Network Working Group
Internet-Draft
Expires: April 13, 2008

K. Weniger
Panasonic

October 11, 2007

MIPv6 Correspondent Node-Targeted Location Privacy and Optimized Routing

draft-irtf-mobopts-mip6-cnlocpriv-00

Status of this Memo

Copyright Notice

Abstract

Mobile IPv6 does not allow a mobile node to hide its location from a correspondent node without compromising optimized routing. Hence, a mobile node has the choice: it can either get location privacy support or short packet delay, but not both at the same time. This document discusses the problem of achieving both simultaneously and specifies a solution. The solution utilizes the Mobile IPv6 bootstrapping mechanisms and does neither introduce new network entities nor changes to home agent or correspondent node implementations.

Table of Contents

1. Terminology 3
2. Introduction and Problem Definition 4
3. Applicability Statement 6
4. Related work 7
5. Changes to Mobile Node Operation 8
5.1. Route Optimization for New Sessions 8
5.2. Route Optimization for Ongoing Sessions 9
5.3. Route Optimization Mode Selection 11
5.4. Source Address Selection 11
6. Location-dependent Home Agent Discovery 12
7. Security Considerations 13
8. Acknowledgements 15
9. References 16
9.1. Normative References 16
9.2. Informative References 16
Author's Address 17
Intellectual Property and Copyright Statements 18

1. 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 [1].

General mobility terminology can be found in [5]. Terminology specific to Mobile IPv6 and Mobile IPv6 bootstrapping can be found in [2] and [6]. Additionally, the following terms are introduced:

Correspondent node-targeted location privacy: Hiding the mobile node's location from the correspondent node

Eavesdropper-targeted location privacy: Hiding the mobile node's location from nodes eavesdropping on the path between mobile node and correspondent node

IP Reachability Home Agent (IRHA): A Mobile IPv6 home agent as specified in [2] that provides IP reachability and global session continuity for the mobile node.

Home Address for IP Reachability (HoA_IR): A Mobile IPv6 home address used for IP reachability and session continuity and that is anchored at the IRHA. This home address is independent of the location of the mobile node and is disclosed to potential correspondent nodes (e.g., by publishing the address in DNS).

Optimized path: A path between mobile node and correspondent node that is shorter than the path between mobile node and correspondent node when the mobile node uses bi-directional tunneling mode to the IRHA. Note that the optimized path may be longer than the path between mobile node and correspondent node when the mobile node uses route optimization mode.

Optimized routing: Routing data packets over the optimized path

Optimized Routing Home Agent (ORHA): A Mobile IPv6 home agent as specified in [2] that is used for providing optimized routing and correspondent node-targeted location privacy. It must support the bootstrapping mechanisms specified in [3] and should be located close to the correspondent node.

Home Address for Optimized Routing (HoA_OR): A Mobile IPv6 home address used for optimized routing and session continuity that is anchored at the ORHA. This home address is typically not public (i.e., not published in DNS).

2. Introduction and Problem Definition

Location privacy is the ability to hide a user's location from other users. This is considered to be an important feature, since disclosure of the location can have serious impacts on the user's life. In general, location privacy can be achieved by hiding the relation between identity and location of a user. In Mobile IPv6 [2], the care-of address and the home address typically represent topological location and identity of a mobile node, respectively. Even though a dynamically assigned home address may not represent a permanent identity itself, a mapping to a mobile node's permanent identifiers is typically published for IP reachability reasons (e.g., in DNS). Consequently, in Mobile IPv6 at least either the care-of address or the home address must be hidden from anyone that is not authorized to obtain the location of the mobile node. Two rather orthogonal sub-problems of location privacy for Mobile IPv6 can be identified: hiding the location from eavesdroppers on the path and hiding the location from the correspondent node [7], which we henceforth call eavesdropper-targeted and correspondent node-targeted location privacy, respectively. This document is concerned with correspondent node-targeted location privacy only, especially with the problem of providing optimized routing at the same time. Eavesdropper-targeted location privacy is out of scope of this document. However, it is expected that the mechanisms defined in this document can be combined with solutions for eavesdropper-targeted location privacy such as the pseudo home address mechanisms specified in [11]. Any location privacy issues not related to Mobile IPv6 are out of the scope of this document.

An example scenario illustrating the problem addressed by this document is the following: A mobile node wants to hide its location from correspondent nodes and uses Mobile IPv6 with a public home address to be reachable. The public home address is anchored at a home agent, which we henceforth call IRHA. The mobile node requires strong location privacy, i.e., hiding only the mobility within an access network and revealing the access network prefix to the correspondent node is not acceptable. An application on the correspondent node initiates a delay-sensitive session with the mobile node such as a VoIP call by sending packets to the mobile node's public home address (HoA_IR). This requires that the correspondent node has obtained the mobile node's home address beforehand, e.g., from DNS. The mobile node receives the packets in bi-directional tunneling mode from its home agent (IRHA) and then may decide to switch to route optimization mode for the session. Let's assume the mobile node is located in the United States and the correspondent node is located in Canada, whereas the mobile node's home agent is located in Europe. Since the mobile node is far away from home, the packet delay and hence the user experience is far from

what could be achieved. However, if the mobile node uses route optimization mode, it reveals its CoA and hence its location to the correspondent node (note that the correspondent node can also be an attacker that just initiates a session to find out the mobile node's location). Consequently, the mobile node has the choice: it can either have good VoIP call quality without location privacy or location privacy with bad VoIP call quality. Currently, there is no way to achieve both simultaneously with Mobile IPv6.

This document proposes a mechanism that can provide both simultaneously, i.e., strong correspondent node-targeted location privacy and optimized routing. Home agents and correspondent node are unchanged and no new entities or messages are introduced. The basic idea is that the mobile node bootstraps with a home agent located topologically close to the correspondent node and which is used for optimized communication with this correspondent node. Such home agent is henceforth called ORHA. A home agent location close to the correspondent node ensures that the route in bi-directional tunneling mode is short and that no location information is contained in the home address, as opposed to a home address anchored at a local home agent. For mobile node-initiated sessions, the mobile node uses the ORHA in bi-directional tunneling mode and HoA_OR on higher

layers. For correspondent node-initiated sessions, the public home address HoA_IR is used on higher layers and the mobile node registers the HoA_OR as care-of address at the correspondent node.

3. Applicability Statement

The solution described in this document relies on the assignment or discovery of an home agent in the vicinity of the correspondent node or at an appropriate location that is uncorrelated with the location of the point of attachment of the mobile node. In deployment scenarios where such a home agent does not exist or if the establishment of security associations with such home agent is not feasible (e.g., because the mobile node's Mobility Service Authorizer does not have any relationship with the provider Mobility Service Provider of the home agent), this solution is not applicable. Furthermore, the mechanisms defined in this document should only be used in scenarios where the number of concurrent sessions that a mobile node runs and that require simultaneous optimized routing and correspondent node-targeted location privacy is low.

The application of the HA discovery mechanisms as specified in the MIP6 bootstrapping documents [3] [8] to ORHA discovery may pose special requirements on deployment. If the DNS-based HA discovery scheme shall be used for ORHA discovery, MSAs or MSPs should maintain DNS entries that allow the MN to discover a home agent at a specific location or in a specific domain. There are different ways to achieve that. For instance, the mobile node's MSA may maintain DNS entries per CN domain according to the scheme "_mip6._ipv6.CNdomain.MSAdomain.com" and the mobile node may be configured to construct the FQDN for ORHA discovery by appending the string "_mip6._ipv6.", CN's domain name, and MSA's domain name. If the DHCP-based HA discovery scheme [9] shall be used for ORHA discovery, the mobile node should be able to request a home agent using DHCP once a session with a new CN begins, i.e., potentially long after completion of the network authentication. Therefore, the ASP should support either storing the HA information received from the mobile node's MSA for as long as the mobile node is attached to the ASP or requesting HA information from the MSA for a specific target domain during the mobile node session (see section 4.2 of [9]).

4. Related work

Qui et. al. [11] propose a solution to the correspondent node-targeted location privacy problem. The basic idea is to hide the home address from the correspondent node in route optimization mode by using a pseudo home address instead of the real home address. Although the care-of address is revealed to the correspondent node, location privacy is protected by hiding the identity (i.e., real home

address) of the mobile node from the correspondent node. This approach has also been proposed in [10]. However, if the correspondent node initiates the communication location privacy is compromised, since the public home address and hence the identity of the mobile node is typically already known by the correspondent node. And even if the real home address can be hidden from the correspondent node, location privacy is compromised if the correspondent node is able to figure out the mobile node's identity by any other means (e.g., during the conversation of a voice call or by higher layer identifiers).

[3] and [8] specify the mechanisms for Mobile IPv6 bootstrapping in the split and the integrated scenario, respectively. They allow a mobile node to bootstrap with any home agent, for which the necessary trust relationships are in place. When bootstrapping with a local home agent, optimized routing can be achieved in bi-directional tunneling mode by using the home address pertaining to the local home agent for the session with the correspondent node. However, since the home address obtained from a local home agent belongs to the network the mobile node is currently visiting, it contains location information. Consequently, location privacy is compromised, if the correspondent node knows that the home agent is local to the mobile node (see security considerations of [3]). Although in many cases the correspondent node will not know, there are cases where the correspondent node can find out whether the mobile node's home agent is local or remote. For instance, a correspondent node may know that a mobile node's home agent is local because the mobile node's Mobility Service Provider (MSP) is known to always assign local home agents for routing efficiency reasons.

5. Changes to Mobile Node Operation

This section describes a mechanism that allows a Mobile IPv6 mobile node to achieve both correspondent node-targeted location privacy and optimized routing simultaneously. The mobile node operation is split in two cases: route optimization for new sessions (i.e., communication sessions that have not yet started) and route optimization for ongoing sessions. The first case applies, e.g., if the mobile nodes wants to initiate a session with a correspondent node and decides to optimized the route before sending the first data packets. The second case applies, e.g., if the correspondent node initiates a session with the mobile node or if the mobile node decides to optimize the route of an ongoing session. A session is defined by an application or transport layer context bound to the IP addresses of the two endpoints, with one of the addresses being the mobile node's home address to achieve session continuity.

5.1. Route Optimization for New Sessions

The mobile node first tries to discover an ORHA as described in Section 6. If the discovery is successful, the mobile node bootstraps with the ORHA, obtains a home address HoA_OR, and uses the ORHA in bi-directional tunneling mode for communication with the correspondent node. Existing registrations with other home agents can be kept for communication with other correspondent nodes. Since the mobile node can continue to use the public home address HoA_IR for IP reachability, the HoA_OR does not need to be published, i.e., no DNS update needs to be triggered for this home address. An exemplary signaling flow is shown in Figure 1.

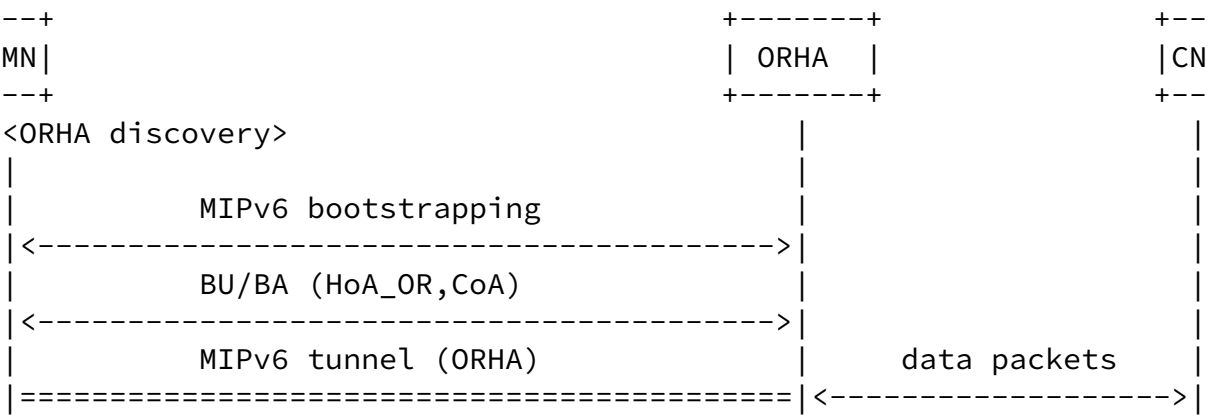

Figure 1: Signaling flow for optimizing the route for a session that has not yet started

Since HoA_OR is independent of the mobile node's location and since

HoA_OR is the only address that is revealed to the correspondent node, strong correspondent node-targeted location privacy is ensured.

5.2. Route Optimization for Ongoing Sessions

After the mobile node has decided to optimize the route of a session (e.g., after receiving the first data packets from the correspondent node tunneled through the IRHA), the mobile node tries to discover an ORHA as described in Section 6. If this is successful, it bootstraps with this ORHA and obtains HoA_OR. Since the ongoing communication session is bound to HoA_IR, packets sent by the correspondent node are still routed through the IRHA. To optimize the route without compromising location privacy, the mobile node moves the session to the ORHA. Therefore, the mobile node switches to route optimization mode and sends care-of test messages, binding update messages, and later data packets destined for the correspondent node over the reverse tunnel to the ORHA. The mobile node uses HoA_IR as home address and HoA_OR as care-of address in the context of this route optimization mode, i.e., headers of care-of test messages, binding update messages, and data packets are as follows (IPsec for signaling protection to ORHA assumed):

Care-of Test Init:

```
IPv6 header (source = care-of address,
             destination = ORHA)
ESP header in tunnel mode
IPv6 header (source = HoA_OR,
             destination = correspondent node address)
Any protocol
```

Data packets and binding updates:

```
IPv6 header (source = care-of address,
             destination = ORHA)
ESP header in tunnel mode
IPv6 header (source = HoA_OR,
             destination = correspondent node address)
Destination Options header
   Home Address option (HoA_IR)
Any protocol
```

Since HoA_OR is the mobile node's care-of address and the HoA_IR is the mobile node's home address from the correspondent node's point of view, data packets sent by the correspondent node contain the HoA_IR in the routing header and the HoA_OR in the destination address field of the IP header. Consequently, data packets sent by the correspondent node are routed to the ORHA and tunneled to the mobile node. An exemplary signaling flow is shown in Figure 2.

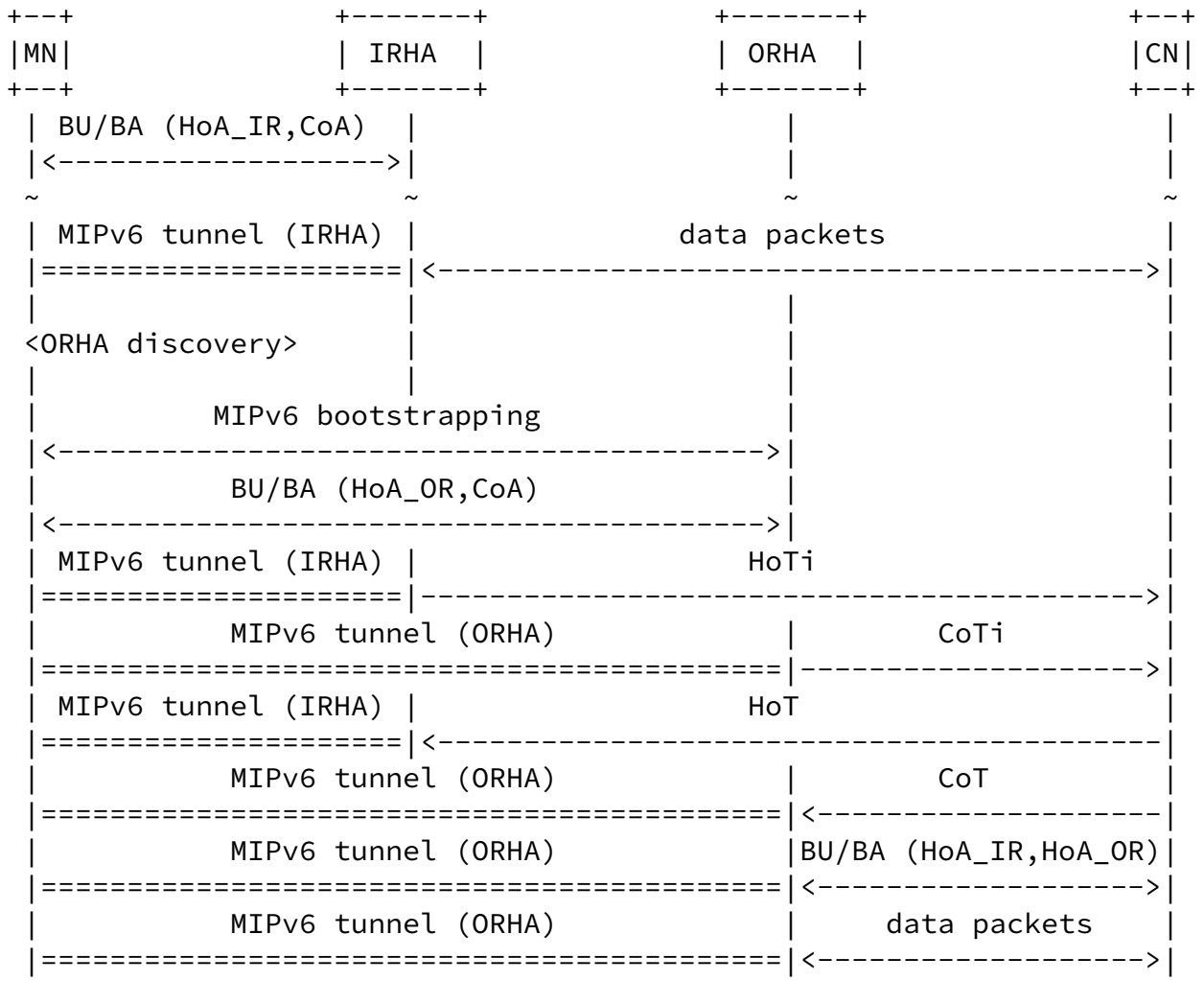

Figure 2: Signaling flow for optimization of the route for an ongoing

session

Location privacy is provided, since the correspondent node only learns HoA_OR and HoA_IR, which both do not contain any information about the mobile node's location. Optimized routing is provided as well, since all data packets exchanged between mobile node and correspondent node are routed over the ORHA, which is located close to the correspondent node.

Note that upon changing the care-of address, the mobile node does not need to send a binding update message to the correspondent node over the reverse tunnel to the ORHA, because the mobile node's care-of address in this context is the HoA_OR.

5.3. Route Optimization Mode Selection

The mobile node has to decide for every correspondent node, whether it wants to use bi-directional tunneling mode, route optimization mode or the mechanisms described in this document. How this decision is made and when route optimization according to this document is triggered is implementation specific and hence out of scope of this document. Generally, bi-directional tunneling to the home agent achieves strong correspondent node-targeted location privacy and is sufficient for non-delay-sensitive services such as simple web browsing. If no location privacy is required, Mobile IPv6 route optimization mode can be used.

Since the number of simultaneous registrations at different home agents has impacts on the overall signaling overhead and resource consumption on the mobile node, the mobile node should try to minimize the number of simultaneously used ORHAs and only apply the mechanisms specified in this document for sessions that really require simultaneous optimized routing and correspondent node-targeted location privacy.

5.4. Source Address Selection

The mobile node may use different home addresses for communication with different correspondent nodes when using the route optimization mechanisms defined in this document. Hence, the mobile node must be able to select the right home address as source address for packets

to be sent to a specific destination address. This can be achieved with the source address selection mechanisms defined in [4]. If the ORHA is located in the correspondent node's domain, the prefix of the home address anchored at the ORHA is similar to the prefix of the correspondent node and rule 9 (Use longest matching prefix) of the default source address selection [4] applies. For other cases, dynamically adding entries for HoA_OR and correspondent node address with matching labels in the policy table [4] when route optimization according to this document is triggered would prefer a home address as source address for communication with a specific correspondent node. However, since this is implementation specific, the details of the source address selection are out of the scope of this document.

6. Location-dependent Home Agent Discovery

The mechanisms defined in Section 5.1 and Section 5.2 require the discovery or assignment of a home agent (ORHA) located close to a correspondent node. One option to achieve that is to pre-configure a list of home agent FQDNs and distances to various prefixes on the mobile node. However, since the list of available home agents and the distances may change, a dynamic discovery of ORHAs is preferable. There are various ways for achieving this, some of them are described in the following.

One option is to re-use the DNS-based home agent discovery specified in [3]. The mobile node would construct the FQDN based on the correspondent node's address, prefix or host name. Some operator (e.g., MSA, ASP or MSP) should maintain DNS entries that allow the MN to discover a home agent at a specific location or in a specific domain. For instance, the mobile node's MSA may maintain DNS entries per CN domain according to the scheme "_mip6._ipv6.CNdomain.MSAdomain.com" and the mobile node may be configured to construct the FQDN for ORHA discovery by appending the string "_mip6._ipv6.", CN's domain name, and MSA's domain name.

Another option is to re-using DHCP-based HA assignment as defined in [8] and [9]. For instance, the MSA would send the home agent information for all the MSPs which the mobile node is authorized to

use to the Network Access Server (NAS) during network authentication. Once the mobile node intends to initiate route optimization according to this document, it sends a DHCP Information Request and appends a Home Network Identifier Option [9] containing the correspondent node's domain as target domain. The id-type can be set to 2 or to a new value specifically defined for ORHA discovery. The NAS would then select a home agent from the set of authorized home agents that is close to the target domain. How this selection is done is out of scope of this document. Finally, the NAS would assign the selected home agent to the mobile node in the Home Network Information Option of the DHCP reply message.

Anycast-based home agent discovery using IKEv2 [12] or DHAAD [2] is another possible solution. The mobile node would construct the anycast destination address based on the correspondent node's prefix. A drawback of this method is that it cannot discover ORHAs located close to, but outside the correspondent node's network.

Finally, the mobile node could query a dedicated server using some application-layer protocol like http. The server would maintain the list of ORHAs and would reply with the name of an ORHA upon receiving a request with a correspondent node's prefix. This server can, e.g., be provided by the MSA or a third party in the public Internet.

7. Security Considerations

The solution specified in this document ensures that a correspondent node at most learns the home addresses HoA_OR and HoA_IR of the mobile node. HoA_IR is used for IP reachability and is independent of the mobile node's movement. Hence, it doesn't contain any information about the mobile node's current location. HoA_OR is anchored at a home agent located close to the correspondent node and thus there is no relation between HoA_OR and the mobile node's current location. Consequently, the correspondent node has no way to infer the mobile node's location or movement, i.e., correspondent node-targeted location privacy is guaranteed. However, the correspondent node may wrongly believe that mobile node has moved close to himself once the mobile node bootstraps with an ORHA and moves the session from IRHA to ORHA as described in Section 5.2. However, since the decision to optimize an ongoing session is independent of the mobile node's movement, the correspondent node cannot infer anything about the mobile node's real movement patterns

from this.

An attacker could initiate many faked communication sessions with spoofed source addresses in order to trigger the mobile node to discover and bootstrap with many different ORHAs. This could consume significant resources on the mobile node and in the network and may cause a DoS. As a countermeasure, the mobile node should not start bootstrapping with a new ORHA just because it receives packets from a new correspondent node or it should limit the number of simultaneously used ORHAs. Faked sessions should be identified as such as quickly as possible and the mobile node should de-register immediately from ORHAs once a session is identified as a fake session.

The ORHA knows the location of the mobile node and could distribute it to third parties without authorization from the mobile node. Hence, the mobile node must be sure that the ORHA is trusted before the mobile node reveals its location to the ORHA. How the trust verification is done depends on the ORHA discovery mechanism in use. One option is that the MSA knows which home agents are trusted with respect to location privacy and only assigns such home agents to the mobile node. The MSA could also deny the authorization request if the MN tries to bootstrap with an untrusted home agent. Another option is that the mobile node verifies the trust by itself, e.g., by pre-configuring a list of trusted home agent addresses on the mobile node or by using certificates. Note that the fact that the ORHA and the correspondent node may be in the same administrative domain doesn't imply that the ORHA reveals the mobile node's location to the correspondent node. This is also true in today's cellular networks, where it is ensured that users of a service provided by a particular

mobile operator don't know the location of other users using a service provided by the same operator.

The return routability procedure over the reverse tunnel to the ORHA is not considered less secure than the standard return routability procedure as long as the ORHA is trusted and the ORHA link is not vulnerable to eavesdropping.

8. Acknowledgements

Thanks to Kuntal Chowdhury, Vijay Devarapalli, Rajeev Koodli, and Ahmad Muhanna for their valuable comments and suggestions to improve

this document.

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] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[3] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-07 (work in progress), July 2007.

9.2. Informative References

[4] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[5] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[6] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[7] Koodli, R., "IP Address Location Privacy and Mobile IPv6: Problem Statement", RFC 4882, May 2007.

[8] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-05 (work in progress), July 2007.

[9] Jang, H., "DHCP Option for Home Information Discovery in MIPv6", draft-ietf-mip6-hiopt-07 (work in progress), September 2007.

[10] Dupont, F., "A Simple Privacy Extension for Mobile IPv6", draft-dupont-mip6-privacyext-04 (work in progress), July 2006.

[11] Qiu, Y., "Mobile IPv6 Location Privacy Solutions", draft-irtf-mobopts-location-privacy-solutions-05 (work in progress), May 2007.

[12] Weniger, K. and F. Dupont, "IKEv2-based Home Agent Assignment in Mobile IPv6/NEMO Bootstrapping", draft-dupont-ikev2-haassign-02 (work in progress),

January 2007.

Author's Address

Kilian A. Weniger
Panasonic R&D Center Germany
Monzastr. 4c
Langen 63225
Germany

Email: kilian.weniger@eu.panasonic.com

Full Copyright Statement

Intellectual Property

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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).