

Internet Engineering Task Force  
Internet Draft  
Expires in October 2004

Wassim Haddad  
Lila Madour  
Jari Arkko  
Ericsson Research  
Francis Dupont  
GET/ENST Bretagne  
April 2004

## Applying Cryptographically Generated Addresses to BUB (BUB+)

[draft-haddad-mip6-cga-bub-00](#)

### 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

This memo describes a method to exploit the Cryptographically Generated Address (CGA) features in highly mobile environment. The draft introduces a new optimization to the "Binding Update Backhauling (BUB)" proposal, which eliminates the need for running a return routability (RR) procedure at the beginning

and improves its security.

## [1.](#) Introduction

The Binding Update Backhauling [[BUB](#)] proposal is a new mode, which has been designed to address scenarios involving two mobile endpoints. BUB offers a highly efficient solution, and substantially reduces the amount of signaling messages.

This draft describes a method, which incorporates the security features provided by the CGA in the BUB mode. The suggested solution adopts the same procedure described in [OMIPv6+].

## [2.](#) Terminology

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

## [3.](#) Glossary

This draft uses the Key option, the Timestamp (TiST) option, the Key Nonce Index (KeNI) option and the Shared Secret (S) bit defined [OMIPv6+]. In addition, this draft defines a new bit called the BUB (B) bit, which will be used in the BU and BA messages to test the other endpoint's willingness to switch to the BUB mode.

## [4.](#) Quick Overview of CGA

As described in [[CGA](#)] and [[Aura](#)], a Cryptographically Generated Address (CGA) is an IPv6 address in which the interface identifier is generated from hashing the address owner's public key. The address owner can then use the corresponding private key to provide a "proof of ownership" of its IPv6 address.

The CGA offers three main advantages: it makes the spoofing attack against the IPv6 address much harder, allows to sign messages with the owner's private key and does not require any additional security infrastructure.

The CGA offers a method for binding a public signature key to an IPv6 address. The binding between the public key and the address can be verified by re-computing and comparing the hash value of the public key and other parameters sent in the specific message with the interface identifier in the IPv6 address belonging to the owner. If the verification succeeds, the verifier knows that the public key in the CGA parameters is the authentic public key of the address owner. Note that an attacker can always create its own CGA address but he won't be able to spoof someone else's

CGA address since he needs to sign the message with the corresponding private key, which is supposed to be known only by the real owner.

## [5.](#) Quick Overview of BUB

BUB is a new mode, which has been especially designed to deal with scenarios involving two mobile endpoints. For this purpose, BUB uses the RR procedure defined in [\[MIPv6\]](#) to allow one MN to check the willingness of the other mobile node about switching to the BUB mode (i.e., defined as BUB procedure). After a successful BUB procedure, the two MNs compute a strong shared secret by running a Diffie-Hellman (DH) exchange. The shared secret is then used it to sign subsequent binding updates (BU) and binding acknowledgments (BA) messages.

After computing a shared secret, the RR procedure is eliminated and the two MNs exchange only BU/BA messages when switching to new links.

## [6.](#) Applying CGA to BUB

This memo assumes that the two MNs use CGAs as their home addresses. By providing a proof of ownership, incorporating CGA in the BUB mode (i.e., BUB+), allows signing the BU messages

carrying the BUB test and the BA messages carrying the shared secret with the MN's private keys. As a result, return routability tests associated with the home address can be eliminated during the initialization phase of BUB+.

In BUB+, the two MNs MUST sign with their private keys, any BU message sent with the bit "S" set, in order to create/refresh the shared secret. For this purpose, a MN SHOULD launch a BUB test in the first BU message sent to the other MN. In BUB+, launching a BUB test consists on setting the BUB "B" bit in the BU message. In response to a BUB test, the receiver MUST set the "B" bit in the BA message ONLY if it is willing to switch to the BUB mode. Otherwise, the bit MUST always be cleared.

In the following, MN1 is using its first BU message to run a BUB test in parallel with sending a request to MN2 to send a new Kbm:

MN1 sends the first BU message to MN2's home address. The BU message SHOULD go through MN2's HA and SHOULD use the new MN1's CoA as its IPv6 source address. As it has been described in [OMIPv6+], MN1 MUST insert in the first BU message a Timestamp (TiST) option and set the "S" bit and sign the message with its private key. In addition, MN1 MUST set the "B" bit. Note that

MN1 SHOULD also send its public key in the first BU message.

When MN2 receives such BU message, it MUST reply by sending a BA message on the direct path between the two MNs. If MN2 is willing to switch to the BUB mode, then, in addition to sending a shared secret and a Key Nonce Index (KeNI), it MUST set the "B" bit in the BA message and send its public key. In BUB+, MN2 MUST sign the BA message carrying a shared secret with its CGA private key and MUST encrypt the key field in the key option with MN1's public key as described in [OMIPv6+].

After receiving a BA message from MN2 with the "B" bit set, both nodes will start using the path going through the two HAs as the main path to exchange the BU messages. However, BUB+ recommends that both nodes duplicates their BU messages and send another copy on the direct path in order to reduce the latency. Note

that when duplicating the BU messages, both messages MUST carry the same sequence number. The BA messages SHOULD be exchanged only on the direct path.

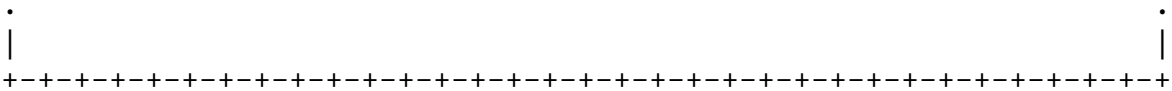
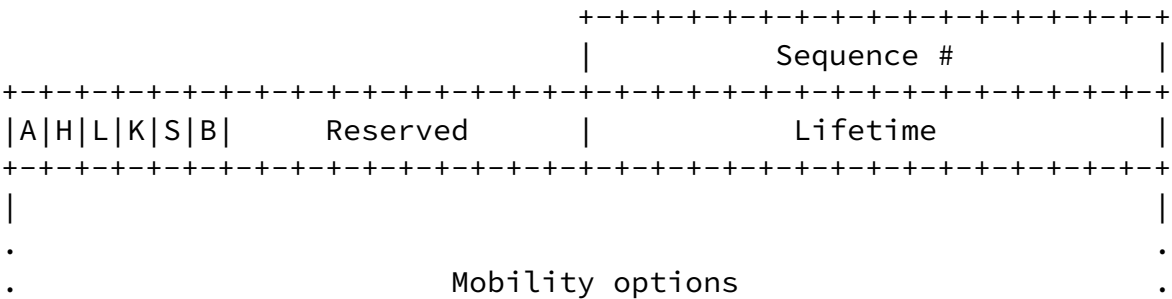
If MN2 is not willing to switch to the BUB mode, it MUST clear the "B" bit in the BA and proceed in the same way as described in [OMIPv6+]. Note that in such scenario, MN2 MUST use its private key to sign the BA message carrying a new shared secret.

A particular case arises when the two MNs exchange BU messages with the bit "S" set, at the same time. In such scenario, the two MNs' home IPv6 addresses SHOULD be compared by each MN, and only the owner of the lower address MUST create the Kbm and send it to the other endpoint.

7. The BUB (B) bit

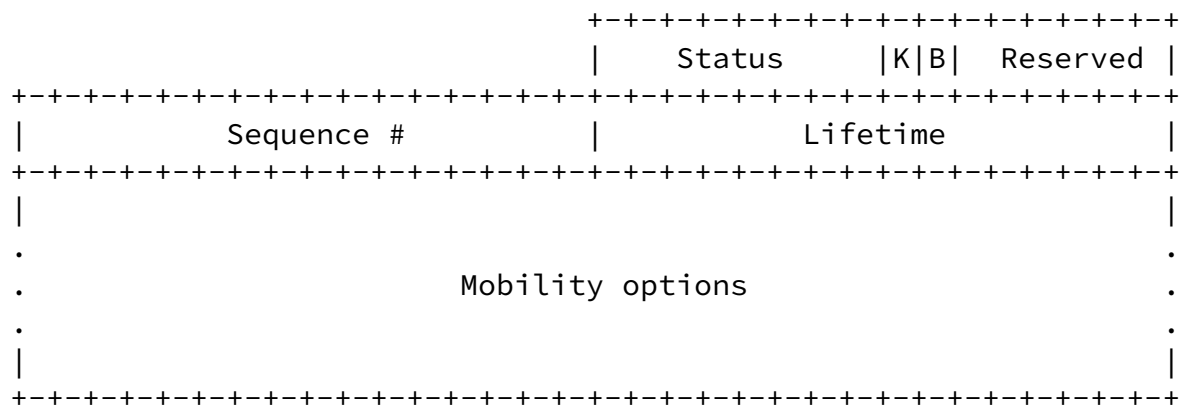
BUB+ introduces a new bit called the BUB (B) bit in the BU/BA messages, which replaces the BUB procedure used in [BUB]. This bit MUST be set only to ask the receiver about switching to the BUB mode. Otherwise, the "B" bit MUST always be cleared.

The format of the BU message with the new bit is as follows:



If the sender of the BA message is willing to switch to the BUB mode, then it MUST set the "B" bit in the BA message. Otherwise, the "B" bit MUST always be cleared.

The format of the BA message with the new bit is as follows:



## 8. Security Considerations

This memo explains how to use CGA in order to switch to the BUB mode. When both endpoints are mobile, it is recommended that both MNs agree on switching to the BUB mode after the first BUB test.

## 9. Normative References

- [MIPv6] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", [draft-ietf-mobileip-ipv6-24.txt](#), June 2003.
- [TERM] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#).

## 10. Informative References

- [Aura] Aura, T. "Cryptographically Generated Address (CGA)", 6th Information Security Conference (ISC'03), Bristol, UK, October 2003.
- [BUB] Haddad, W., Dupont, F., Kavanagh, A., Krishnan, S., Madour, L., Park, SD., "Binding Update Backhauling", [draft-haddad-mipv6-bub-01](#), Februray 2004.
- [CGA] Aura, T. "Cryptographically Generated Address (CGA)", [draft-ietf-send-cga-06](#), April, 2004.
- [OMIPv6+] Haddad, W., Arkko, J., Dupont, F., "Applying Cryptographically Generated Address (CGA) to OMIPv6", [draft-haddad-mipv6-cga-omipv6-01](#), May 2004.

INTERNET-DRAFT

Applying CGA to BUB (BUB+)

April 2004

11. Authors' Addresses

Wassim Haddad  
Ericsson Research Canada  
8400, Decarie Blvd  
Town of Mount Royal  
Quebec H4P 2N2  
Canada  
Tel: +1 514 345 7900  
Fax: +1 514 345 6105  
E-mail: Wassim.Haddad@ericsson.com

Lila Madour  
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: Lila.Madour@ericsson.com

Jari Arkko  
Ericsson Research Nomadic Laboratory  
Jorvas 02420  
Finland  
E-mail: Jari.Arkko@ericsson.com

Francis Dupont  
ENST Bretagne  
Campus de Rennes  
2, rue de la Chataigneraie  
CS 17607  
35576 Cesson-Sevigne Cedex  
FRANCE  
Fax: +33 2 99 12 70 30



#### Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list

of claimed rights.

## 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

Haddad, et al.

Expires October 2004

[Page 8]

---

INTERNET-DRAFT

Applying CGA to BUB (BUB+)

April 2004

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.

