

Mobility Optimizations
Internet-Draft
Expires: November 4, 2005

W. Haddad
L. Madour
J. Arkko
Ericsson Research
F. Dupont
GET/ENST Bretagne
May 3, 2005

Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-
OMIPv6)
draft-haddad-mip6-cga-omipv6-04

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 November 4, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This memo suggests a new and enhanced route optimization security mechanism for Mobile IPv6 (MIPv6). The primary motivation for this new mechanism is the reduction of signaling load and handoff delay. The performance improvement achieved is elimination of all signaling

while not moving, and 33% of the per-movement signaling.

Table of Contents

1.	Introduction	3
2.	Efficiency of Current Protocols	3
3.	Overview of CGA	5
4.	Protocol	6
4.1	Requirements	7
4.2	Design Rationale	7
4.3	Overview of Signaling	9
4.4	Cryptographic Calculations	11
4.5	Simultaneous Movements	12
5.	Message Formats	12
5.1	The Pre Binding Update Message	12
5.2	The Pre Binding Acknowledgement Message	14
5.3	The Pre Binding Test Message	15
5.4	The CGA Key Option	17
5.5	The Shared Key Option	17
5.6	The Keep Flow Option	18
5.7	The Extended Sequence Number Option	19
5.8	The Signature (SIG) Option	20
5.9	Status Codes	21
6.	Security Considerations	21
7.	Performance Considerations	22
8.	IANA Considerations	23
9.	References	23
9.1	Normative References	23
9.2	Informative References	24
	Authors' Addresses	25
A.	Acknowledgments	26
	Intellectual Property and Copyright Statements	27

[1.](#) Introduction

This document describes a new and enhanced route optimization (RO) security mechanism for Mobile IPv6[6], based on the Cryptographically Generated Addresses (CGAs) as described in [[11](#)]. The main goals of this protocol are the reduction of the signaling load and the handoff delay times. In addition, the protocol offers some additional security benefits.

This document is a complete specification of an optional, alternative mechanism to the standard scheme, and can be applied independently of other specifications. In particular, it does not depend on ongoing research work related to route optimization schemes, although it is conceivable that some future enhancements can be applied on top of this specification.

This rest of this document is structured as follows. [Section 2](#) discusses the performance of the current Mobile IPv6 route optimization mechanisms, and [Section 3](#) introduces the concept of CGAs. [Section 4](#) gives an overview of our new mechanism and describes its design rationale. [Section 5](#) describes detailed message formats. Finally, [Section 6](#) and [Section 7](#) analyze the security and performance properties of the mechanism.

[2.](#) Efficiency of Current Protocols

This section discusses the efficiency of the current Mobile IPv6 route optimization mechanisms.

When evaluating the impact of signaling on performance, one should take into account the whole stack and not inspect just one layer or task. For instance, if the mobile node actually moved, the Mobile IPv6 signaling would have to be compared to the link layer signaling, access control and authentication signaling, and IPv6 tasks such as router discovery, neighbor discovery, and duplicate address detection. Such other signaling introduces delays, in many cases

significantly larger delays than exists in Mobile IPv6. In this document we ignore these other delays, however, and concentrate on making the mobility signaling as efficient as possible. But given this, an improvement of, say, 50% in mobility signaling may become just 10% unless other delays are also addressed. Other optimization work is ongoing in other parts of the stack, however.

The performance of the current route optimization mechanism can be evaluated according to its impact on handover delay, the amount of bandwidth it uses per movement, the amount of bandwidth it uses when not moving, and the overhead it causes for payload traffic. These are discussed in the following:

Payload traffic overhead

The primary reason for using route optimization is to avoid routing all traffic through a home agent. We assume that this benefit is significant, particularly when two mobile nodes communicate with each other. However, an overhead is associated both with packets sent via bidirectional tunneling (tunnel) and directly (options for carrying home addresses). A more detailed analysis of the benefits and drawbacks are outside the scope of this document, however, as we concentrate on the signaling aspects only.

Latency

Basic home registration introduces a latency of zero to one roundtrips before payload traffic can flow, depending on which direction of traffic is looked at and whether the mobile node chooses to wait for an acknowledgement.

With route optimization, the combined latency is one to three roundtrips, depending again on the direction of packets and waiting for acknowledgements.

More specifically, [RFC 3775](#) allows mobile nodes to send data packets after having sent the home registration Binding Update. (If the Binding Update is lost or packets get reordered, the data packets can be lost as well. But this may happen in any case.)

Home agents and correspondent nodes can start to send data packets

once they have sent the Binding Acknowledgement. The overall latency until inbound traffic can start flow to the mobile is therefore at least 1.5 roundtrips.

[RFC 3775](#) assumes also that the home and care-of tests are run in parallel. Some implementations may perform poorly, however. We have seen implementations that do not run the home and care-of tests in parallel, resulting in an overall delay of 3.5 to 4 roundtrips. But even when parallelism is employed, the latency across the two different paths can be different. When two mobile nodes are located close to each other, the home test exchange typically takes longer than the rest of the messaging.

Bandwidth usage upon movement

As discussed in [\[12\]](#), one full run of the return routability and binding update procedures is about 376 bytes. Assuming relatively infrequent movements, for instance, every half hour, this corresponds to about 1.7 bits/second average bandwidth usage.

The situation changes when more frequent movements are assumed. Using a cell size of 100 meters and the speed of 120 km/h, there will be one movement every 3 seconds. This amounts to a constant route optimization-related signaling of about 1,000 bits/second. This can be compared to a highly compressed voice stream which typically have a rate about 10,000 to 30,000 bits/second.

Bandwidth usage when not moving

Current specifications require a periodic return routability test and the re-establishment of the binding at the correspondent node. This results in an average bandwidth of about 7 bits/second, if performed every seven minutes as required in [RFC 3775](#). While this is an insignificant bandwidth for nodes that are actually communicating, it can still represent a burden for hosts that just have the bindings ready for a possible packet but are not currently communicating. This can be problematic for hosts in standby mode, for instance.

In summary, setting up the route optimization requires some signaling and causes some latency. The latency issue is perhaps more critical than the amount of signaling. This is because internet-wide RTTs are

typically much longer (some hundreds of milliseconds) than desired latencies for real-time applications such as voice over IP (tens of milliseconds).

3. Overview of CGA

As described in [[11](#)], a Cryptographically Generated Address (CGA) is an IPv6 address, which contains a set of bits generated by hashing the IPv6 address owner's public key. Such feature allows the user 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 and allows to sign messages with the owner's private key. CGA does not require any upgrade or modification in the infrastructure.

The CGA offers a method for binding a public 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. Note that an attacker can always create its own CGA address but he will not be able to spoof someone else's address since he needs to sign the message with the corresponding private key, which is supposed to be known only by the real owner.

CGA assures that the interface identifier part of the address is correct, but does little to ensure that the node is actually reachable at that identifier and prefix. As a result, CGA needs to be employed together with a reachability test where redirection denial-of-service attacks are a concern.

Each CGA is associated with a public key and auxiliary parameters. For OMIPv6, the public key MUST be formatted as a DER-encoded [[7](#)] ASN.1 structure of the type SubjectPublicKeyInfo defined in the Internet X.509 certificate profile [[4](#)].

The CGA verification takes as input an IPv6 address and auxiliary parameters. These parameters are the following:

- o a 128-bit modifier, which can be any value,

- o a 64-bit subnet prefix, which is equal to the subnet prefix of the CGA,
- o an 8-bit collision count, which can have values 0, 1 and 2.

If the verification succeeds, the verifier knows that the public key in the CGA parameters is the authentic public key of the address owner. In order to sign a message, a node needs the CGA, the associated CGA parameters, the message and the private cryptographic key that corresponds to the public key in the CGA parameters. The node needs to use a 128 bit type tag for the message from the CGA Message Type name space. The type tag is an IANA-allocated 128 bit integer.

To sign a message, a node performs the following two steps:

1. Concatenate the 128 bit type tag (in the network byte order) and message with the type tag to the left and message to the right. The concatenation is the message to be signed in the next step.
2. Generate the RSA signature. The inputs to the generation procedure are the private key and the concatenation created in a).

[4.](#) Protocol

This section discusses first the requirements of the protocol and its design rationale. An overview of the signaling is given after this, followed by the rules regarding the cryptographic calculations and a discussion of behaviour during simultaneous movements of two mobile nodes.

[4.1](#) Requirements

The main functional requirement is that the mobile node is able to update the correspondent node with its current location. The protocol also needs to work when two mobile nodes communicate with each other. Finally, the solution must be suitable with the rest of the Mobile IPv6 protocol [\[6\]](#), including, for instance, rules on how Mobility Header messages are processed.

The desired characteristics of the protocol involve as small latency as possible upon movements, and the avoidance of signaling for non-moving hosts. Other things being equal, a protocol which uses the smallest amount of bandwidth for signaling should be chosen.

The security requirements for the protocol are discussed in more depth below:

- o Attackers should not be able to redirect communication flows of legitimate hosts to themselves, at least not beyond what is already possible in plain IPv6. This requirement applies both to ongoing and future communication flows.
- o Attackers should not be able to redirect communication flows to third parties. Otherwise, denial-of-service vulnerabilities exist; while such vulnerabilities already exist in the current Internet, we would like to avoid amplification possibilities introduced through mobility mechanisms.

Note that this requirement applies even to attackers who are themselves parties in a legitimate communication with another node.

- o Attackers should not be able to cause denial-of-service through the potentially expensive computations involved in the route optimization protocol itself.

[4.2](#) Design Rationale

The design of the protocol follows the same principles as in the original return routability protocol, but adds the following mechanisms in order to make it more efficient:

CGA

CGA provides more assurance about the correctness of claimed address than the pure use of routing paths. This makes it possible to have a significant decrease in the signaling

In addition, the public keys used in the CGA technique allow certain data to be communicated privately between the nodes, which makes some of our other techniques possible.

This technique is taken from [\[17\]](#) and [\[11\]](#), and appeared originally in [\[9\]](#) and in [\[8\]](#).

Semi-permanent security associations

CGA alone is not very efficient, due to its reliance public key computations and its need for relatively long messages. We employ semi-permanent security associations, created with the help of the CGA public keys. After an initial CGA exchange, this makes subsequent signaling efficient.

This technique appeared originally in [\[14\]](#).

Minimal address testing

CGA is unable to guarantee that a particular address is actually reachable at a given prefix. For this reason there is a need for both home and care-of address tests. However, due to the higher security of the CGA technique we can make these test much less frequent.

The home address test is necessary, because otherwise a malicious mobile node could create a CGA for the victim network prefix, request a stream of packets to its current location from a public server, and then let the binding expire. The result would be a flooding attack against the victim network. In order to avoid this, we require an initial home address test at the same time as the CGA technique is applied. Signaling on subsequent movements does not need to repeat this test, however.

This technique appeared originally in [\[14\]](#).

The care-of address test is necessary, because otherwise flooding attacks could be launched against unsuspecting third parties. This test is still performed in our protocol, though in a slightly different form than in [RFC 3775](#).

This technique appeared originally in [\[13\]](#).

Home routing while moving

Given that the per-movement signaling takes some time, mobile nodes can optionally request their traffic to be routed through their home address while this signaling is being completed.

This technique appeared originally in [\[18\]](#).

Extended Sequence Numbers

In Secure Neighbor Discovery (SEND), CGA has been applied using time stamps. However, this requires that the mobile nodes have somewhat accurate clocks. In our application the concept of sequence numbers is more appropriate, although the base Mobile IPv6 sequence numbers have to be extended. Upon initial contact the mobile node may send its current sequence number value to the correspondent node, and the mobile is expected to increase this value on every new signaling message to avoid replay attacks.

[4.3](#) Overview of Signaling

The protocol is divided into two separate cases: establishing the initial contact, and subsequent messaging. The subsequent messaging is much more efficient than the initial contact.

The initial phase can be rerun at any time, if either node loses its state, but it should be rerun at least once every 24 hours.

The following figure shows the signaling diagram for the initial contact. The options shown **MUST** be included in the messages, where conformance to this document is claimed.

1. MN to CN (via HA): Pre Binding Update
- 2a. CN to MN (via HA): Pre Binding Acknowledgement
- 2b. CN to MN (directly): Pre Binding Test
3. MN to CN (directly): Binding Update + ESN + CGA Key + SIG + BAD
4. CN to MN (directly): Binding Acknowledgment + ESN + SKey + BAD

Steps 1, 2a, and 2b implement an exchange which is needed to ensure that the home and care-of addresses are reachable. It is also needed in order to guard against CPU consumption attacks against CGA RSA computations. The correspondent node **SHOULD** reject any Pre Binding Update message carrying a home address not included in its IPv6 Destination Cache entry [\[3\]](#). This ensures that at least some communication has taken place before the exchange (see [Section 6](#) for

a discussion of the security impacts of this). Steps 2a and 2b provide keygen tokens which are used to construct a Kbm according to

the usual [RFC 3775](#) rules.

If the correspondent node does not support a Pre Binding Update, it returns a regular Binding Error. Upon receiving a Binding Error, the mobile node decides to fall back to the use of the standard return routability method or bidirectional tunneling, depending on its policy.

Step 3 is the usual Binding Update, but includes the mobile node's public key, signature, and its extended sequence number. At the same time, these three options tell the correspondent node that the mobile node supports this optimization. The Binding Authorization Data option is included as well, and protects against replay attacks..

In Step 4, the correspondent node it returns the deliver the semi-permanent security association key in the SKey option, encrypted with the mobile node's public key. It also returns the Extended Sequence Number option.

As a result of the initial procedure, the following state has been established in both nodes:

- o A standard Binding Cache Entry. The lifetime of the binding is not as severely limited as it is in standard Mobile IPv6. The maximum allowed lifetime is 24 hours.
- o The current extended sequence number value of the mobile node node.
- o A semi-permanent security association with a key, Kbmperm.
- o The public keys and other parameters (see [[11](#)]) associated with the addresses.

Security-wise, we know that the parties own their addresses (via CGA), and we have some assurance that they are at least now at the locations they claim to be (via address tests). The two endpoints MUST silently discard any Binding Update or Acknowledgement message sent and/or received, to/from any of them and not signed with the

Kbmperm and with correct Extended Sequence Number and Mobile IPv6 sequence number values. The only exception to this rule applies for the valid Binding Update messages sent by the mobile node, containing the CGA Key option.

The following figure shows the signaling diagram for subsequent movements. The options shown in brackets MAY be included and other options MUST be included in the messages.

1. MN to CN (directly): Care-of Test Init [+ ESN + KeepFlow + BAD]
2. CN to MN (directly): Care-of Test
3. MN to CN (directly): Binding Update + NI + ESN + BAD
4. CN to MN (directly): Binding Acknowledgment + ESN + BAD

Steps 1 through 2 implement the care-of address test operation; home address tests are not needed. Note that even the care of address test operation might be optimized away, if some additional mechanisms such as [\[13\]](#) or [\[19\]](#) are employed. Such mechanisms are outside the scope of this document, however.

However, Step 1 has also another purpose. Its goal is to inform the correspondent node that it is in the process of moving but has not yet completed the required signaling. If the mobile node has already lost its previous care-of address, it includes the Extended Sequence Number, KeepFlow, and Binding Authorization Data options to tell the correspondent node that its current traffic should be redirected to its home address until the Binding Update arrives. This request is secured through authenticating it with Kbmperm.

Step 3 and 4 are the Binding Update and Acknowledgement. Instead of the normal Kbm calculation, they are authenticated via Kbmperm' defined as HMAC_SHA1(care-of keygen token | Kbmperm). Note that the correspondent node will send the Binding Acknowledgment message ONLY after a successful verification of the address owner's public key and the signature in the Binding Update message. The correspondent node MUST use the extended sequence number sent in the Binding Update message to prevent against replay attacks that use past Binding Update messages.

Security-wise, at this point we know that we are still talking between the same nodes as we did in the initial contact. We have

also verified the care-of address, which assures that there's no flooding attack going on.

[4.4](#) Cryptographic Calculations

The Signature option is calculated with the mobile node's private key over the following sequence of octets:

Mobility Data = care-of address | correspondent | MH Data

Where | denotes concatenation and "correspondent" is the correspondent node's IPv6 address. Note that in case the correspondent node is mobile, correspondent refers to the correspondent node's home address.

MH Data is the content of the mobility message including the MH

Haddad, et al.

Expires November 4, 2005

[Page 11]

Internet-Draft

CGA-Base MIPv6 Optimization

May 2005

header. The Authenticator within the Binding Authorization Data option is zeroed for purposes of calculating the signature.

The RSA signature is generated by using the RSASSA-PKCS1-v1_5 [\[5\]](#) signature algorithm with the SHA-1 hash algorithm.

When the SKey option is used, the correspondent node MUST encrypt the Kbm with the MN's public key using the RSAES-PKCS1-v1_5 format [\[5\]](#).

[4.5](#) Simultaneous Movements

As specified in [RFC 3775](#) [\[6\]](#), Mobility Header messages are generally sent via the mobile node's home agent and to the peer's home address, if it is also mobile. This makes it possible for two mobile nodes to communicate even if they are moving simultaneously. (The exceptions to tunneling via the home agent are the Binding Update/Acknowledgement messages. In addition, Care-of Test and Init message are also sent directly to the current address.)

This approach is also used in this document to ensure that simultaneous movements can be achieved. That is, the Pre Binding Update message MUST be sent via the home agent and addressed to the peer's home address, if it is mobile. The Pre Binding Acknowledgment message MUST be sent via the correspondent node's home agent (if any) and addressed to the source address of the Pre Binding Update

message. The Pre Binding Test message MUST be sent via the correspondent node's home agent (again if any), but addressed to the claimed care-of address from the Pre Binding Update message.

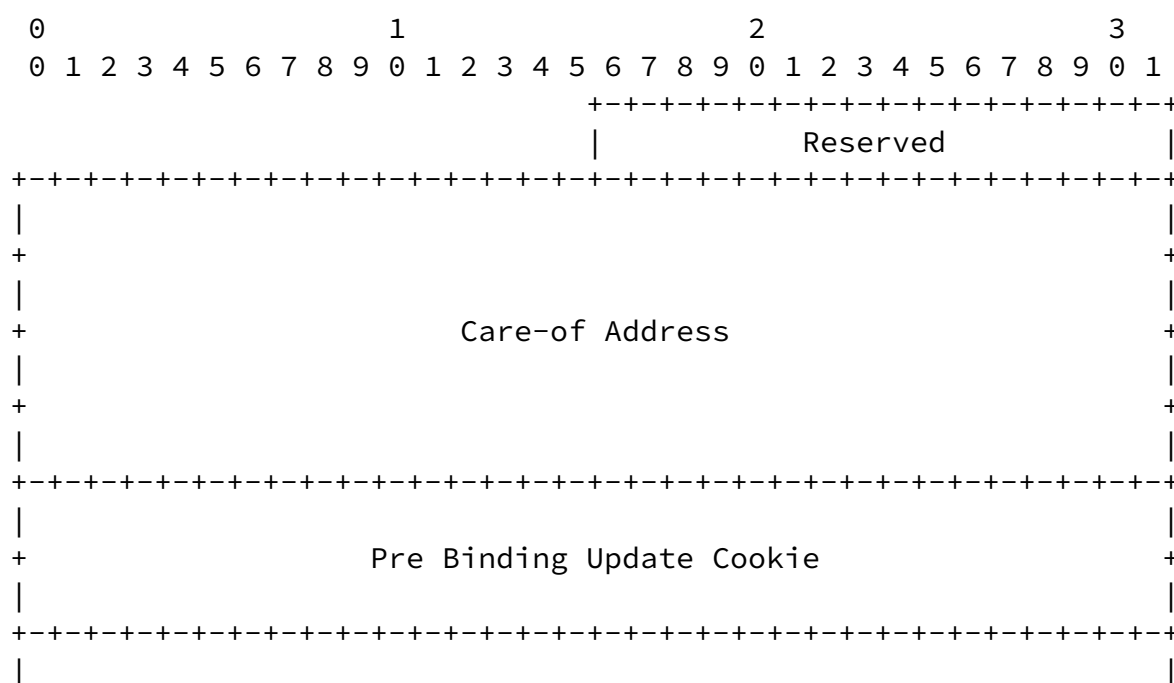
The Binding Update, Binding Acknowledgement, Care-of Test, and Care-of Test Init messages follow the rules from [RFC 3775](#).

5. Message Formats

5.1 The Pre Binding Update Message

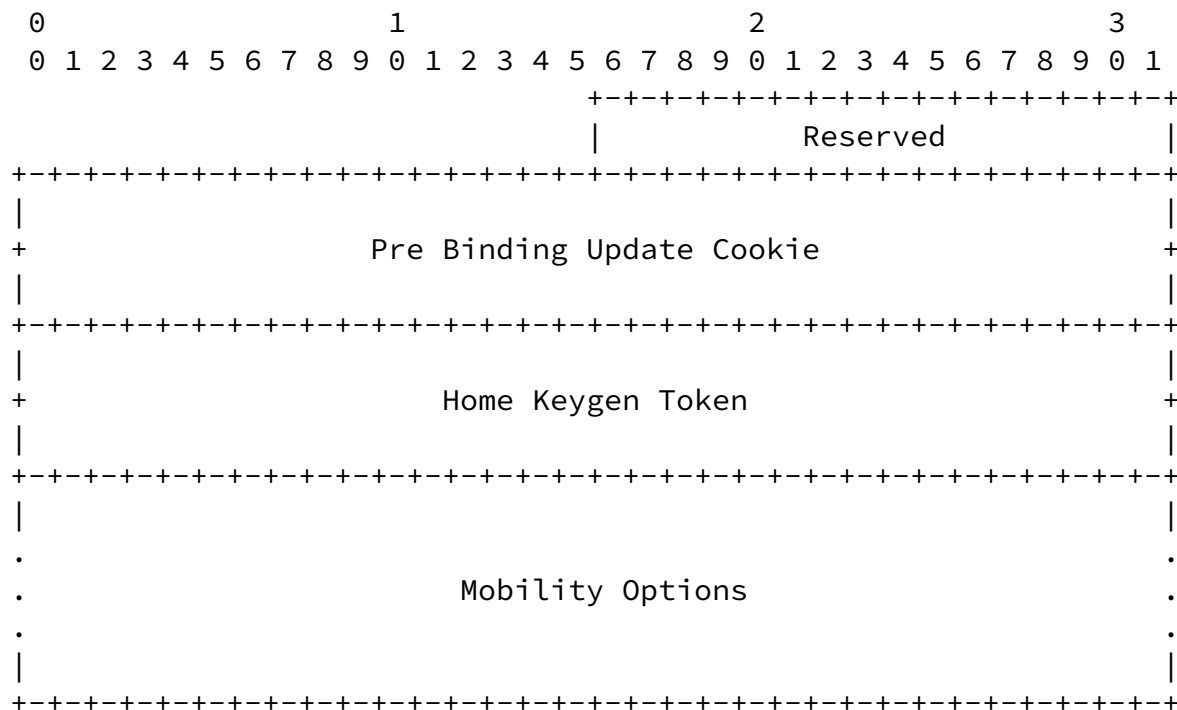
This message is similar to a Binding Update message, but does not yet establish any state at the correspondent node. The purpose of this operation is to initiate the sending of two address tests.

This message uses MH Type <To Be Assigned By IANA>. The format of the message is the following:



This message acknowledges a Pre Binding Update message. The purpose of this acknowledgement is to provide a part of the key Kbm required in the initial phase of our mechanism.

This message uses MH Type <To Be Assigned By IANA>. The format of the message is the following:



Reserved

16-bit field reserved for future use. This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Pre Binding Update Cookie

This 64-bit field contains the value from the same field in the Pre Binding Update message.

Home Keygen Token

This 64-bit field contains a Home Keygen Token, calculated as specified in [RFC 3775](#).

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for this message.

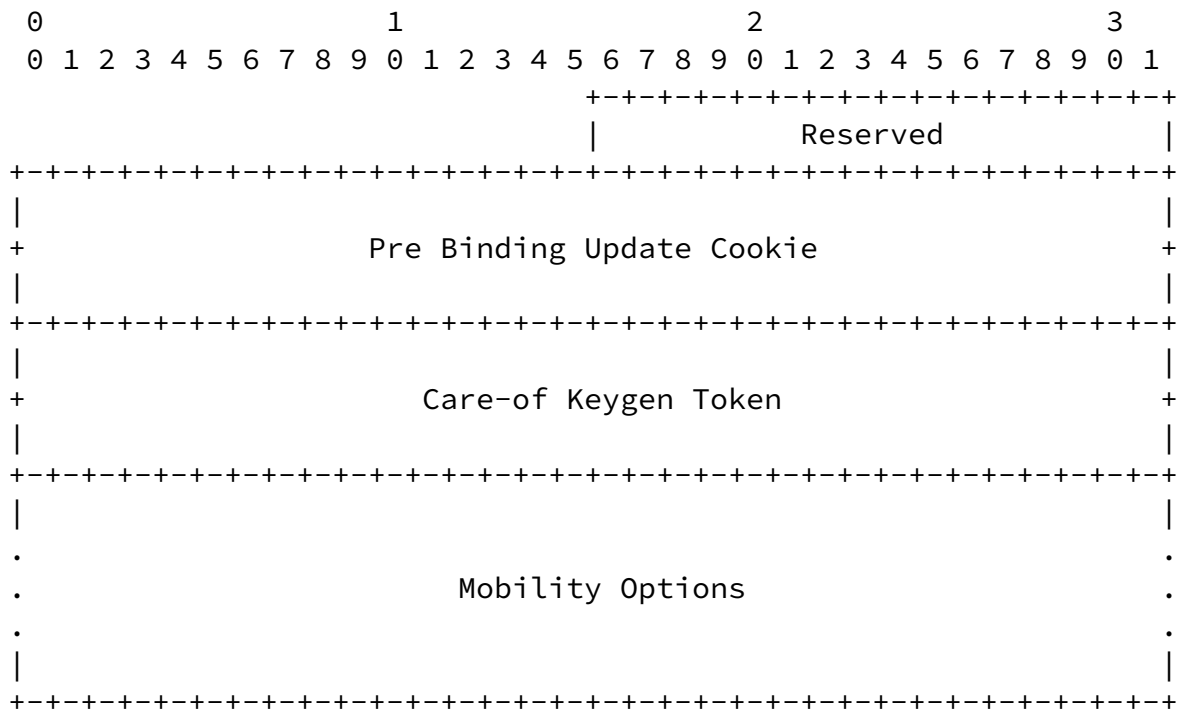
If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

This message is tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This protection is indicated by the IPsec security policy database, similarly to the protection provided for Home Test messages.

[5.3](#) The Pre Binding Test Message

This message also acknowledges a Pre Binding Update message, and ensures that the mobile node is reachable at its claimed address. The purpose of this acknowledgement is to provide the second part of the key Kbm required in the initial phase of our mechanism.

This message uses MH Type <To Be Assigned By IANA>. The format of the message is the following:



Reserved

16-bit field reserved for future use. This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Pre Binding Update Cookie

This 64-bit field contains the value from the same field in the Pre Binding Update message.

Care-of Keygen Token

This 64-bit field contains a Care-of Keygen Token, calculated as specified in [RFC 3775](#).

Mobility Options

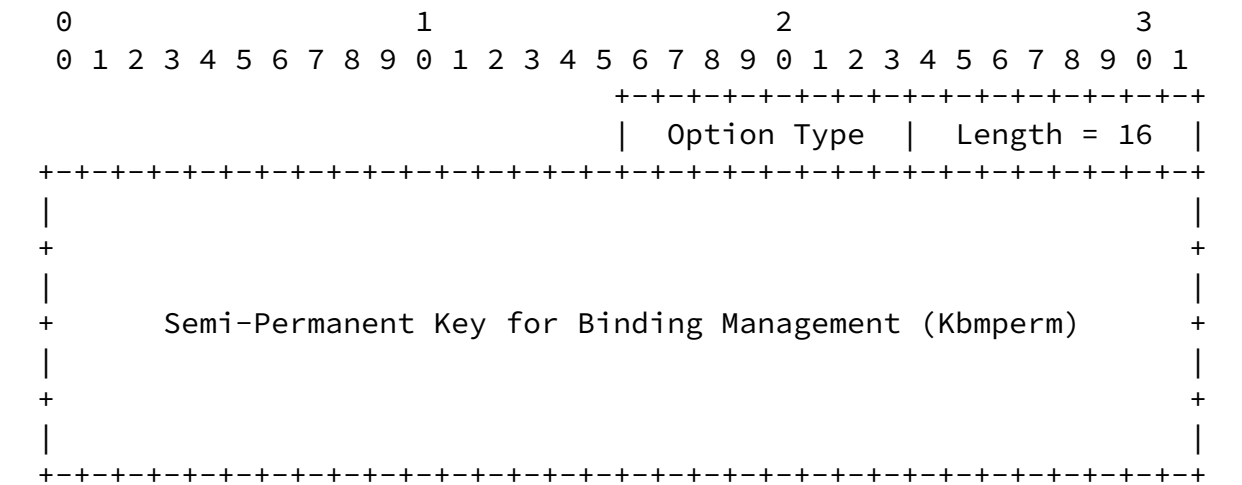
Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for this message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

As it has been mentioned above, the correspondent node **MUST** send a

new Kbm each time it receives a Binding Update message containing the CGA Parameter option. For this purpose, this proposal uses a new option called SKey option, which MUST be inserted in the Binding Acknowledgment message.

The format of the option is as follows:



Option Type

<To Be Assigned By IANA>.

Option Length

Length of the option.

Option Data

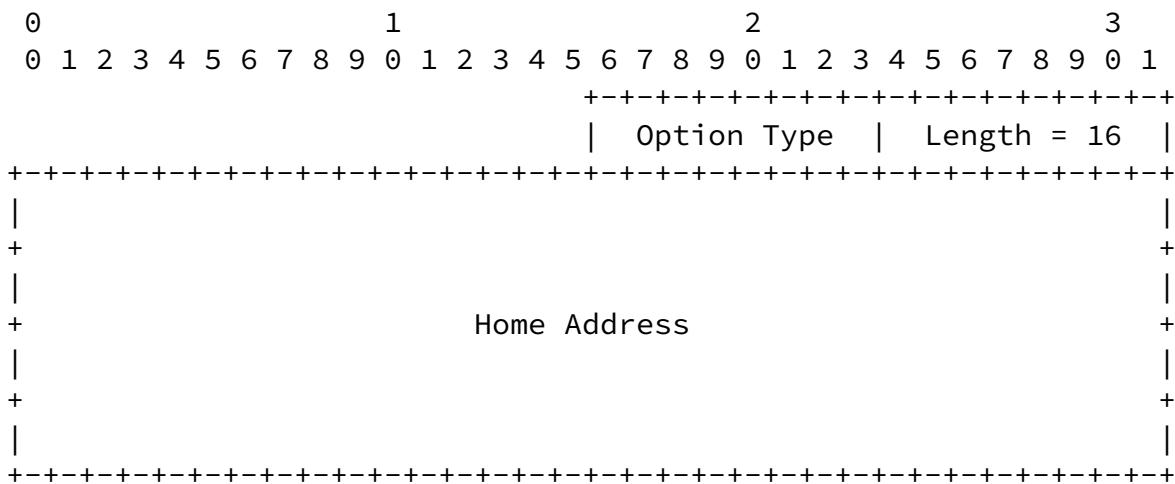
This field contains the Kbmperm value. Note that the content of this field MUST be encrypted with the mobile node's public key as defined in [Section 4.4](#). The length of Kbmperm value is 20 octets (before encryption or padding possibly involved [\[5\]](#)).

5.6 The Keep Flow Option

A mobile node which is in the process of moving may use this option

to indicate to the correspondent node that its traffic should be redirected via its home address. This option MUST always be used together with the Extended Sequence Number and Binding Authorization Data options, using the Kbmperm to authenticate the message.

The format of the option is as follows:



Option Type

<To Be Assigned By IANA>.

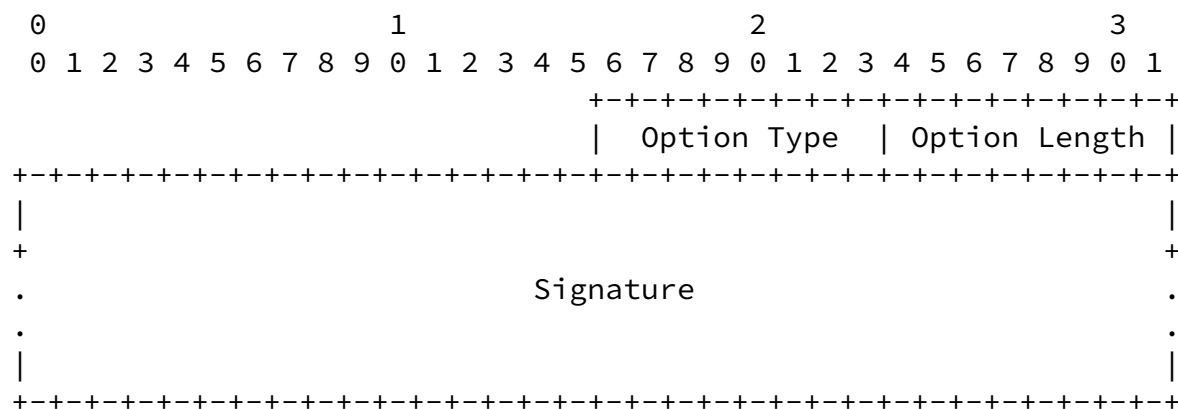
Option Length

Length of the option = 16.

Option Data

This field contains the home address of the mobile node. This address needs to be carried here, as the Care-of Test Init message

The option format is as follows:



<To Be Assigned By IANA>.

Length of the option.

This field contains the signature of the MH message it is contained within.

The following new Status codes are allocated:

Lost Kbmperm State (<To Be Allocated By IANA>)

This code is returned when the correspondent node does not have a Binding Cache Entry, Kbmperm, or has an invalid Binding Authorization Data option. The code MUST only be used in to respond to Binding Updates that contain one of the mobility options defined in this document.

6. Security Considerations

This draft describes a method to exploit the CGA features in order to authenticate route optimization signaling. In fact, the CGA replaces the authentication by providing a proof of ownership while the RR procedure replaces the authentication by a routing property.

This proof of ownership ensures that only the mobile node will be able to change the routing of packets destined to it, modulo exhaustive attacks on the CGA mechanism itself. The feasibility of such attacks and the defenses against them have been discussed in [\[11\]](#).

Note that, as specified, the proof of ownership protection applies only to the correspondent node believing the statements made by the mobile node. There is no guarantee that the answers from the correspondent node truly come from that correspondent node and not from someone who was on the path to the correspondent node during the initial contact phase. This is because we do not require correspondent nodes to have CGAs, and as a result, they can not make any statements that are authenticated in the strong sense. We chose not to protect against this, because this attack is something that already exists in plain IPv6, as is explained in the following. Lets assume that the correspondent node does not care about the IP address of the peers contacting it and that it does not protect its payload packets cryptographically. Then, a man-in-the-middle can always use its own address when communicating to the correspondent node, and the correspondent node's address when communicating to the mobile node. Philosophically, one can also argue that since the problem we attempt

to solve here is routing modifications for the mobile node's address, it is sufficient to ensure that these modifications are protected.

It should be mentioned that while the CGA can provide a protection against unauthenticated Binding Updates, it can expose the involved

nodes to denial-of-service attacks since it is computationally expensive. The draft limits the use of CGA to only the first registration and if/when re-keying is needed. In addition, it is RECOMMENDED that nodes track the amount of resources spent to the CGA processing, and disable the processing of new requests when these resources exceed a predefined limit.

The method specified in this document is secure against replay and flooding attacks, due to the introduction of the Extended Sequence Number option, the use of care-of address tests, and the use of an initial home address test.

The Pre Binding Update message handling deserves also some discussion. In contrast to existing messages in Mobile IPv6, the responses to this message will be sent to two different addresses. As such, it may be used in amplification and redirect attacks. In the following we discuss these attacks and argue that the vulnerability does not exceed the vulnerabilities already present in the current IPv6 as it is. While the Destination Cache check is a very weak test, it helps in this situation because the attacker must have sent at least one packet beforehand. Thus, the potential 1:2 amplification attack is reduced to only a 2:3 amplification. In addition, given that no serious attempt exists today to provide tracing for spoofed packets, it does not matter whether flooding attacks are direct, reflected from some node via a spoofed source address, or reflected via the Pre Binding Update message.

7. Performance Considerations

Performance of our protocol depends on whether we look at the initial or subsequent runs. The number of messages in the initial run is one less as in base Mobile IPv6, but the size of the messages is increased somewhat.

On a mobile node that does not move that often, there is a significant signaling reduction, as the lifetimes can be set higher than in return routability. For instance, a mobile node that stays in the same address for a day will get a 99.52% signaling reduction. Such long lifetimes can be achieved immediately, as opposed to methods like [\[12\]](#) that grow them gradually.

On a mobile node that moves fast, the per-movement signaling is reduced by 33%.

Latency on the initial run is not affected, but on the subsequent movements there's a significant impact. This is because the home address test is eliminated. The exact effect depends on network topology, but if the home agent is far away and the correspondent node is on the same link, latency is almost completely eliminated.

Additional latency and signaling improvements could be achieved through mechanisms that optimize the care-of address tests in some way. This is outside the scope of this document, however.

8. IANA Considerations

This document defines a new CGA Message Type name space for use as type tags in messages that may be signed using CGA signatures. The values in this name space are 128-bit unsigned integers. Values in this name space are allocated on a First Come First Served basis [2]. IANA assigns new 128-bit values directly without a review.

CGA Message Type values for private use MAY be generated with a strong random-number generator without IANA allocation.

This document defines a new 128-bit value under the CGA Message Type [11] namespace, 0x5F27 0586 8D6C 4C56 A246 9EBB 9B2A 2E13.

This document defines a set of new mobility options, which must be assigned Option Type values within the mobility option numbering space of [6]. This document also allocates a new Status code value.

9. References

9.1 Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.
- [3] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.
- [4] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 3280](#), April 2002.
- [5] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", [RFC 3447](#), February 2003.

- [6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [7] International Telecommunications Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, July 2002.

[9.2](#) Informative References

- [8] O'Shea, G. and M. Roe, "Child-proof Authentication for MIPv6", Computer Communications Review, April 2001.
- [9] Nikander, P., "Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World", Proceedings of the Cambridge Security Protocols Workshop, April 2001.
- [10] Nikander, P., "Mobile IP version 6 Route Optimization Security Design Background", [draft-ietf-mip6-ro-sec-00](#) (work in progress), April 2004.
- [11] Aura, T., "Cryptographically Generated Addresses (CGA)", [draft-ietf-send-cga-04](#) (work in progress), December 2003.
- [12] Arkko, J. and C. Vogt, "Credit-Based Authorization for Binding Lifetime Extension", [draft-arkko-mipv6-binding-lifetime-extension-00](#) (work in progress), May 2004.
- [13] Dupont, F. and J. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes", [draft-dupont-mipv6-cn-ipsec-00](#) (work in progress), April 2004.
- [14] Haddad, W. and S. Krishnan, "Optimizing Mobile IPv6 (OMIPv6)", [draft-haddad-mipv6-omipv6-01](#) (work in progress), February 2004.
- [15] Haddad, W., "Applying Cryptographically Generated Addresses to BUB (BUB+)", [draft-haddad-mip6-cga-bub-00](#) (work in progress), May 2004.
- [16] Haddad, W., "BUB: Binding Update Backhauling", [draft-haddad-mipv6-bub-01](#) (work in progress), February 2004.

- [17] Roe, M., "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", [draft-roe-mobileip-updateauth-02](#) (work in progress), March 2002.
- [18] Vogt, C., Bless, R., Doll, M., and T. Kuefner, "Early Binding

Haddad, et al.

Expires November 4, 2005

[Page 24]

Internet-Draft

CGA-Base MIPv6 Optimization

May 2005

- Updates for Mobile IPv6",
[draft-vogt-mip6-early-binding-updates-00](#) (work in progress),
February 2004.
- [19] Vogt, C., Arkko, J., Bless, R., Doll, M., and T. Kuefner,
"Credit-Based Authorization for Mobile IPv6 Early Binding
Updates", [draft-vogt-mip6-credit-based-authorization-00](#) (work
in progress), May 2004.
- [20] Perkins, C., "Preconfigured Binding Management Keys for Mobile
IPv6", [draft-ietf-mip6-precfgKbm-00](#) (work in progress),
April 2004.

Authors' Addresses

Wassim Haddad
Ericsson Research
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2, Canada

Email: wassim.haddad@ericsson.com

Lila Madour
Ericsson Research
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2, Canada

Email: lila.madour@ericsson.com

Jari Arkko

Ericsson Research
FI-02420 Jorvas
Finland

Email: jari.arkko@ericsson.com

Haddad, et al.

Expires November 4, 2005

[Page 25]

Internet-Draft

CGA-Base MIPv6 Optimization

May 2005

Francis Dupont
GET/ENST Bretagne
Campus de Rennes 2, rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Email: Francis.Dupont@enst-bretagne.fr

[Appendix A](#). Acknowledgments

The authors would like to thank Pekka Nikander, Tuomas Aura, Greg O'Shea, Mike Roe, Gabriel Montenegro, and Vesa Torvinen for interesting discussions around CGA. The authors would also like to acknowledge that [\[17\]](#) pioneered the work in the use of CGA for Mobile IPv6. Finally, we would like to thank Marcelo Bagnulo, Suresh Krishnan and Mohan Parthasarathy for their review and comments on this document.

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.

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.

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 (2005). 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.

Haddad, et al.	Expires November 4, 2005	[Page 27]
----------------	--------------------------	-----------

Internet-Draft	CGA-Base MIPv6 Optimization	May 2005
----------------	-----------------------------	----------

Acknowledgment

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

