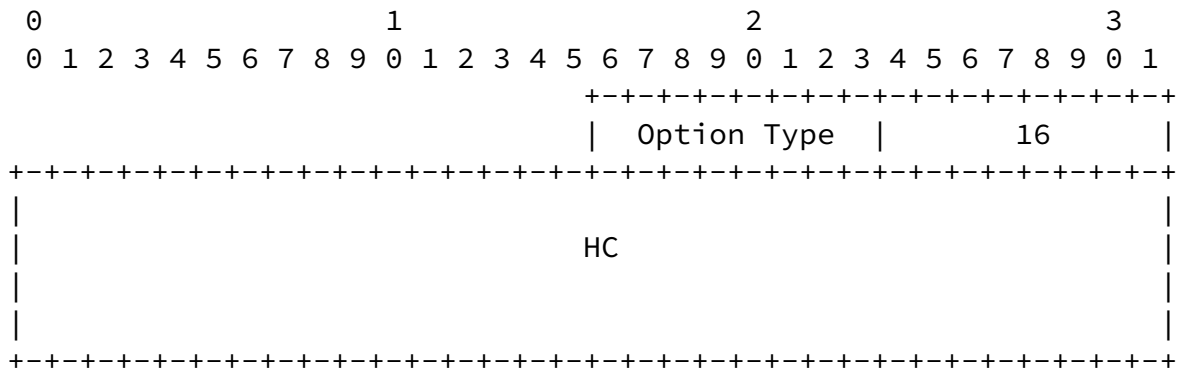
Option Length  
8.

Option Data  
Contains the 64-bit HV.

### 5.5. Hash Chain Option (HCO)

This option is carried by the HI message sent by the pAR to the nAR upon receiving a valid FBU message. The HCO carries the 128-bit OWHC value computed by the MN's pAR from data received in the FBU message sent by the MN.

The format of the option is the following:



Option Type  
<To Be Assigned By IANA>

Option Length  
16

Option Data	Contains the last disclosed 128-bit value from the MN's OWHC.
-------------	---

## 6. Security Considerations

This document specifies a simple scheme to secure the handover signaling using one way hash chains. The values generated in a one way hash chain will be used one at a time during each handover to secure the fast mobility signaling.

The suggested proposal relies also on the assumption that a trust relationship between the MN and the network access infrastructure exists in order to guarantee that the HV parameter won't be forwarded to a malicious node at a particular time.

The suggested proposal fulfills the requirements dictated by low processing and battery power mobile devices regarding the number of signaling messages sent by the mobile node and the use of RSA signatures, without creating nor amplifying new and/or existing threats.

## 7. References

[OptiSEND]

Haddad, W., Krishnan, S., and J. Choi, "Secure Neighbor Discovery (SEND) Optimization and Adaptation for Mobility: The OptiSEND protocol", Internet Draft, [draft-haddad-mipshop-optisend-01.txt](#), June 2006.

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

[RFC4068] Koodli, R., "Fast Handovers for Mobile IPv6", Internet Draft, [draft-ietf-mipshop-fmipv6-rev-00.txt](#), April 2006.

Authors' Addresses

Wassim Haddad  
Ericsson Research  
Torshamnsgatan 23  
SE-164 80 Stockholm  
Sweden

Phone: +46 8 4044079  
Email: [Wassim.Haddad@ericsson.com](mailto:Wassim.Haddad@ericsson.com)

Suresh Krishnan  
Ericsson Research  
8400 Decarie Blvd.  
Town of Mount Royal, QC  
Canada

Phone: +1 514 3457900  
Email: Suresh.Krishnan@ericsson.com

Haddad & Krishnan Expires March 25, 2007 [Page 14]

---

Internet-Draft FMIPv6 Authentication September 2006

#### 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.