

MIPSHOP Working Group  
Internet-Draft  
Expires: February 8, 2007

W. Haddad  
S. Krishnan  
Ericsson Research  
H. Soliman  
Qualcomm-Flarion  
August 7, 2006

Using Cryptographically Generated Addresses (CGA) to secure HMIPv6  
Protocol (HMIPv6sec)  
draft-haddad-mipshop-hmipv6-security-06

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 February 8, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This memo describes a method for establishing a security association between the mobile node and the selected mobility anchor point in an hierarchical mobile IPv6 domain. The suggested solution is based on using the cryptographically generated address technology.

Internet-Draft

HMIPv6sec

August 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>	Proposed Solution . . . . .	<a href="#">6</a>
<a href="#">5.</a>	New Messages and Options Format . . . . .	<a href="#">9</a>
<a href="#">5.1.</a>	The Pre-Binding Update (PBU) Message Format . . . . .	<a href="#">9</a>
<a href="#">5.2.</a>	Third Party Shared Key (TPSK) Option . . . . .	<a href="#">10</a>
<a href="#">5.3.</a>	The MAP Session Mobility Secret (MSMS) Option . . . . .	<a href="#">10</a>
<a href="#">5.4.</a>	The Session Mobility Secret (SMS) Option . . . . .	<a href="#">11</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">13</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">14</a>
<a href="#">8.</a>	Change Log . . . . .	<a href="#">15</a>
<a href="#">9.</a>	References . . . . .	<a href="#">16</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">16</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">16</a>
	Authors' Addresses . . . . .	<a href="#">17</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">18</a>

---

Internet-Draft

HMIPv6sec

August 2006

## 1. Introduction

The Hierarchical Mobile IPv6 Mobility Management [[HMIPv6](#)] did not specify nor favor any particular mechanism for establishing a Security Association (SA) between the Mobile Node (MN) and the Mobility Anchor Point (MAP) located within an HMIPv6 domain.

This memo describes a method, which allows the MN to establish an SA with the selected MAP. The suggested solution is based on using the Cryptographically Generated Address technology (described in [[CGA](#)]).

## 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 [[TERM](#)].

### [3.](#) Glossary

#### Access Router

The Access Router is the Mobile Node's default router. The AR aggregates the outband traffic of mobile nodes.

#### Mobility Anchor Point (MAP)

A Mobility Anchor Point is a router located in a network visited by the mobile node, which is used by the MN as a local Home Agent (HA).

#### Regional Care-of Address (RCoA)

A Regional Care-of Address is an address obtained by the MN from the visited network. An RCoA is an address on the MAP's subnet and is auto-configured by the MN when receiving the MAP option.

#### On-link Care-of Address (LCoA)

The LCoA is the on-link CoA configured on a mobile node's

interface based on the prefix advertised by its default router.

#### Local Binding Update (LBU) Message

The MN sends a Local Binding Update message to the MAP in order to establish a binding between the RCoA and the LCoA.

#### Pre-Binding Update (PBU) Message

The MN's default router sends a Pre-Binding Update message to the MAP upon receiving a Router Solicitation (RtSol) message signed with CGA technology as described in the secure neighbor discovery protocol [[SEND](#)].

#### Cryptographically Generated Address (CGA)

A technique described in [[CGA](#)] whereby an IPv6 address of a node is cryptographically generated by using a one-way hash function from the node's public key (Kp) and some other parameters.

#### Binding Acknowledgment (BA) Message

The MAP sends a binding acknowledgment message to the MN in response to an LBU message.

## [4.](#) Proposed Solution

We assume that the MN's LCoA is always computed based on the CGA technology, in order to allow the MN to run SEND protocol. Such assumption has also been made in [[FMIPkey](#)], which aims to provide a security mechanism for [[FMIPv6](#)] protocol, and in the ongoing work on optimizing the SEND protocol (described in [[OptiSEND](#)]).

In addition, we assume that the MN can discover the presence of an HMIPv6 domain before sending a RtSol message. One example on how to discover the HMIPv6 domain may consist on using technologies described in [[FRD](#)]. However, it is important to mention that the proposed solution works with the same performance without such assumption.

A third assumption is the existence of secure links between all routers located within the MAP tree. Such assumption is justified by the fact that HMIPv6 protocol requires that routers within the MAP tree get involved in delivering the RtAdv message sent by the MAP(s) and in assisting the MN in selecting the most appropriate MAP. The lack of secure links between nodes involved in offering the MAP service can make it vulnerable to denial of service (DoS) attacks.

The suggested solution introduces a new signaling message, i.e., the Pre-Binding Update (PBU) message, which is sent by the AR to the MAP upon receiving a RtSol message from the MN carrying a valid signature (i.e., the message is signed with the MN's CGA private key).

The following figure shows the signaling diagram for establishing a bidirectional SA between the MN and the MAP:

1. MN to AR: Router Solicitation [CGA Signature] (RtSol)
- 2a. AR to MN: Router Acknowledgement [Ks] (RtAdv)
- 2b. AR to MAP: Pre-Binding Update [Ks + LCoA] (PBU)
3. MN to MAP: Local Binding Update [DH value (X)] (LBU)
4. MAP to MN: Binding Acknowledgment [DH value (Y)] (BA)

The suggested solution is described in the following steps:

- o the MN configures a 64-bit interface identifier (IID) from using CGA technology then uses it to send a RtSol message signed with CGA, according to the SEND protocol. Note that at this stage, the MN may not be aware that it has entered an HMIPv6 domain.
- o Upon receiving a valid unicast RtSol message, the AR replies immediately by sending back a unicast RtAdv message to the MN and in parallel, a PBU message to the MAP. For this purpose, the AR MUST compute a secret (Ks), encrypts it with the MN's CGA public

key and sends it in the unicast RtAdv message. The shared secret is inserted in a new option (Third Party Shared Key (TSPK)), which is carried by the unicast RtAdv message.

The AR MUST also compute the LCoA and RCoA that the MN is supposed to autoconfigure. For this purpose, the LCoA is computed by appending the 64-bit IID used in the RtSol message to the 64-bit prefix advertised by the AR and the RCoA is computed by appending the 64-bit prefix advertised by the MAP with the 64-bit IID

computed in the following way:

$$\text{RCoA (IID)} = \text{First}(64, \text{SHA1}(\text{Ks} \mid \text{LCoA}))$$

Where  $\text{First}(x,y)$  is a function, which extracts the first  $x$  bits from  $y$  and LCoA is the MN's on link care-of address.

After computing the MN's LCoA and RCoA, the AR inserts the two IPv6 addresses and Ks in the PBU message and sends it to the MAP. As noted earlier, it is assumed that the PBU messages are signed by the ARs and the paths between the ARs and the MAP are secure.

- o After receiving the PBU message, the MAP creates a binding cache entry (BCE) for the MN, in which it stores the MN's LCoA, RCoA and Ks carried by the PBU message. Once the BCE is created, the MAP waits for a limited amount of time for the owner of the two addresses to send the LBU message. If no valid LBU message is received during the BCE preconfigured lifetime then the MAP SHOULD delete it.
- o When the MN gets a valid RtAdv message, it discovers that it has entered an HMIPv6 domain. The following is based on the assumption that the MN decides to use the MAP as its local Home Agent, which means that the MN has to configure an RCoA then request the MAP to create a BCE. For this purpose, the MN SHOULD use the same method as the AR (described earlier) to autoconfigure its RCoA and LCoA. After that, the MN initiates a Diffie-Hellman (DH) procedure with the MAP by sending its DH public value (X) in a new option (Session Mobility Secret (SMS)), which is carried by the first LBU message sent to the MAP in order to request the MAP to bind its LCoA to its new RCoA. The MN MUST protect the integrity of the LBU message by including a keyed hash of the message using Ks. The keyed hash is syntactically and semantically similar to the Binding Authorization Data option specified in [\[MIPv6\]](#).
- o Upon receiving an LBU message, the MAP searches its BCEs table for an LCoA, which matches the one sent in the LBU message. If the same LCoA is found, then the MAP computes the RCoA IID in the same way as described above, and compares it to the one claimed by the

MN in the LBU message then it checks the authenticity of the



message.

If the LBU message is valid, then the MAP completes the DH exchange by sending its own DH public value (Y) in a new option (MAP Session Mobility Secret (MSMS)), which is carried by the BA message sent to the MN. The MAP MUST protect the integrity of the BA message by including a keyed hash of the message using Ks. The keyed hash is syntactically and semantically similar to the Binding Authorization Data option specified in [\[MIPv6\]](#).

By sending (Y) to the MN, both nodes will be able to compute the session mobility key (Ksm) (i.e., from values (X) and (Y)).

Note that if the RCoA address sent in the LBU message is not the same as the one stored in the corresponding BCE then the MAP MUST simply discard the LBU message.

- o After sending the first BA message, the MAP SHOULD keep Ks and (Y) in the MN's corresponding BCE until a new value of the binding update sequence number is stored. This is needed in case the MN goes out of reach for a short period of time and misses the first BA message (i.e., (Y)), in which case it has to re-send the LBU message.
- o When the MN gets a BA message carrying a DH value, i.e., an SMS option, it starts by checking its authenticity with Ks. If the message is valid then the MN computes Ksm and establishes a bidirectional SA with the MAP.
- o By completing the DH procedure, both nodes will be able to compute the session mobility key (Ksm) (i.e., from values (X) and (Y)) and use it to authenticate subsequent LBU/BA messages exchanged between them.

Note that the SA lifetime is set to 24 hours, after which the MN has to request the MAP to renew it.

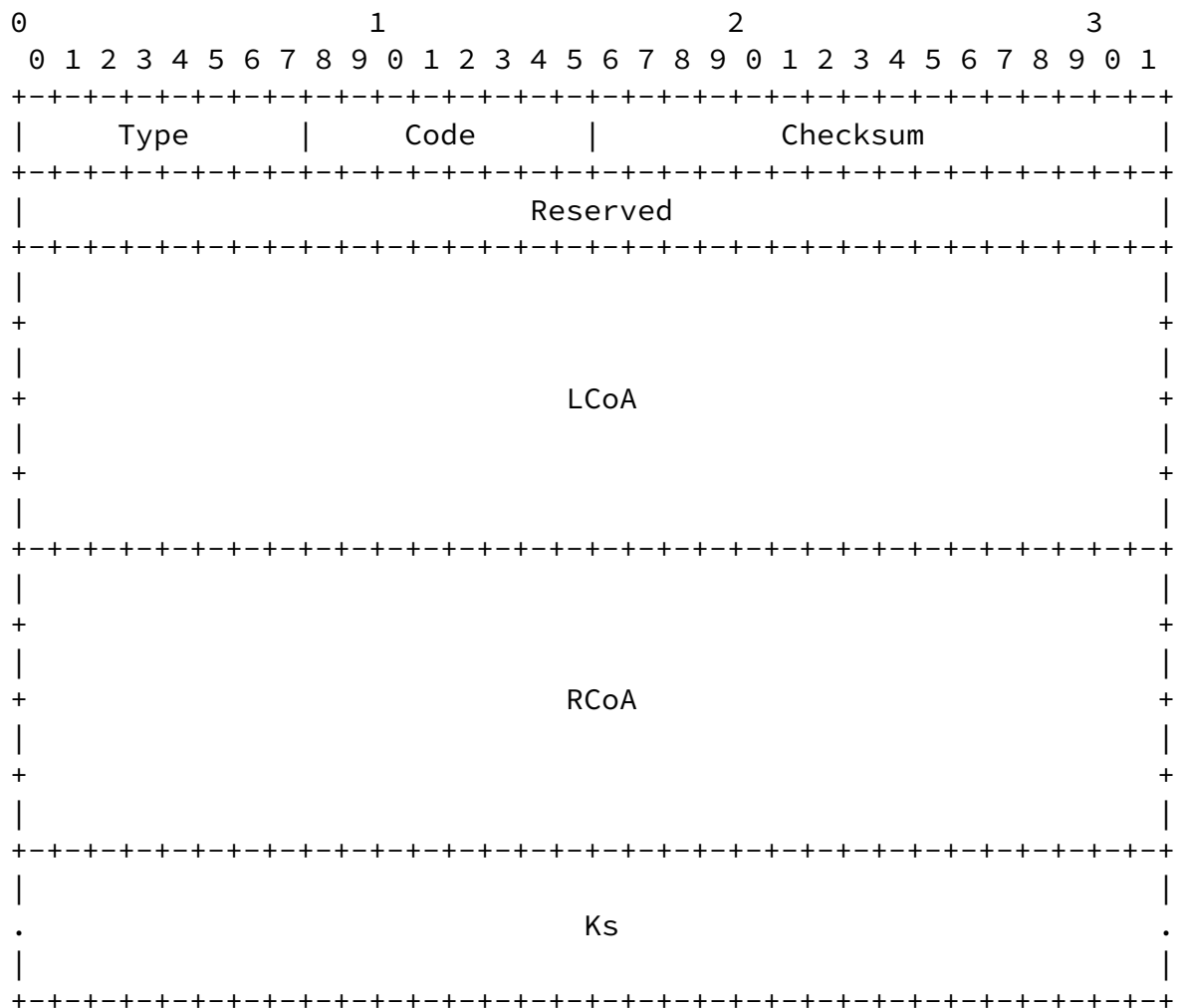
## 5. New Messages and Options Format

In the following, we describe the PBU message structure and the format of the four new options.

### 5.1. The Pre-Binding Update (PBU) Message Format

When the AR receives a valid RtSol message signed with CGA, it sends a PBU message to the MAP, which carries the MN's LCoA, RCoA and Ks.

The format of the PBU message is as follows:



Type

<To Be Assigned By IANA>

Code 0

The ICMP checksum. For more details see [\[ICMPv6\]](#).

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

This field contains the MN's LCoA.

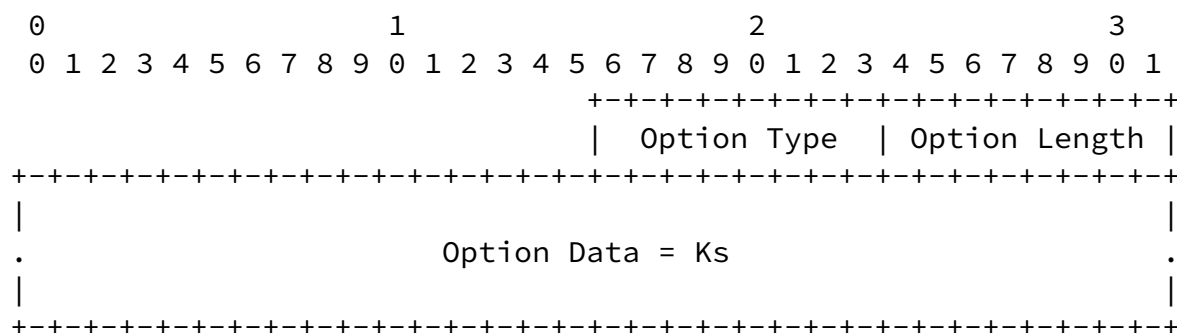
This field contains the MN's RCoA.

The shared secret sent by the AR to the MN and to the MAP.

### 5.2. Third Party Shared Key (TPSK) Option

The Third Party Shared Key Option is carried by the unicast RtAdv message sent by the AR to the MN, in response to a RtSol message carrying a valid signature. The TPSK option **MUST** carry the shared secret  $K_s$ .

When used, the TPSK option has the following format:



<To Be Assigned By IANA>

Length of the option.

This field contains the shared secret  $K_s$ .

### 5.3. The MAP Session Mobility Secret (MSMS) Option

The MSS Option is used by the MAP to carry the DH public value (Y) sent in the BA message, in response to the first LBU message carrying an SMS option sent by the MN to the MAP.

[Page 10]

August 2006

Note that the first BA message sent by the MAP to the MN MUST be authenticated with  $K_s$ .

The MSMS option has the following format:

[illegible]

<To Be Assigned By IANA>

Length of the option.

The Option Data field contains the DH public value (Y) sent by the MAP to the MN in the BA message.

#### 5.4. The Session Mobility Secret (SMS) Option

The SMS option is carried by the first LBU message sent by the MN to the MAP after receiving an unicast RtAdv message carrying a TPSK option. The SMS option contains the DH public value (X) sent by the MN to the MAP to initiate a DH exchange, which will allow both nodes

Note that the first LBU message sent by the MN to the MAP MUST be authenticated with  $K_s$ .

```

0                                     1                                     2                                     3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                     | Option Type | Option Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|
.           Option Data = (X)
|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

```

<To Be Assigned By IANA>

Length of the option.

The Option Data field contains the DH public value (X) sent by the MN to the MAP in the first LBU message.

## 6. IANA Considerations

This document introduces 3 new types of options and one new type of message. The values of these types are 8-bit unsigned integers. These values are allocated according to the Standards Actions or IESG approval policies defined in [[IANA](#)].

## [7.](#) Security Considerations

This proposal suggests using the CGA technology to secure the exchange between the MN and the AR as described in the SEND protocol, to derive a first shared secret between the two entities and to use it later to authenticate Diffie-Hellman messages exchanged between the MN and the MAP. This is recommended due to the fact that public key signature is a computationally expensive and lengthy procedure.

The suggested proposal does not create nor enhance any new and/or existing threats. In particular, launching a man-in-the middle

attack against the MN is not possible because the attacker is not aware of the shared secret  $K_s$ .

The proposal provides integrity protection by including a keyed hash of the message. The proposal provides replay protection by using the sequence number in the binding updates. The proposal does not require the MAP to have prior knowledge of the MN's identity.

The suggested proposal DOES NOT guard against compromise of the access router. If the access router is compromised it can act as a man-in-the-middle for the MN-MAP exchange. But a compromised router can do far worse things like null routing all the packets emanating from the mobile node, or modify router advertisements to conceal the presence of a HMIPv6 domain. We consider the AR compromise problem to be orthogonal to the issues addressed in this draft.

## [8.](#) Change Log

This document introduces the following changes from previous versions:



- Remove the reliance on the crypto-based identifier (CBID) in order to further simplify the protocol.
- Remove any new option from the RtSol message and adopt the same format as used in SEND.
- Reduce the size of the PBU message by eliminating the need to send the MN's CGA public key.
- Change the document title to reflect the new modifications.
- Correct few typos.

## [9.](#) References

### [9.1.](#) Normative References

- [CGA] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [HMIPv6] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6)", Internet Draft, [draft-soliman-mipshop-4140bis-00.txt](#), June 2006.
- [IANA] Narten, T. and H. Alverstrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 2434](#), [BCP 26](#), October 1998.
- [ICMPv6] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6 (IPv6) Specification", [RFC 2463](#), July 2005.
- [MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [SEND] Arkko, J., Kempf, J., Nikander, P., and B. Zill, "Secure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [TERM] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", [RFC 2119](#), BCP , March 1997.

### [9.2.](#) Informative References

- [FMIPkey] Kempf, J. and R. Koodli, "Bootstrapping a Symmetric IPv6 Key Handover Key from SEND", Internet Draft, [draft-kempf-mipshop-handover-key-00.txt](#), June 2006.
- [FMIPv6] Koodli, R., "Fast Handovers for Mobile IPv6", Internet Draft, [draft-ietf-mipshop-fmipv6-rev-00.txt](#), April 2006.
- [FRD] Choi, J., Chin, D., and W. Haddad, "Fast Router Discovery with L2 Support", Internet Draft, [draft-ietf-dna-frd-01.txt](#), June 2006.
- [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](#), March 2006.

Internet-Draft

HMIPv6sec

August 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: +1 514 345 7900  
Email: [Suresh.Krishnan@ericsson.com](mailto:Suresh.Krishnan@ericsson.com)

Hesham Soliman  
Qualcomm-Flarion

Phone: +1 908 997 9775  
Email: [hsoliman@qualcomm.com](mailto:hsoliman@qualcomm.com)

Internet-Draft

HMIPv6sec

August 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.