

Network Working Group  
Internet-Draft  
Expires: January 19, 2006

H. Tschofenig  
Siemens  
W. Haddad  
Ericsson Research  
July 18, 2005

OMIPv6 Multi-Homing and Privacy  
draft-tschofenig-omipv6-multihoming-01.txt

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 January 19, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

The Optimized Mobile IPv6 with CGA (OMIPv6-CGA) protocol specifies a new route optimization (R0) to solve the mobility problem. Privacy extensions for OMIPv6 adds anonymity and unlinkability support to the OMIPv6-CGA protocol.

This document combines OMIPv6-CGA including its privacy extension with support for multi-homing. As such, it offers an efficient and

Internet-Draft

OMIPv6 Multi-Homing and Privacy

July 2005

secure multi-homing and mobility support for MIPv6 using CGAs  
including privacy support.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Assumptions . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Strawman Protocol Proposal . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Packet Format . . . . .	<a href="#">5</a>
<a href="#">5.1</a>	Alternate Care-of Address extension . . . . .	<a href="#">5</a>
<a href="#">6.</a>	Example . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">10</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">10</a>
<a href="#">9.</a>	Contributors . . . . .	<a href="#">10</a>
<a href="#">10.</a>	Open Issues . . . . .	<a href="#">10</a>
<a href="#">11.</a>	References . . . . .	<a href="#">10</a>
<a href="#">11.1</a>	Normative References . . . . .	<a href="#">10</a>
<a href="#">11.2</a>	Informative References . . . . .	<a href="#">11</a>
	Authors' Addresses . . . . .	<a href="#">12</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">13</a>

## 1. Introduction

Optimized Mobile IPv6 with CGA [[I-D.haddad-mip6-cga-omipv6](#)] protocol specifies a new route optimization (R0) to solve the mobility problem. Privacy extensions for OMIPv6 added anonymity and unlinkability support to the OMIPv6-CGA protocol.

This document combines these previously mentioned documents and adds multi-homing support. As such, it offers an efficient and secure multi-homing and mobility support for MIPv6 using CGAs with privacy support.

To provide multi-homing support based on [I-D.haddad-privacy-omipv6-anonymity] requires to deal with the following aspects:

- o Ability to inform the other peer about the peer address set
- o Ability to inform the other peer about the preferred address
- o Ability to test connectivity along a path and thereby to detect an outage situation
- o Ability to change the preferred address
- o Ability to change the peer address set

Additionally, it is worth pointing out that a new care-of address must be authorized prior to its usage. The procedure detailed in OMIPv6 [[I-D.haddad-mip6-cga-omipv6](#)] and not repeated in this document. Finally, the aspect of state indexing needs to be considered. OMIPv6 selects the Binding Cache Entry (BCE) based on the Home Address. The privacy extensions defined for OMIPv6 modify this state selection approach and use a specially generated "Sequence Value" (SQV). Since this document builds on top of the privacy extensions for OMIPv6 SQV state indexing approach is reused.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

Terms, such as peer, peer address set, path or preferred address, are reused from MOBIKE [[I-D.ietf-mobike-design](#)]. Terminology related to OMIPv6 [[I-D.haddad-mip6-cga-omipv6](#)] and its privacy extension [[I-D.haddad-privacy-omipv6-anonymity](#)] can be found in the respective documents.

### 3. Assumptions

This document makes the following assumptions:

- o The home agent (HA) is supporting multiple care of addresses since otherwise "Dynamic Home Agent Address Discovery" extensions, as proposed in [[I-D.wakikawa-mobileip-multiplecoa](#)] are needed, to query HAs for their capabilities regarding this option.
- o Implicitly selecting the preferred address by using the information from IP headers is sufficient. In contrast, [[I-D.wakikawa-mobileip-multiplecoa](#)] uses an explicit signaling mechanism based on flag in the binding update.
- o Extension to the "Alternate Care-of address" field in the Binding Update message to the CN and the HA. [[I-D.wakikawa-mobileip-multiplecoa](#)] states that registering multiple CoAs to single HA is prohibited:
  - \* "However, according to [Section 11.5.3](#) of the Mobile IPv6 specification, a mobile node is not allowed to register multiple care-of addresses bound to a single home address."
  - \* [Section 11.5.3](#) of the Mobile IPv6 RFC does not state this restriction explicitly.
- o The entire document that OMIPv6 [[I-D.haddad-mip6-cga-omipv6](#)] and its privacy extension [[I-D.haddad-privacy-omipv6-anonymity](#)] is used.

### 4. Strawman Protocol Proposal

This document requires the following protocol processing:  
Ability to inform the other peer about the peer address set:

The MN indicates support for multihoming in the Binding Update with the Alternate Care-of Address extension. This payload also indicates the available addresses.

Ability to inform the other peer about the preferred address:

The source and the destination address of a packet directly sent to the CN is the preferred address pair.

Ability to test connectivity:

Procedures for path testing need further study. This procedure ensures that a currently used path stopped working. [Editor's Note: Some words about congestion control for concurrent path tests are needed.]

Ability to change the preferred address:

The source and the destination address of a packet directly sent to the CN is the preferred address pair. As a policy the MN thereby decides about the preferred address pair being used. This allows the protocol to work if stateful packet filtering firewalls

are deployed in IPv6 networks.

Ability to change the peer address set:

The mobile node can change its peer address set at any time by sending a new Binding Update with a modified list of addresses in the Care-of Address payload.

[Editor's Note: Detailed protocol processing rules for the MN and the CN will be described in a future version of the document.]

## [5.](#) Packet Format

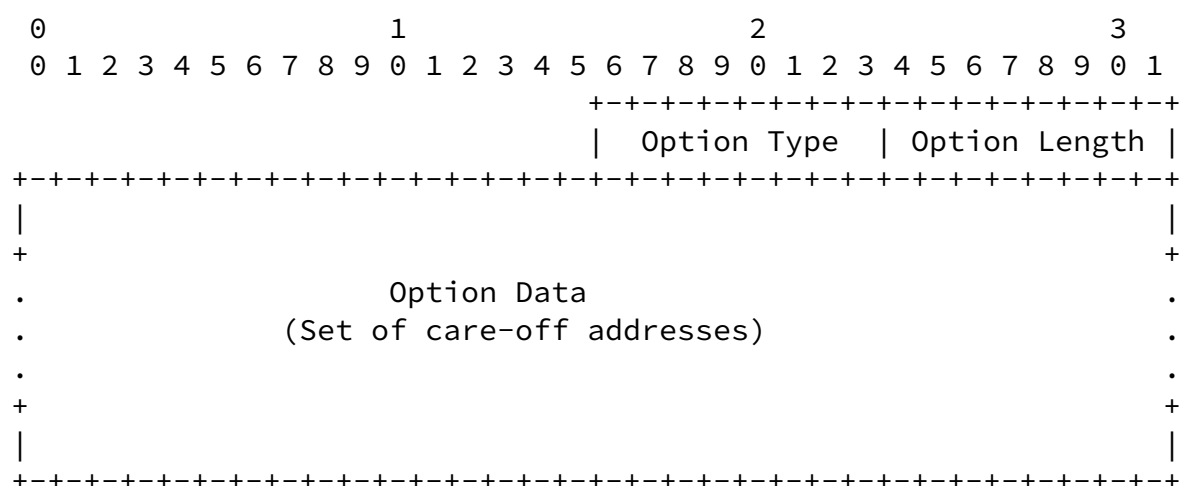
This document defines an extension for the alternate care-of address extension to carry multiple care-of address values.

### [5.1](#) Alternate Care-of Address extension

This extensions is used to carry multiple care-of addresses of the mobile node. Normally, the "Alternate Care-of Address" field can only carry a single IPv6 address. The number of CoAs can be calculated by dividing the number of bytes indicated by "Option

Length" with 16. The field should be inserted in any Binding Update message sent by the mobile node in case a mobile node wants to convey more than one care-of address. The data structure transmits all care-of addresses at once and the preferred address is implicitly selected by the source/destination pair of the data packet it is encapsulated. For any changes, adding or deleting addresses a new set of addresses will be transmitted.

The format of the option is defined as shown in Figure 1:



Option Type

<To Be Assigned By IANA>. (ADDRESS\_LIST)

#### Option Length

Length of the option.  
(Length/16 indicates the number of stored IPv6 addresses)

#### Option Data

This field contains the mobile node's care-of addresses it wishes to convey to Cn/HA.

Figure 1: Alternate Care-of Address Payload Format

As an alternative the extensions proposed in [I-D.wakikawa-mobileip-multiplecoa] could be used. This proposal is based on serial transmission of multiple CoAs and explicit signaling of preferred CoA by means of a primary flag in the Binding-Update.

For identification and selection of registered bindings, a Binding Unique Identification number (BID) is used.

A BID is selected by the MN for each CoA. Together with the HoA it is used as a selector for Binding Cache Entries.

## 6. Example

This section shows a few example message flows. The first exchange shows the usage of multiple CoAs as part of the OMIPv6 draft:

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 + CoA set + ESN + CGA Key + SIG + BAD
4. CN to MN (directly): Binding Acknowledgment + ESN + SKey + BAD
- 5a. CN to MN (via HA): Home Test remaining CoA (HoT)
- 5b. CN to MN (directly): Care-of Test remaining CoA (CoT)

The message exchanges shown in (1), (2a) and (2b) establishes the binding cache for the preferred address. The preferred address is chosen implicitly by learning the source address of the MN from the IPv6 header.

Then, in step (3) the Binding Update is performed, which transmits all remaining Care-of Addresses \_at once\_ ('CoA set' in the list) by using the extended version of the "Alternate Care-of Address" object defined in [Section 5](#).

Later, steps (5a) and (5b) are repeated for all CoAs except the preferred one. The decision when performing the address test is a matter of local policy.

Subsequent movement will then require the following message exchange to take place.

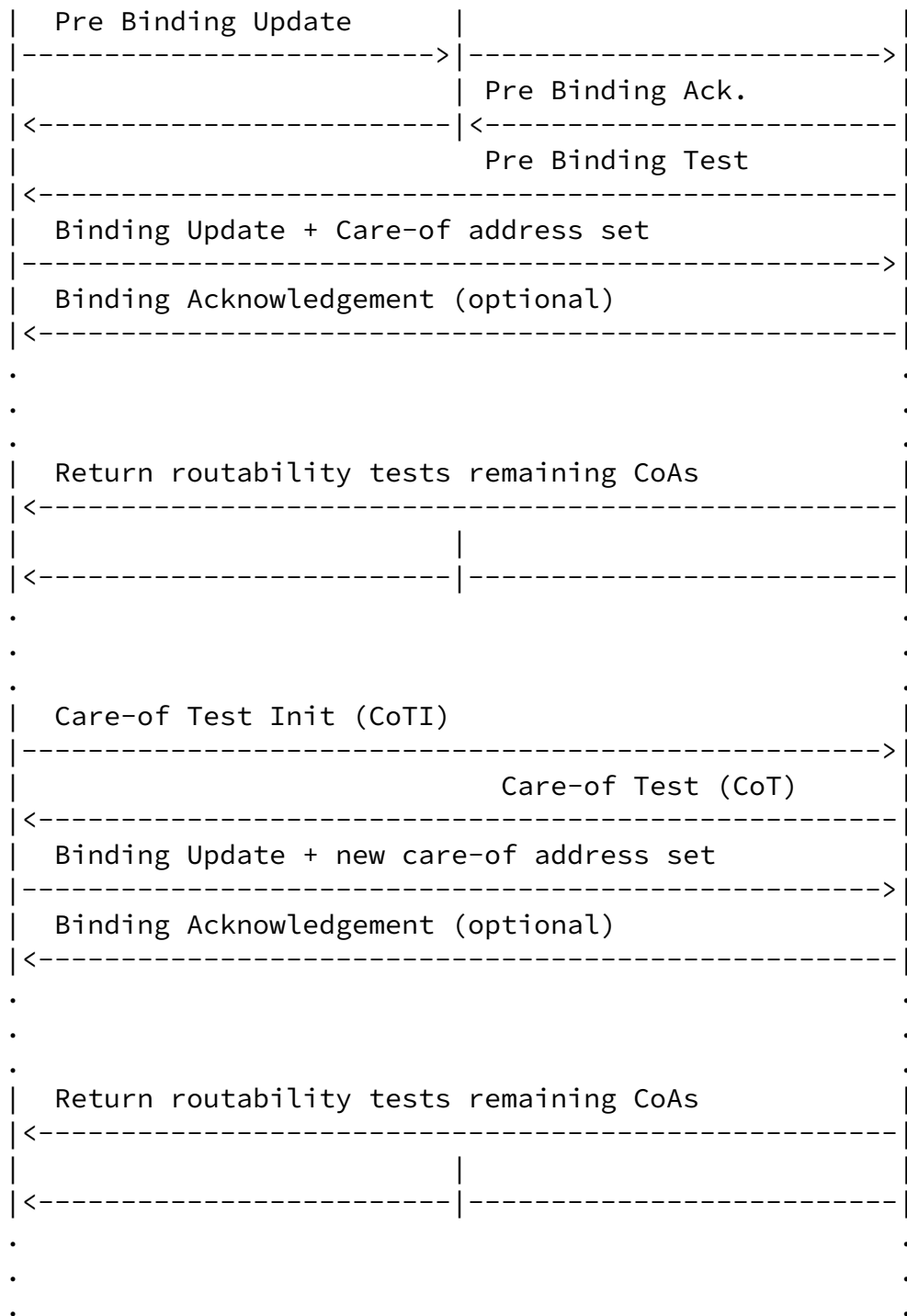
- 6. MN to CN (directly): Care-of Test Init [+ ESN + KeepFlow + BAD]
- 7. CN to MN (directly): Care-of Test
- 8. MN to CN (directly): Binding Update + new CoA set +  
+ NI + ESN + BAD
- 9. CN to MN (directly): Binding Acknowledgment + ESN + BAD
- 10a. CN to MN (via HA): Home Test remaining CoA (HoT)
- 10b. CN to MN (directly): Care-of Test remaining CoA (CoT)

Like in the initial case, the new preferred address will first be checked for return routability with steps (6) and (7). The Binding Update (8), may then contain an updated set of Care-of Addresses, which will again be acknowledged by a Binding Acknowledgment message (9).

Finally, the remaining CoAs of the CoA set are checked for return routability, which is done by messages (10a) and (10b).

Graphically, the exchange between the involved parties can be shown as follows:





As a comparison the mechanisms proposed in [I-D.wakikawa-mobileip-multiplecoa] would require the following protocol exchange to the place.

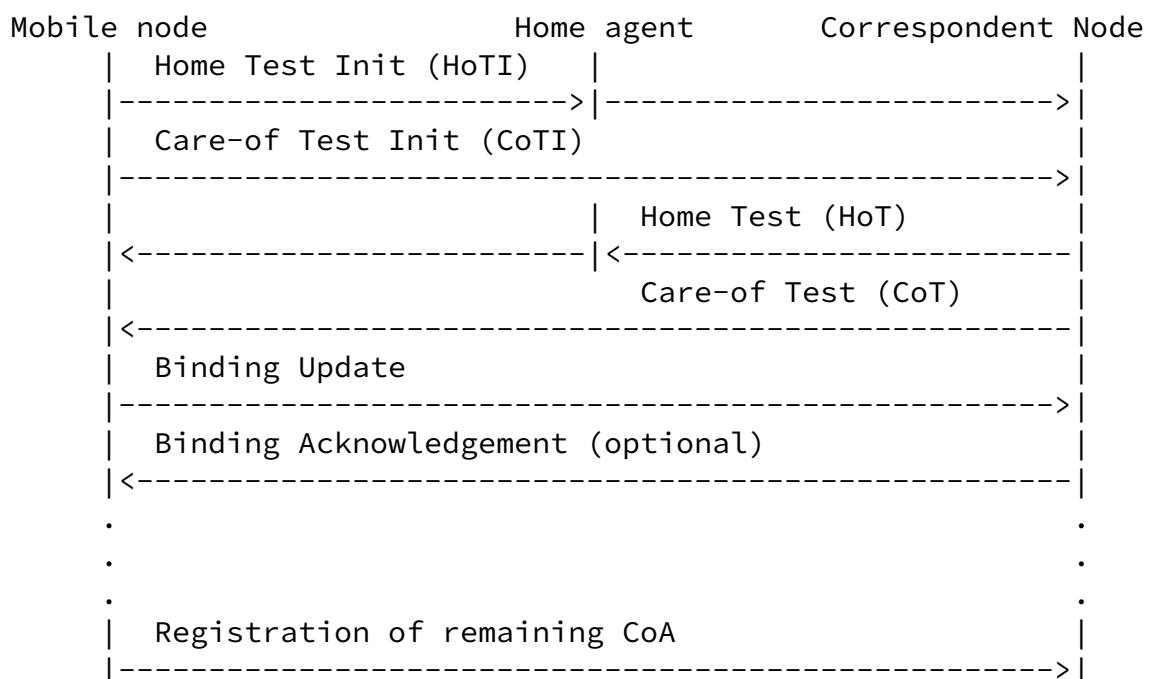
- 1a. MN to CN (via HA): Home Test Init (HoTI)
- 1b. MN to CN (directly): Care-of Test Init (CoTI)
- 2a. CN to MN (via HA): Home Test (HoT)
- 2b. CN to MN (directly): Care-of Test (CoT)
3. MN to CN (directly): Binding Update
4. CN to MN (directly): Binding Acknowledgment
5. MN to CN (directly): Registration of remaining CoA

Step (5) is repeated for all CoA except the preferred one.

The flow shown by the list above and the figure below is an extension of the one given in the Mobile IPv6 [RFC3775]. Unlike the OMIPv6 draft example, this message flow is based on two initial MN to CN messages (1a), (1b) for performing a return routability check. After receiving, the CN sends two answers back to the MN, one directly and one through the HA. (2a), (2b)

If the return routability check has succeeded, the MN sends a Binding Update message (3), which is acknowledged by an Binding Acknowledgement message from the CN (4), in case the MN signaled the request by setting the 'A' flag in the Binding Update.

The first Binding Update message also conveys the "Primary Care-of Address". Furthermore, the "Primary CoA" is marked with the 'B' flag to indicate that multiple CoA will be used by the MN. Afterwards, the MN sends all remaining CoA serially (5) to the CN, with a separate message.



.  
.

.  
.

.

.

## [7.](#) Security Considerations

The security properties of the extension defined in this document are based on the OMIPv6-CGA [[I-D.haddad-mip6-cga-omipv6](#)] and subsequently on the security of CGAs (see [[I-D.ietf-send-cga](#)]). Privacy related aspects are discussed in [[I-D.haddad-momipriv-problem-statement](#)] and in [[I-D.haddad-privacy-omipv6-anonymity](#)] and applicable to this document. Mobility specific threats, such as traffic redirecting and hijacking, third-party flooding and blackholing, are addressed by the base OMIPv6-CGA proposal.

## [8.](#) IANA Considerations

This document does not require actions by IANA.

## [9.](#) Contributors

We would like to thank Franz Muenz for his contributions to this draft.

## [10.](#) Open Issues

The aspect of multiple HoA/HAs is not addressed in this document. Registration of multiple CoA will provide benefits for the MN in a sending case. However, the CN will still have only one HoA it may choose from. For achieving goals like load balancing in both directions, i.e., spreading work load over several interfaces, a correspondent node would benefit from more than one HoA.

Another scenario which requires a change in the HoA is the battery consumption. In fact, a user may be interested for example, to switch off its 802.xx backup interface, i.e., HoA1, and switch on its CDMA2000 backup interface, i.e., HoA2, while keeping the R0 mode running on WLAN interface. Of course it will always be possible to update the HA1 with the HoA2 (as a CoA). However, applying OMIPv6 Anonymity design in such scenario can provide flexibility to do

changes on both sides: the R0 interface and eventually backup interfaces.

## [11.](#) References

### [11.1](#) Normative References

[I-D.haddad-mip6-cga-omipv6]

Haddad, W., "Applying Cryptographically Generated

Tschofenig & Haddad

Expires January 19, 2006

[Page 10]

---

Internet-Draft

OMIPv6 Multi-Homing and Privacy

July 2005

Addresses to Optimize MIPv6 (CGA-OMIPv6)",  
[draft-haddad-mip6-cga-omipv6-04](#) (work in progress),  
May 2005.

[I-D.haddad-privacy-omipv6-anonymity]

Haddad, W., "Anonymity and Unlinkability Extension for  
CGA-OMIPv6", [draft-haddad-privacy-omipv6-anonymity-00](#)  
(work in progress), June 2005.

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

### [11.2](#) Informative References

[I-D.haddad-momipriv-problem-statement]

Haddad, W., "Privacy for Mobile and Multi-homed Nodes:  
MoMiPriv Problem Statement",  
[draft-haddad-momipriv-problem-statement-01](#) (work in  
progress), February 2005.

[I-D.ietf-mobike-design]

Kivinen, T. and H. Tschofenig, "Design of the MOBIKE  
protocol", [draft-ietf-mobike-design-02](#) (work in progress),  
February 2005.

[I-D.ietf-mobike-protocol]

Eronen, P., "IKEv2 Mobility and Multihoming Protocol  
(MOBIKE)", [draft-ietf-mobike-protocol-01](#) (work in  
progress), July 2005.

[I-D.ietf-send-cga]

Aura, T., "Cryptographically Generated Addresses (CGA)",

[draft-ietf-send-cga-06](#) (work in progress), April 2004.

[I-D.wakikawa-mobileip-multiplecoa]

Wakikawa, R., "Multiple Care-of Addresses Registration",  
[draft-wakikawa-mobileip-multiplecoa-04](#) (work in progress),  
June 2005.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support  
in IPv6", [RFC 3775](#), June 2004.

Tschofenig & Haddad

Expires January 19, 2006

[Page 11]

---

Internet-Draft

OMIPv6 Multi-Homing and Privacy

July 2005

#### Authors' Addresses

Hannes Tschofenig  
Siemens  
Otto-Hahn-Ring 6  
Munich, Bavaria 81739  
Germany

Email: [Hannes.Tschofenig@siemens.com](mailto:Hannes.Tschofenig@siemens.com)

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

Phone: +1 514 345 7900 (#2334)

Email: [Wassim.Haddad@ericsson.com](mailto:Wassim.Haddad@ericsson.com)

#### 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 (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.

#### Acknowledgment

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