James Kempf
DoCoMo Labs USA
Rajeev Koodli
Nokia Research
Center

Internet Draft
Document: draft-kempf-mipshop-handover-key-00.txt

Expires: November, 2006

June, 2006

# Distributing a Symmetric FMIPv6 Handover Key using SEND (draft-kempf-mipshop-handover-key-00.txt)

## Status of this Memo



## Abstract

Fast Mobile IPv6 requires that a Fast Binding Update is secured using a security association shared between an Access Router and a Mobile Node in order to avoid certain attacks. In this document, a method for distributing a shared key to secure this signaling is defined. The method utilizes the RSA public key that the Mobile Node used to generate its Cryptographically Generated Address in SEND. The RSA public key is used to encrypt a shared key sent from the Access Router to the Mobile Node prior to handover. The ability of the Mobile Node to decrypt the shared key verifies its possession of the private key corresponding to the CGA public key used to generate the address. This allows the Mobile Node to use the shared key to sign and authorize the routing changes triggered by the Fast Binding Update.

Table of Contents

## 1.0 Introduction

In Fast Mobile IPv6 (FMIPv6) [FMIP], a Fast Binding Update (FBU) is sent from a Mobile Node (MN), undergoing IP handover, to the previous Access Router (AR). The FBU causes a routing change so traffic sent to the MN's previous care-of address on the previous AR is tunneled to the new care-of address on the new AR. The previous AR requires that only an authorized MN be able to change the routing for the old care-of address. If such authorization is not established, an attacker can redirect a victim MN's traffic at will.

In this document, a lightweight mechanism is defined by which a key for securing FMIP can be provisioned on the MN. The mechanism utilizes the RSA public key with which the MN generates a care-of Cryptographically Generated Address (CGA) in the SEND protocol [SEND] to encrypt a shared handover key between the MN and the AR". The shared handover key itself is established between the AR and the MN at some arbitrary time prior to handover. In SEND, the CGA public key is used to authorize possession of an address, and, thereby, to perform operations associated with the address. The connection between the address and the CGA public/private key pair is called the key pair's CGA property. The shared handover key derives its authorization potential from the ability of the MN to decrypt the handover key using the CGA private key [CGA]. The timing of the handover key provisioning is independent of the handover timing, thus eliminating any potential additional latency in handover.

Handover keys are an instantiation of the purpose built key architectural principle [PBK].

## 1.1 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 RFC 2119 [RFC2119].

In addition, the following terminology is used:

CGA key Public key used to generate the CGA according to RFC 3972 [CGA].

## 2.0 Brief Review of SEND

SEND protects against a variety of threats to local link address resolution (also known as Neighbor Discovery) and last hop router (AR) discovery in IPv6 [RFC3756]. These threats are not exclusive to wireless networks, but they generally are easier to mount on certain wireless networks because the link between the access point and MN can't be physically secured.

SEND utilizes CGAs in order to secure Neighbor Discovery signaling [CGA]. Briefly, a CGA is formed by hashing together the IPv6 subnet prefix for a node's subnet, a random nonce, and an RSA public key, and the CGA key. The CGA key is used to sign a Neighbor Advertisement (NA) message sent to resolve the link layer address to the IPv6 address. The combination of the CGA and the signature on the NA proves to a receiving node the sender's authorization to claim the address. The node may opportunistically generate one or several keys specifically for SEND, or it may use a certified key that it distributes more widely.

## 3.0 Handover Key Provisioning and Use

### 3.1 Mobile Node Considerations

At some time prior to handover, the MN MUST send an IPv6 Router Solicitation (RS) [RFC2461] exactly as specified for IPv6 Router Discovery. A CGA for the MN MUST be the source address on the packet, and the MN MUST include the SEND CGA Option and SEND Signature Option with the packet, as specified in [SEND]. The MN indicates that it wants to receive a shared handover key by setting the handover authentication Algorithm Type (AT) extension field in the CGA Option (described in Section 4.2) to the MN's preferred authentication algorithm.

Receiving routers that are enabled to perform FMIPv6 with SEND handover key distribution reply directly to the CGA with a Router Advertisement (RA) including a Handover Key Option as described in the next section, containing the encrypted, shared handover key and the authentication algorithm type. The MN SHOULD choose an AR from the returned RAs, decrypt the handover key using the private key corresponding to the CGA key, and store the associated

handover key for later use along with the algorithm type. If more than one router responds to the RS, the MN MAY keep track of all such keys. The MN MUST use the returned algorithm type provided by the ARs. The MN MUST index the handover keys with the AR's IPv6

address, to which the MN later sends the FBU, and the CGA. This allows the MN to select the proper key when communicating with a previous AR.

When the MN needs to signal the previous AR using an FMIPv6 FBU, the MN MUST utilize the handover key and the corresponding authentication algorithm to generate an appropriate authenticator for the message. The MN MUST select the appropriate key for the AR using the AR's destination address and the care-of CGA. The MN MUST generate the MAC using the handover key and include it in the FBU message as defined by the FMIPv6 spec using the appropriate algorithm. As specified by FMIPv6 [FMIP], the MN MUST include the care-of CGA in a Home Address Option.

## 3.2 Access Router Considerations

When an FMIPv6 capable AR with SEND receives an RS from a MN including a SEND CGA Option with the AT field set and a Signature Option, and the source address is a CGA, the AR MUST verify the signature and CGA as described in [SEND]. If the signature and CGA verify, the AR MUST then determine whether the CGA key already has an associated shared handover key. If the CGA key has an existing handover key, the AR MUST return the existing handover key to the MN. If the CGA key does not have a shared handover key, the AR MUST construct a shared handover key as described in Section 3.3. The AR MUST encrypt the handover key with the MN's CGA key. The AR MUST insert the encrypted handover key into a Handover Key Option (described in Section 4.1) and MUST attach the Handover Key Option to the RA. The AR SHOULD set the AT field of the Handover Key Option to the MN's preferred field if it is supported; otherwise, the AR MUST select an authentication algorithm which is of equivalent strength and set the field to that. The RA is then unicast back to the MN with the CGA as the destination address. The handover key MUST be stored by the AR for future use, indexed by the CGA key and the CGA, and the authentication algorithm type recorded with the key.

If either the CGA or the signature do not verify, the AR MUST NOT include a Handover Key Option in the reply. The AR also MUST NOT change any existing key record for the address, since the message may be an attempt by an attacker to disrupt communications for a legitimate MN.

When the AR receives an FBU message containing appropriate authorization, the AR MUST find the corresponding handover key using the care-of CGA in the Home Address Option as the index. If a handover key is found, the AR MUST utilize the handover key and the appropriate algorithm to verify the MAC in the Binding Authorization Option according to the procedure described in the

FMIPv6 specification.

### 3.3 Key Generation and Lifetime

The AR MUST randomly generate a key having sufficient strength to match the authentication algorithm. The actual size of the key depends on the authentication algorithm, but should be sufficiently large to mitigate birthday attacks. Some authentication algorithms may specify a required key size. The AR MUST generate a unique key for each CGA key, and SHOULD take care that the key generation is uncorrelated between keys.

The handover key lifetime depends on the lifetime of the CGA key [CGA], which, in turn, is determined by the lifetime of the addresses generated using the CGA key. The CGA key and handover key SHOULD be renewed by the MN when the preferred lifetime of the last address generated with the CGA key expires and MUST be discarded if the valid lifetime of the last address generated with the key expires [RFC2462]. The handover key is renewed by sending a SEND-secured RS as described in Section 3.1 for one of the CGAs associated with the handover key.

Unless the MN renews the handover key with another RS, the AR MUST discard the handover key when the valid lifetime of the last CGA to be generated with the key expires. Note that CGAs generated with the CGA key for which there is an associated handover key may expire prior to the expiration of the key, if the MN does not renew the CGAs prior to the expiration of the CGAs' valid lifetime.

The AR SHOULD NOT discard the handover key immediately after use if it is still valid. It is possible that the MN may undergo rapid movement to another AR prior to the completion of Mobile IPv6 binding update on the new AR, and the MN MAY as a consequence initialize another, subsequent handover optimization to move traffic from the previous AR to another new AR. In that case, keeping the key active until the expiration of the address ensures that the MN can continue to use the handover key for FMIP signaling purposes if necessary.

If the MN returns to a previous AR prior to the expiration of the handover key, the MN MAY receive the same handover key as was previously returned, if the MN uses the same CGA key for address generation and the previous care-of CGA has not yet expired. However, the MN MUST NOT assume that it can continue to use the old key without actually receiving the handover key again from the router in an RA, regardless of how much time is left on the valid lifetime of the care-of CGAs.

### 3.4 Signaling Optimization

As described here, the signaling for handover key provisioning may require an additional RS-RA exchange beyond that used for basic IP

level movement detection [DNA]. This is because a host performing router discovery typically includes a link local IPv6 address as the source address for the RS sent to perform movement detection, and not a global IPv6 address. The care-of address, however, is a global address. Since a MN may not have the collection of prefixes

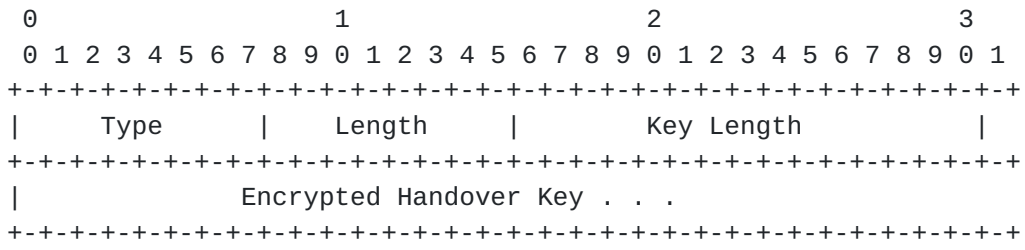
on the subnet when it sends the RS, it may not be able to generate a global IPv6 address until the RA returns with the prefixes supported on the link. While it is possible that the MN may have another source of information about prefixes supported on the link (for example, from a Proxy Router Advertisement [FMIP]), the usual case is that the MN learns these prefixes as part of the initial RS-RA exchange used to perform movement detection. If that is the case, the MN must later perform another RS-RA exchange with the MN's global care-of address as the source address of the RS, and destination address of the returned RA, in order to obtain a handover key tied to the CGA.

One possible way to eliminate the need for an additional RS-RA exchange is to tie the handover key on the MN to both the link local IPv6 address and the global IPv6 care-of addresses. However, if this is done, the same CGA key MUST be used for both the link local IPv6 address and the global IPv6 care-of addresses. If the MN requires multiple global IPv6 addresses, it MUST either utilize different subnet prefixes for the different global addresses or use a different 16 octet modifier for the CGA calculation. Note that this optimization does not affect the ability of the MN to generate privacy care-of addresses [RFC3041], since the MN can utilize a different 16 octet modifier for each address.

## 4.0 Message Formats

### 4.1 Handover Key Option

The Handover Key Option is a standard IPv6 Neighbor Discovery option in TLV format.




Fields:

Type: To be assigned by IANA.

Length: The length of the option in units of 8 octets, including the Type and Length fields.

Key Length: Length of the encrypted handover key, in units of octets.

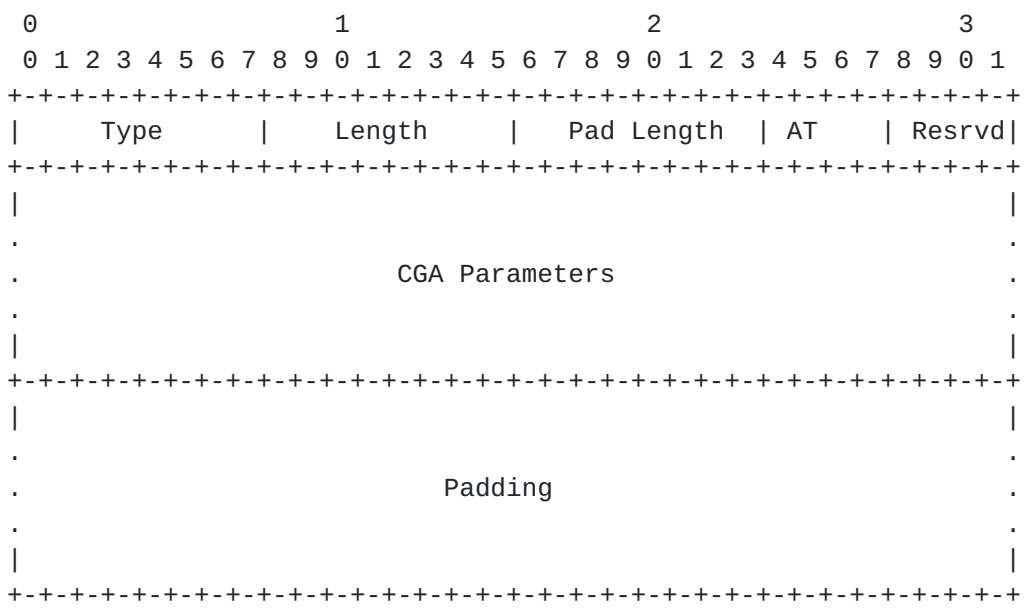
Encrypted Handover Key:

The encrypted handover key.

The option is padded to an 8 octet boundary, as required for IPv6 Neighbor Discovery Protocol options.

## 4.2 Handover Authentication Algorithm Type Field

Handover keys extend the SEND CGA Option to include an Algorithm Type (AT) field. This allows the MN to ask for and the AR to acknowledge a particular algorithm for FBU authentication.




Fields:

Type: 11

Length: The length of the option, including the Type and Length fields, in units of 8 octets.

Pad Length: The number of padding octets beyond the end of the CGA Parameters field but within the length specified by the Length field. Padding octets MUST be set to zero by senders and ignored by receivers.

AT: A 4-bit algorithm type field describing the algorithm used by FMIPv6 to calculate the authenticator. See [FMIP] for details.

Reserved: A 4-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

CGA Parameters:

A variable-length field containing the CGA Parameters data structure described in Section 4 of [CGA]. This specification requires that if both the CGA option and the RSA Signature option are

present, then the public key found from the CGA Parameters field in the CGA option MUST be that referred by the Key Hash field in the RSA Signature option. Packets received with two different keys MUST be silently discarded. Note that a future extension may provide a mechanism allowing the owner of an address and the signer to be different parties.

Padding: A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

## 5.0 Security Considerations

This document describes a key distribution protocol for the FMIPv6 handover optimization protocol. The key distribution protocol utilizes the CGA key of SEND to bootstrap a shared key for authorizing changes due to handover associated with the MN's former address on the wireless interface of the AR. General security considerations involving CGAs apply to the protocol described in this document, see [CGA] for a discussion of security considerations around CGAs.

The shared handover key is indexed by the CGA key on the AR. Multiple addresses can be generated using the same CGA key, and handover for these addresses is authorized by the same handover key. If the handover key corresponding to the CGA key used to generate the addresses is compromised, handover authorization for all addresses generated using the CGA key is also compromised. This is similar to the case when the private key corresponding to the public key used to generate the CGAs is compromised, resulting in SEND security for the CGAs being compromised. These risks can be mitigated by using different CGA keys to generate different addresses, at the expense of additional signaling to establish the handover keys.

The protocol described in this document coupled with the FBU authorization protocol described in [FMIP] provides protection against redirection of traffic on the previous AR by nodes that are not authorized to claim the previous care-of CGA. This includes nodes having authorized care-of CGAs on the previous AR's wireless link that attempt to redirect traffic for addresses for which they are not authorized. However, this protocol does not protect against redirection attacks against nodes on the new AR's link. In such an attack, the MN sends an FBU to the previous AR with its previous care-of CGA in the Home Address Option, but the address for another node as the new care-of address. The victim on the new link is them bombarded with the MN's traffic. The FMIPv6

specification [FMIP] includes a few recommendations about how to mitigate redirection attacks of this sort.

## 6.0 IANA Considerations

A new IPv6 Neighbor Discovery option, the Handover Key Option, is defined, and requires a IPv6 Neighbor Discovery option type code from IANA.

## 7.0 Normative References

[FMIP] Koodli, R., editor, "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[SEND] Arkko, J., editor, Kempf, J., Zill, B., and Nikander, P., "SEcure Neighbor Discovery (SEND)", RFC 2971, March 2005.

[CGA] Aura, T., "Cryptographically Generated Addresses", RFC 3972, March 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC3756] Nikander, P., editor, Kempf, J., and Nordmark, E., " IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RFC2461] Narten, T., and Nordmark, E., "Neighbor Discovery for IP version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] Thomas, S., and Narten, T., "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC3041] Narten, T., and Draves, R., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

## 8.0 Informative References

[DNA] Kempf, J., Narayanan, S., Nordmark, E., Pentland, B., and Choi, JH., "Detecting Network Attachment in IPv6 Networks (DNAv6)", Internet Draft, work in progress.

[PBK] Bradner, S., Mankin, A., and Schiller, J., "A Framework for Purpose-Built Keys (PBK)", Internet Draft, work in progress.

## 9.0 Author Information

James Kempf Phone: +1 408 451 4711
DoCoMo Labs USA Email: kempf@docomolabs-usa.com

181 Metro Drive
Suite 300
San Jose, CA
95110

USA

Rajeev Koodli
Nokia Research Center
313 Fairchild Drive
Mountain View, CA
94043
USA

Phone: +1 650 625 2359
Fax: +1 650 625 2502
Email: Rajeev.Koodli@nokia.com

## 10.0 IPR Statements

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.

## 11.0 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.

## 12.0 Copyright Statement

## 13.0 Acknowledgment

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