

Internet Engineering Task Force
Internet Draft
Expires in July 2004

Wassim Haddad
Ericsson Research Canada
Helsinki University of Technology
Francis Dupont
ENST Bretagne
Lila Madour
Alan Kavanagh
Suresh Krishnan
Ericsson Research Canada
Soohong Daniel Park
Samsung Electronics
Hannu Kari
Helsinki University of Technology
February 2004

BUB: Binding Update Backhauling

<[draft-haddad-mip6-bub-01.txt](#)>

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

This document is an Internet-Draft. 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>.

Distribution of this memo is unlimited

Abstract

Mobile IPv6 protocol defines two different modes to address the mobility problem. This document describes a new mode, called Binding Update Backhauling (BUB), which has been especially

designed for highly mobile environment, i.e, the two mobile nodes are mobile. The BUB mode offers a more secure and optimized exchange of binding updates (BUs) between the two mobile endpoints.

Table of Contents

1. Introduction.....	2
2. Terminology.....	3
3. Motivation.....	3
4. Proposed solution.....	4
5. Defining BUB.....	5
5.1 The BUB test.....	5
5.2 The BUB Option format.....	7
5.3 The BUB Complete Message Structure.....	8
6. The Diffie Hellman Exchange.....	10
7. Impact on BU/BA Messages.....	10
8. Security Considerations.....	12
9. Acknowledgments.....	12
10. Normative References.....	12
11. Informative References.....	13
12. Author's Addresses.....	13
13. Full Copyright Statement.....	14
Appendix A.....	16

[1. Introduction](#)

The mobility problem has been described in most cases, as a scenario involving one mobile endpoint referred to as MN and another static endpoint referred to as CN.

Mobile IPv6 defines two different modes to handle the mobility problem. These modes are the bidirectional tunneling (BT) and route optimization (RO). The two modes represent a trade-off between security and efficiency. For instance, the BT mode enables a secure exchange but is not optimized at all, while the RO mode offers better efficiency but raises many security concerns.

This draft describes a new mode called Binding Update Backhauling (BUB), which has been especially designed to be used in scenarios involving two mobile endpoints. This mode enables a more secure and reliable way for exchanging mobility signaling messages, while preserving at the same time the efficiency of the routing optimization mode.

[2](#). Terminology

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "MAY" in this document are to be interpreted as described in [RFC 2219](#) [3].

[3](#). Motivation

The route optimization (RO) mode allows two endpoints to exchange data traffic by using the direct path between them. This is achieved by using new mobility headers and relies on exchanging mobility signaling messages each time the MN switches to a new network (i.e., changes its IP address).

Each time a MN gets a new IP address (i.e., care-of address), it needs, according to [\[1\]](#), to run a return routability (RR) test in order to test the reachability of its new care-of address and home address by the CN, prior to sending any binding update (BU) message to the CN.

Such test is performed by exchanging two signaling messages (CoTI/CoT) on the new direct path (i.e., the path used to exchange data traffic), and two signaling messages (HoTI/HoT) using the path going through the MNs'HA. The result of the test creates a new state at the CN to be used to check the authenticity of the BU sent by the MN. Only a successful test

allows the MN to send a BU to the CN to update its binding cache entry (BCE). The CN should acknowledge the BU by sending a binding acknowledgment (BA) to the MN.

In total, 6 messages are needed to update the CN with the new MN's IP address.

If the CN becomes mobile, it needs to go through the same procedure (i.e., exchange 6 messages) each time it gets a new IP address, in order to keep the session alive.

Note that, for security reasons, it is stated in [1] and explained in [4] that the lifetime of the state created at the correspondent node is deliberately restricted to a few minutes, in order to limit the potential ability of time shifting attack.

From the above scenario it appears that when the RO mode is used between two mobile endpoints, it may create additional and undesirable traffic, due to a high redundancy of unprotected mobility signaling messages, thus more vulnerabilities. Actually, when the CN becomes mobile, the frequency, as well as the redundancy, of mobility signaling messages will increase, thus making them more visible for a malicious node moving nearby the two endpoints.

Note that when the CN is mobile, it is highly probable that a malicious node may be positioned nearby, thus creating a vulnerability on both sides (since another one may probably be located nearby the MN). Such scenario makes the exchange of signaling messages between the two endpoints more challenging with regards to the security requirements.

If MN2 moves at the same time than MN1, mobility signaling messages may get lost due to the fact that MN1's care-of address and MN2's care-of address have changed at the same time. Such scenario will probably increase the latency of the handover process, which is not desired especially for time sensitive applications.

To address all issues described above, any possible solution should offer an efficient optimization with regards to security

requirements, the number of signaling messages and the handover latency.

This document describes one such optimization which meets all these requirements.

4. Proposed solution:

The Binding Update Backhauling (BUB) is a new mode designed to be used between two mobile endpoints. The suggested mode should be considered as an enhancement to the route optimization mode since it uses the same direct path between the MN and CN for the data traffic exchange.

The main objectives of the BUB mode are to reduce the number of mobility signaling messages exchanged between the two MNs and increase the security of what will remain. This is achieved by eliminating the HoTI/HoT and CoTI/CoT messages, diverting the BU messages to a more secure and reliable path going through the two HAs and keep using the direct path for the data traffic exchange.

The design of the proposed solution is based on the following:

- a) The paths between the MNs and their HAs are protected by an ESP tunnel [2].
- b) The path between the two HAs, being part of the backbone, is assumed to be more secure and more stable than the dynamic path between the two MNs.
- c) A malicious node cannot be at the same time near the MNs and near the path going between the two HAs.

By diverting the signaling messages to a more reliable path, BUB addresses the following issues:

- Security of BUs

By sending the BUs through the link between the two HAs

and by establishing a bidirectional security association (SA) between the two MNs.

- Double Jumping Problem

By avoiding the loss of mobility signaling messages, BUB reduces the latency caused by such loss.

- Excessive Signaling

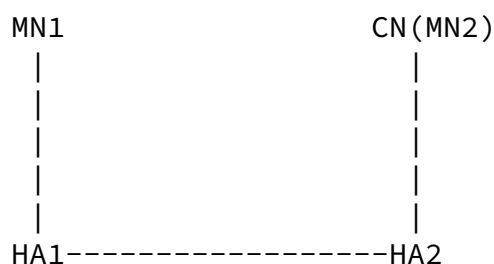
BUB reduces the number of signaling messages, exchanged between the two MNs, by eliminating the need for the HoTI/HoT and CoTI/CoT messages.

The mobile nodes should be able to switch to the BUB mode once both nodes have moved outside their home networks. The BUB mode can be applied at any time during the ongoing session.

[5. Defining BUB](#)

[5.1 The BUB Test](#)

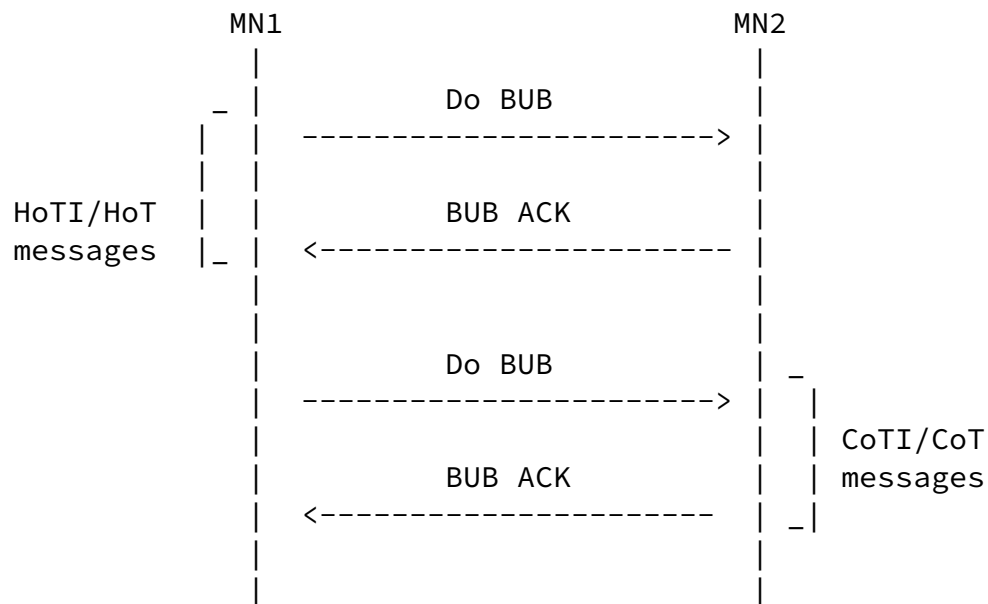
When both endpoints are mobile, the following four entities become involved:



In the above scenario, switching to BUB mode should not occur before running a successful BUB test. The BUB test makes both endpoints agree on using the link going through the two HAs for

exchanging the BU messages. The BUB test consists on exchanging four messages and MUST be run in parallel with the RR test.

In the following scheme, MN1 is asking MN2 to switch to BUB mode:



A successful completion of a BUB test consists of sending two messages "Do BUB" and receiving two messages "BUB ACK". Each request is incorporated into a HoTI and a CoTI message and each reply is incorporated into a HoT and a CoT message. Using these two messages enables MN1 to use two different paths to test the willingness of MN2, without adding new ones.

If the sender gets two different responses in the CoT and the HoT messages, it SHOULD re-run the RR test procedure and the BUB test. In the latter case, if the sender gets again two different responses, it MUST abandon switching to the BUB mode.

A BUB test fails if both of the "BUB ACK" messages are not received after two successive tries. In this case, MN1 MUST send the BUs according to the R0 mode.

Note that in case of test failure, the endpoint, which has launched the BUB test procedure MUST NOT run it again during the same session. However, the other endpoint MUST always be able to start a BUB test at any time during the same ongoing

session.

If one mobile node launches a BUB test and the other endpoint does not wish to switch to the BUB mode, it MUST reply to the

BUB test by sending two negative acknowledgments (NACK). Such scenario may occur in case the other endpoint is static or it has become static (i.e., it has not sent any BUs since a predefined time).

If the two mobile endpoints agree to switch to the BUB mode, they SHOULD NOT switch back at any time to the R0 mode in the ongoing session.

A positive BUB test will generate an additional message called BUB Complete (BUBC) message, which will be sent by the responder to the BUB test. The BUB complete message MUST follow the following rules:

- The BUBC message is sent on the direct path to the MN's care-of address used as the source address in the CoTI message or as the destination address in the CoT message.
- The source address of the BUBC message is the same one used as the source address in the CoT message.
- The BUBC message MUST contain a HAO including the home address of the sender and the care-of init cookie sent by the MN in the CoTI message.
- The BUBC message will contain a cookie called BUB cookie and MUST be signed by the Kbm. The cookie MUST be used with the Kbm to sign the DH messages.
- The BUBC message is sent after the CoT message.

If the MN receives the BUBC message before the CoT, it will stop processing it and wait for the CoT message. If the CoT/BUBC message is lost, then a new CoTI message is sent and the responder MUST re-send a new CoT and BUBC messages.

The signature of the DH messages will use the Kbm as pre-shared secret and the cookie sent in the BUB message. The signature MUST be equal to:

Signature (DH_Message) =
 First(96, HASH_SHA1(Kbm , DH_Message | cookie))

5.2 The BUB Option format

A new BUB option will be defined for carrying BUB messages. This option MAY be inserted in all Return Routability test messages (i.e., HoTI, HoT, CoTI, CoT). The format of the new option is the following:

```

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...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Option Type

TBD

Option Length

Length of the option: 1

Option Data

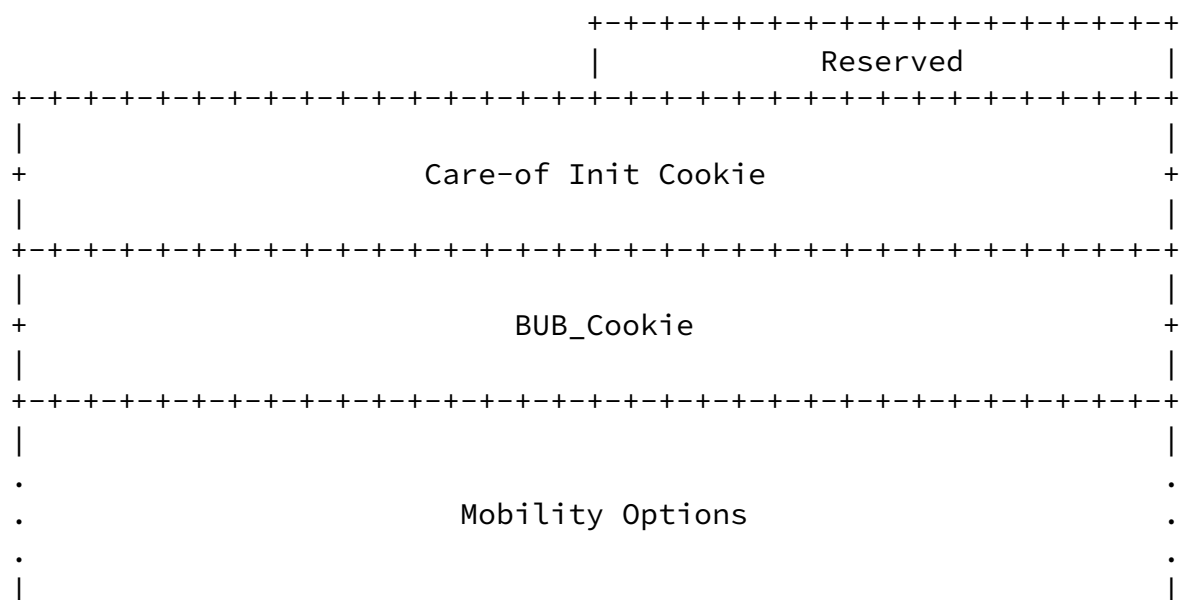
This field can contain one of two possible messages defined in three different codes as following:

code 0 => "Do BUB"
 code 1 => "BUB ACK"
 code 2 => "BUB NACK"

- When used in a HoTI message: the field MUST contain the code "0".

- ### 5.3 The BUB Complete Message Structure

The BUB complete message uses the MH Type value 8. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

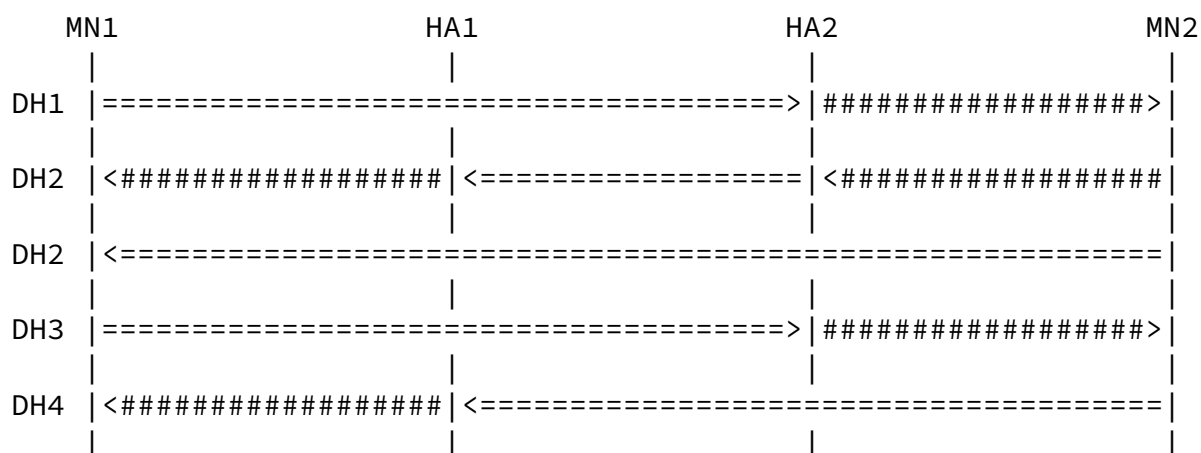


The DH exchange is launched immediately after a successful BUB test, by the MN, which has launched the test (e.g., MN1).

In order to mitigate a MiTM attack, MN1 MUST insert its IP home address in a HAO attached to the first DH message and send it to the MN2's home address (i.e., via HA2).

After receiving the first DH message, MN2 MUST duplicate the second DH message and send one copy on the direct path to MN1's care-of address and another copy to MN1's home address. The second copy MUST be sent on the path going through the two HAs. The third DH message MUST be sent by MN1 to MN2's home address on the same path than DH1. Upon receiving the third message, MN2 MUST completes the DH message by sending the fourth message to MN1's home address.

The different paths taken by the DH messages are shown in the following:



====>: denotes an authenticated message

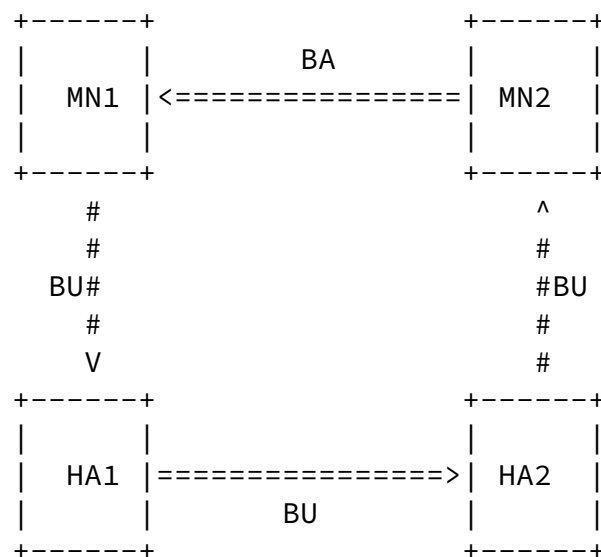
#####>: denotes an encrypted message

7. Impact on BU/BA Messages

As it has been mentioned earlier, the main reasons for designing BUB are the security concerns around the BU messages and the high redundancy in mobility signaling messages. The

establishment of a bidirectional SA between the two MNs enables them to substantially improve the safety of the BU messages and eliminates the need for any further HoTI/HoT and CoTI/CoT messages during the ongoing session. Such optimization leads to a reduction of 4 messages between the two MNs each time a BU is sent.

The different paths used to exchange the BU/BA messages appears in the following scheme:



====>: denotes an authenticated message

####>: denotes an encrypted message

When MN1 switches to a new network (i.e., gets a new care-of address), it sends a BU message to MN2 on the path going through the two HAs. MN1 MAY duplicate the BU message and another copy on the direct path. The two BU messages MUST have the same sequence number and MUST be signed with the authenticated binding management (Kabm) key.

After switching to the BUB mode, the following rules MUST be applied:

- The MNs MUST NOT use the alternate care-of address option in

the BU messages sent to each other, in order to counter 3rd party bombing attack [6].

- The MN MUST NOT use the nonce indices option in all new

binding updates messages sent after a care-of address change.

The MN SHOULD set the Acknowledge (A) bit in the BU message after switching to OMIPv6.

To avoid replay attacks, the MN, which has launched the BUB test will keep the sequence number sent in the first BU immediately after the DH exchange and increment it in all subsequent BU messages. The same rule MUST be adopted by the other mobile endpoint.

In case the session starts with one MN and one static node (CN) and OMIPv6 [7] is applied, then switching to the BUB mode (i.e., the static node becomes mobile) can be done seamlessly. In such scenario, the same Kabm key can be used to sign the BU message sent by the CN (i.e., MN2) and MN2 MUST send its BU messages on the path going through the two HAs. MN1 MUST use the same path for any subsequent BU messages. Both nodes can duplicate their BU messages and use the direct path to send the second copy.

[8.](#) Security considerations

This draft proposes a new mode which makes the exchange of BUs more secure. It should be considered as an enhancement to the security of the signaling messages exchange between two mobile endpoints.

[9.](#) Acknowledgments

Authors would like to thank Laurent Marchand for his review and comments on the draft. Many Thanks to Karim El-Malki and Shinta Sugimoto for improving the draft.

10. Normative References

- [1] D. Johnson and C. Perkins, "Mobility Support in IPv6",
[draft-ietf-mobileip-ipv6-24.txt](#), June 2003.
- [2] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect
Mobile IPv6 Signaling between Mobile Nodes and Home Agents",
[draft-ietf-mobileip-mipv6-ha-ipsec-06.txt](#).
- [3] S. Bradner, "Key words for use in RFCs to Indicate
Requirement Levels", [BCP 14](#), [RFC 2119](#).

Haddad, et al.

Expires July 2004

[Page 12]

INTERNET-DRAFT

Binding Update Backhauling

January 2004

11. Informative References

- [4] P. Nikander, T. Aura, J. Arkko, G. Montenegro and E. Nordmark
"Mobile IP version 6 Route Optimization Security Design
Background", [draft-nikander-mobileip-v6-ro-sec-01](#).
- [5] Krawczyk, H., "SIGMA: the 'SIGn-and-MAC' Approach to
Authenticated Diffie-Hellman and its use in the IKE
Protocols", in Advances in Cryptography - CRYPTO 2003
Proceedings, LNCS 2729, Springer, 2003. Available at:
<http://www.ee.technion.ac.il/~hugo/sigma.html>.
- [6] F. Dupont, "A note about 3rd party bombing in Mobile IPv6",
[draft-dupont-mipv6-3bombing-00](#), February 2004.
- [7] W. Haddad, F. Dupont, L. Madour, S. Krishnan, S. D. Park,
"Optimizing Mobile IPv6 (OMIPv6)",
[draft-haddad-mipv6-omipv6-01](#), February 2004.

12. Authors' Addresses

Wassim Haddad
Ericsson Research Canada
8400, Decarie Blvd

Town of Mount Royal
Quebec H4P 2N2
CANADA
Phone: +1 514 345 7900
Fax: +1 514 345 7900
E-Mail: Wassim.Haddad@ericsson.com

Francis Dupont
ENST Bretagne
Campus de Rennes
2, rue de la Chataigneraie
BP 78
35510 Cesson Sevigne Cedex
FRANCE
Fax: +33 2 99 12 70 30
E-Mail: Francis.Dupont@enst-bretagne.fr

Lila Madour
Ericsson Research Canada
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
CANADA
Phone: +1 514 345 7900

Haddad, et al.

Expires July 2004

[Page 13]

INTERNET-DRAFT

Binding Update Backhauling

January 2004

Fax: +1 514 345 6195
E-Mail: Lila.Madour@ericsson.com

Alan Kavanagh
Ericsson Research Canada
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
CANADA
Phone: +1 514 345 7900
Fax: +1 514 345 6195
E-Mail: Alan.Kavanagh@ericsson.com

Suresh Krishnan
Ericsson Research Canada
8400, Decarie Blvd

Town of Mount Royal
Quebec H4P 2N2
CANADA
Phone: +1 514 345 7900
Fax: +1 514 345 6195
E-Mail: Suresh.Krishnan@ericsson.com

Soohong Daniel Park
Mobile Platform Laboratory, Samsung Electronics
416. Maetan-Dong, Yeongtong-Gu, Suwon
Korea
Phone: +81 31 200 4508
E-Mail: soohong.park@samsung.com

Hannu Kari
Helsinki University of Technology
Laboratory for Theoretical Computer Science
P.O. Box 5400
FIN-02015 HUT
FINLAND
Phone: +358 9 451 2918
E-Mail: Hannu.Kari@hut.fi

13. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.
This document and translations of it may be copied and furnished
to others, and derivative works that comment on or otherwise
explain it or assist in its implementation may be prepared,
copied, published and distributed, in whole or in part, without
restriction of any kind, provided that the above copyright
notice and this paragraph are included on all such copies and
derivative works. However, this document itself may not be

modified in any way, such as by removing the copyright notice or
references to the Internet Society or other Internet
organizations, except as needed for the purpose of developing
Internet standards in which case the procedures for copyrights
defined in the Internet Standards process must be followed, or
as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Appendix A: Establishing the Bidirectional Security Association

As it has been stated in 4.3, after a successful BUB test, the two MNs MUST establish a bidirectional security association between them and generate a session key. The session key MUST be used to authenticate BUs/BAs messages exchanged between the two MNs via the path going through their two HAs. The session key MAY also be used to authenticate the CoTI/CoT messages exchanged via the direct path.

The session key is generated from a Diffie-Hellman (DH) exchange which MUST be authenticated. Such authentication MAY use the Kbm key as a pre-shared secret used to sign the DH messages. Note that the Kbm key MUST be the last key generated from the RR test (i.e., the RR test during which, the BUB test has been launched).

The DH messages exchanged between the two MNs are described in the following (for more details about the messages structure and how to generate different keys, please refer to [5]):

```

                                sid    , gX, N    , info
MN1                                MN1      MN1      MN1
----->

```

```

                                sid    , sid    , gY, N    , info
                                MN1      MN2      MN2      MN2
<-----

```

```

sid    ,sid    ,MN1,SIG (N    ,sid    ,gX,info ,info ), MAC(MN1)
MN1      MN2      Kbm  MN2  MN1      MN1      MN2      Km
----->

```

```

sid    ,sid, ,info ,MN2,SIG (N    ,sid    ,gY,info ,info),MAC(MN2)
MN1      MN2      MN2      Kbm  MN1  MN2      MN2      MN1  Km
<-----

```

In the above scheme, the following abbreviations have been adopted:

- gX = shared part of MN1's secret
- gY = shared part of MN2's secret
- sid = session identifier used to specify the ongoing session.
- N = nonce
- info = additional information carried in the protocol messages
- MN1 = Identity of MN1 (e.g., MN1's Home IP address)
- MN2 = Identity of MN2 (e.g., MN2's Home IP address)
- Kbm = key generated from the RR test
- SIG(msg) = denotes the signature of "msg" using the Kbm.
- Km = key generated from DH (known only by MN1 and MN2)
- MAC(msg) = denotes a message authenticated code computed from Km "msg" and signed by Km.

