Network Working Group	S. Krishnan	
Internet-Draft	Ericsson	
Intended status: Standards Track	J. Laganier	
Expires: December 8, 2008	DoCoMo Euro-Labs	
	M. Bonola	
	Rome Tor Vergata University	
	June 06, 2008	

TOC

Secure Proxy ND Support for SEND
draft-krishnan-csi-proxy-send-00

Status of this Memo

Abstract

Secure Neighbor Discovery (SEND) specifies a method for securing Neighbor Discovery (ND) signaling against specific threats. As specified today, SEND assumes that the node advertising an address is the owner of the address and is in possession of the private key used to generate the digital signature on the message. This means that the Proxy ND signaling initiated by nodes that do not possess knowledge of the address owner's private key cannot be secured using SEND. This document extends the current SEND specification with support for Proxy ND, the Secure Proxy ND Support for SEND.

Table of Contents

1. Requirements notation

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

2. Introduction

TOC

Secure Neighbor Discovery [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.) specifies a method for securing neighbor discovery signaling [RFC4861] (Narten, T., Nordmark, E., Simpson, W., and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6),” September 2007.) against specific threats. As specified today, SEND assumes that the node advertising an address is the owner of the address and is in possession of the private key used to generate the digital signature on the message. This means that the Proxy ND signaling initiated by nodes that do not possess knowledge of the address owner's private key cannot be secured using

SEND.

This document extends the current SEND specification with support for Proxy ND. From this point on we refer to such extension as "Secure Proxy ND Support for SEND".

---

3. Terminology

TOC

Secure Proxy ND
: A node authorized to either modify or generate a SEND message without knowing the private key related to the source address of the ICMPv6 ND message.

Proxied IPv6 address
: An IPv6 address that doesn't belong to the Secure Proxy ND and for which the Secure Proxy ND is advertising.

---

4. Application Scenarios

TOC

In this section we provide three different application scenarios for which the ICMPv6 Neighbor Discovery signaling cannot be secured by using the current SEND specification.

Either of the entities described in the following three scenarios, (i.e.: ND Proxy, MIPv6 Home Agent, PMIPv6 Mobile Access Gateway) can be consider as a Secure Proxy ND.

4.1. Scenario 1: RFC 4389 Neighbor Discovery Proxy

TOC

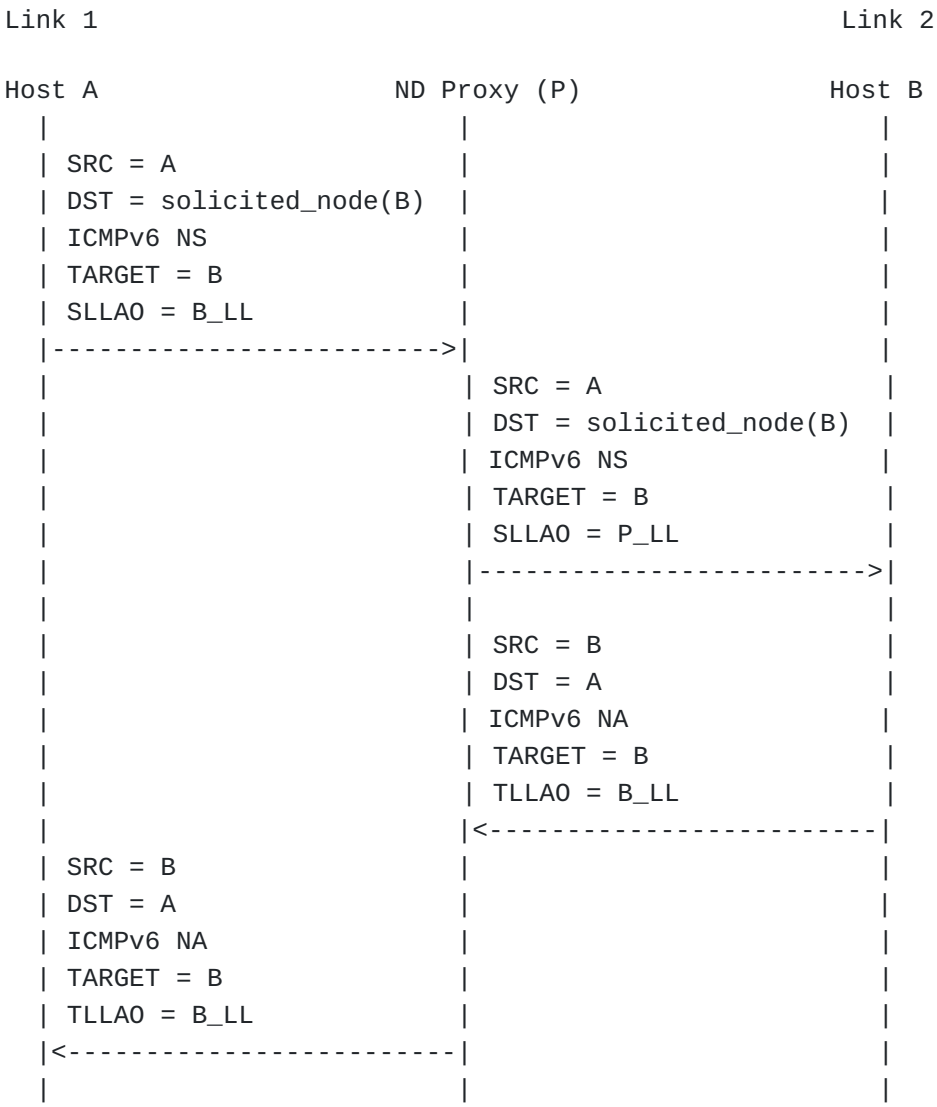

Figure 1: Proxy ND operations

[The Neighbor Discovery (ND) Proxy specification (Thaler, D., Talwar, M., and C. Patel, “Neighbor Discovery Proxies (ND Proxy),” April 2006.)] [RFC4389] provides a method by which multiple link layer segments are bridged into a single segment and specifies the IP-layer support that enables bridging under these circumstances.

A ND Proxy shall parse any IPv6 packet it receives on a proxy interface to check whether it contains one of the following ICMPv6 messages: Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Advertisement, or Redirect. Since each of these messages contains a link-layer address which might not be valid on another segment, the ND

Proxy proxies these packets as follows, and as illustrated in Figure 1 (Proxy ND operations):

1. The source link layer address will be the address of the outgoing interface.

2. The destination link layer address will be the address in the neighbor entry corresponding to the destination IPv6 address.

3. A link layer address within the payload (that is, in a Source Local Link Address option - SLLAO, or a Target Local Link Address option - TLLAO) is substituted with the link-layer address of the outgoing interface.

Moreover, when any other IPv6 unicast packet is received on a proxy interface, if it is not locally destined then it is forwarded unchanged (other than using a new link-layer header) to the proxy interface for which the next hop address appears in the neighbor cache. If no neighbor cache entry is present, the ND proxy should queue the packet and initiate a Neighbor Discovery signalling as if the ICMPv6 NS message were locally generated.

A ND proxy cannot protect proxied ND messages since protection of an ND message as per the current SEND specification requires knowledge of the private key of each node for which it is generating or forwarding a ND message on the bridged link layer segments.

4.2. Scenario 2: Mobile IPv6

TOC

The Mobile IPv6 protocol [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.) allows a mobile node (MN) to move from one link to another while maintaining reachability at a stable address, the so-called MN's home address (HoA.) When a mobile node attaches to a foreign network, all the packets sent to the MN's HoA and forwarded on the home link by a correspondent node (CN) or a router are intercepted by the home agent (HA) on that home link, encapsulated and tunneled to the mobile node's registered care-of address (CoA.)

The HA intercepts these packets by being a Neighbor Discovery proxy for this MN. When a Neighbor Solicitation (NS) is intercepted on the home link, the home agent checks if the Target address within the NS matches with any of the MN's Home Address in the Binding Cache and if so, it replies with a Neighbor Advertisement (NA) containing its own link layer address (HA_LL) as the Target Link Layer Address Option (TLLAO), as illustrated in Figure 2 (Proxy ND role of the Home agent in MIPv6).

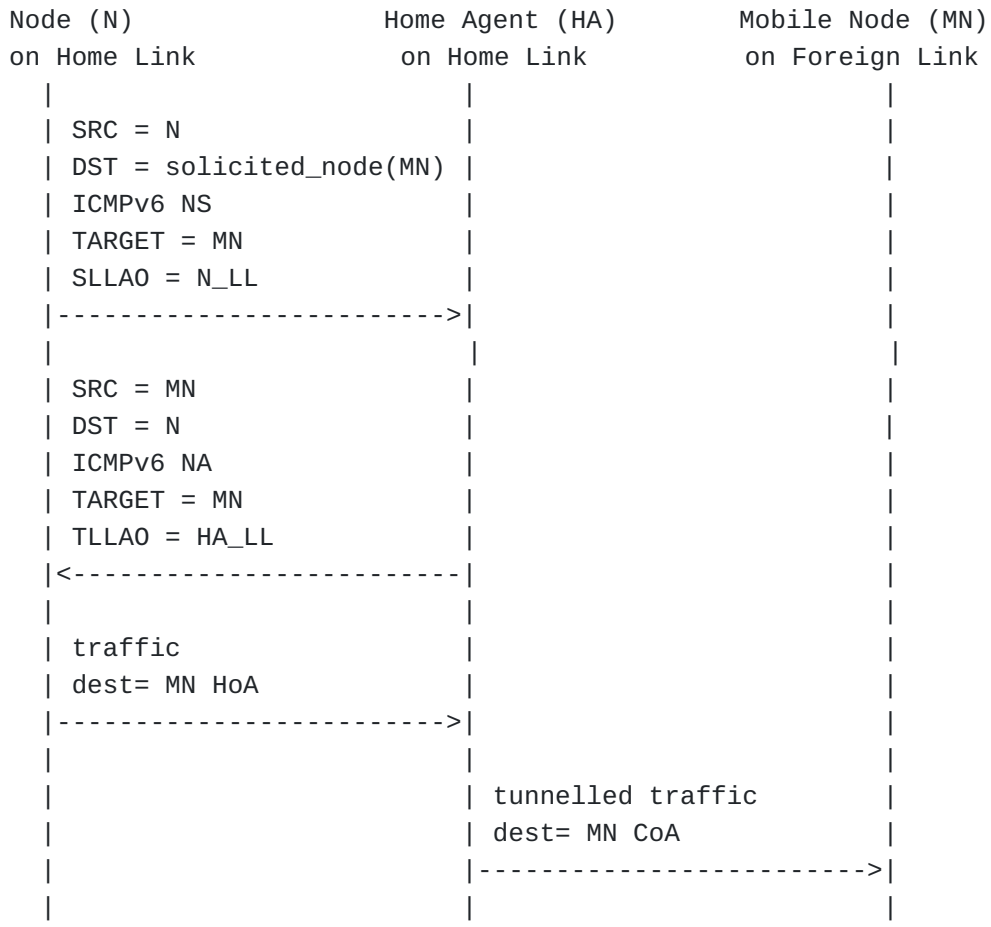

Figure 2: Proxy ND role of the Home agent in MIPv6

It is not possible to apply the current SEND specification to protect the NA message issued by the HA. To generate an ICMPv6 NA with a valid CGA option and the corresponding RSA Signature option, the HA needs knowledge of the private key related to the MN's Cryptographically Generated Address (CGA.) Any ICMPv6 NA without a valid CGA and RSA signature option is to be treated as insecure by a SEND receiver.

4.3. Scenario 3: Proxy Mobile IPv6

TOC

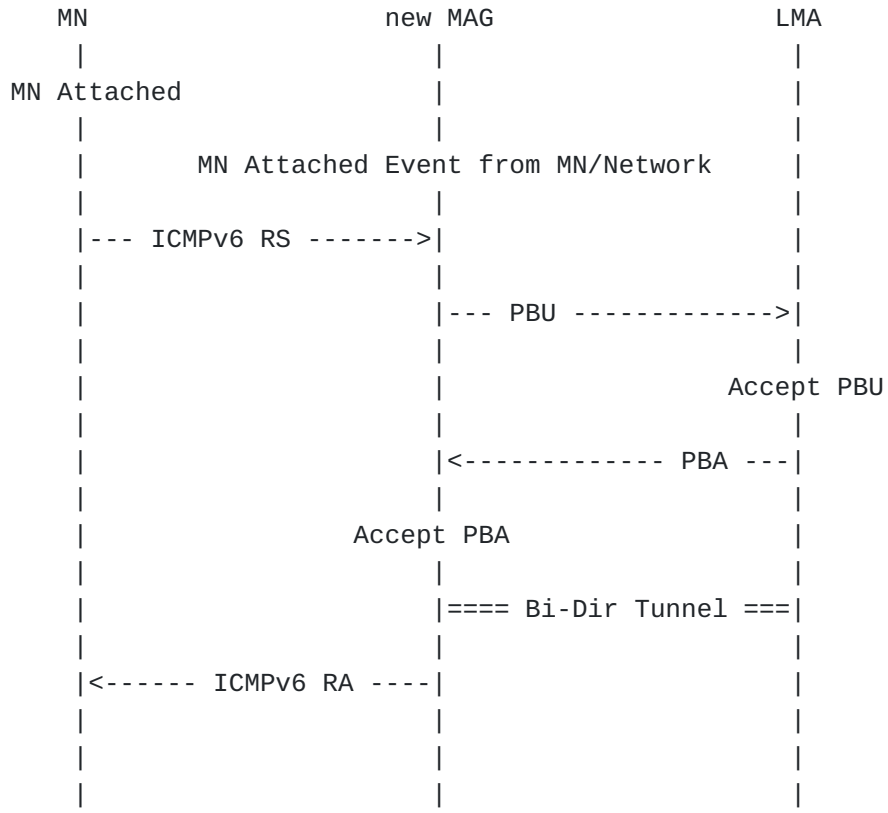

Figure 3: Mobile node's handover in PMIPv6

Proxy Mobile IPv6 [I-D.ietf-netlmm-proxymip6] (Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, “Proxy Mobile IPv6,” May 2008.) is a network-based mobility management protocol that provides an IP mobility management support for MNs without requiring MNs being involved in the mobility related signaling. The IP mobility management is totally hidden to the MN in a Proxy Mobile IPv6 domain and is performed by two functional entities: the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG.)

When the MN connects to a new access link it will send a multicast ICMPv6 Router Solicitation (RS.) The MAG on the new access link, upon detecting the MN's attachment, will signal the LMA for updating the binding state of the MN (Proxy Binding Update - PBU) and once the signaling is complete (Proxy Binding Ack - PBA - received), it will reply to the MN with a ICMPv6 Router Advertisement (RA) containing its home network prefix(es) that were assigned to that mobility session, making the MN believe it is still on the same link and not triggering the IPv6 address reconfiguration (figure Figure 3 (Mobile node's handover in PMIPv6).)

To avoid potential link-local address collisions between the MAG and the MN after a handoff to a new link, the Proxy Mobile IPv6 specification requires the MAG's link-local address configured on the link to which the MN is attached to be generated once by the LMA when the MN first attach to a PMIPv6 domain, and to be provided to the new MN's serving MAG after each handoff. Thus, from the MN's point of view, the MAG's link-local address remains constant for the duration of that MN's session.

The approach described above and the current SEND specification are incompatible since:

> Sharing the same link-local address on different MAGs would require all MAGs of a PMIPv6 domain to construct the CGA and the RSA Signature option with the same public-private key pair, which is not acceptable from a security point of view.
>
> Using different public-private key pairs on different MAGs would mean different MAGs use different CGAs as link-local address. Thus the serving MAG's link-local address changes after each handoff of the MN which is contradiction with the way MAG link-local address assignment occurs in a PMIPv6 domain.

---

5. Secure Proxy ND Overview

TOC

The original SEND specification [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.) has implicitly assumed that the owner of the address was the one who was advertising the prefix. This assumption does not allow proxying of a CGA based address as the receiver requires the advertiser to generate a valid CGA and RSA Signature option, which in turns requires possession of the public-private key pair that was used to generate the CGA.

This specification explicitly separates the roles of ownership and advertiser by extending the SEND protocol as follows:

*A certificate authorizing an entity to act as an ND proxy is introduced. This is achieved via specifying explicitly in the X509v3 certificate the purpose for which the certificate is issued, as described in a companion document [I-D.krishnan-cgaext-send-cert-eku] (Krishnan, S., Kukec, A., and K. Ahmed, “Certificate profile and certificate management for SEND,” March 2009.). Briefly, two KeyPurposeID values are defined: one for authorizing routers, and one for authorizing proxies. The inclusion of the proxy authorization value allows

the certificate owner to perform proxying of SEND messages for a set of prefixes indicated in the same certificate.

*A new option called Proxy Signature option (PSO) is defined. This option contains the key hash value of the Secure Proxy ND's public key and the digital signature computed over the SEND message. The key has value is computed over the public key within the Secure Proxy ND's certificate.

*The SEND processing rules are modified for all Neighbor Discovery messages: NA, NS, RS, RA, and Redirect. When any of these messages is received with a valid Proxy Signature option, it is considered as secure even if it doesn't contain a CGA option.

The Secure Proxy ND becomes part of the trusted infrastructure just like a SEND router. The Secure Proxy ND is granted a certificate that specifies the range of addresses for which it is allowed to perform proxying of SEND messages. Hosts can use the same process to discover the certification path between a proxy and one of the host's trust anchors as the one defined for routers in Section 6 of SEND specification (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) [RFC3971].

The proposed approach resolves the incompatibilities between the current SEND specification and the application scenarios described in Section 4 (Application Scenarios). Since SEND messages containing a Proxy Signature option are not required to carry a CGA option, the IPv6 source address is no longer cryptographically bound to the signature, and the sender of a Neighbor Discovery message is not required to be the owner of the claimed address. Thus, the Secure Proxy ND is able to either forward and generate SEND messages for a proxied address within the set of prefixes for which it is authorized.

---

6. Secure Proxy ND Specification

TOC

A Secure ND Proxy performs all the operation described in the SEND specification [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) with the addition of new processing rules to ensure that the receiving node can differentiate between an authorized proxy generating or forwarding a SEND message for a proxied address, and a malicious node doing the same.

This is accomplished by signing the message with the public key of the authorized Secure Proxy ND. The signature of the neighbor discovery proxy is included in a new option called Proxy Signature option (PSO.)

The signature is performed over all the NDP options present in the message and the PSO is appended as the last option in the message.

6.1. Proxy Signature Option

TOC

The Proxy Signature option allows public key-based signatures to be attached to NDP messages. The format of the PSO is described in the following diagram:

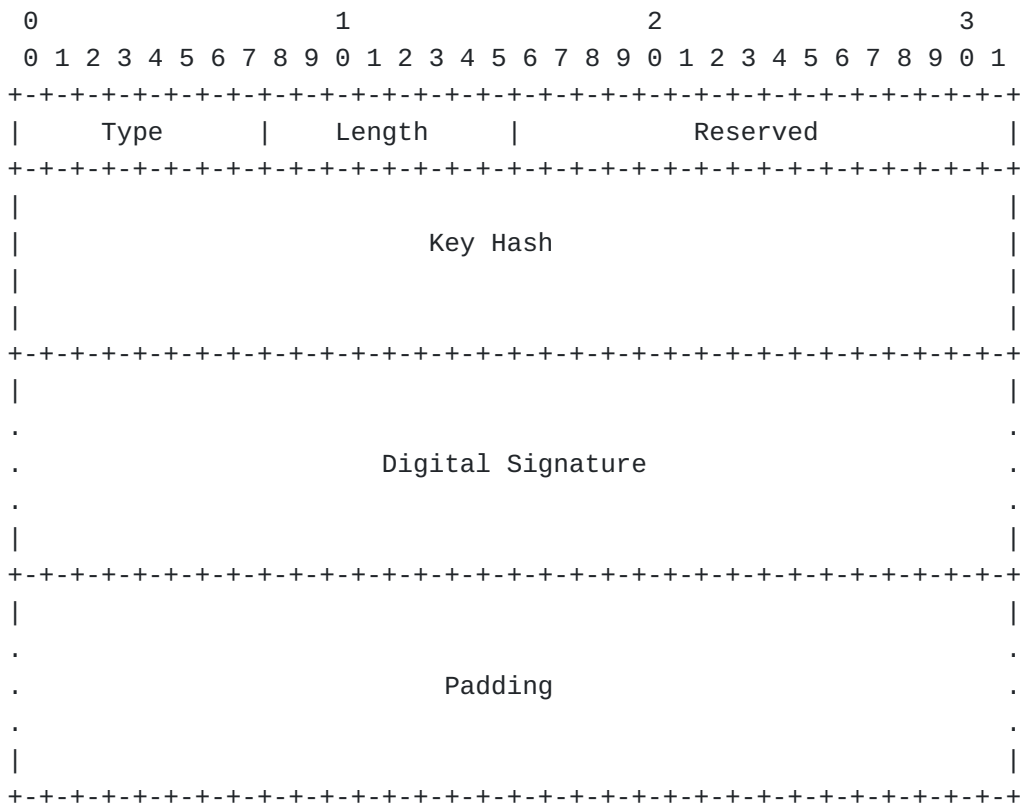

Figure 4: PSO layout

Type
TBA

Length
The length of the option (including the Type, Length, Reserved, Key Hash, Digital Signature, and Padding fields) in units of 8 octets.

Reserved

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

Key Hash

A 128-bit field containing the most significant (leftmost) 128 bits of a SHA-1 [SHA1] (National Institute of Standards and Technology, "Secure Hash Standard," April 1995.) hash of the public key used for constructing the signature. Its purpose is to associate the signature to a particular key known by the receiver. Such a key MUST be the same one within the Secure Proxy ND's certificate.

Digital Signature

A variable-length field containing a PKCS#1 v1.5 signature, constructed by using the sender's private key over the following sequence of octets:

1. The 128-bit CGA Message Type tag [RFC3972] (Aura, T., "Cryptographically Generated Addresses (CGA)," March 2005.) value for Secure Proxy ND, 0x09F5 2BE5 3B62 4C76 CB96 4E7F CDC9 2804 (The tag value has been generated randomly by the editor of this specification.)

2. The 128-bit Source Address field from the IP header.

3. The 128-bit Destination Address field from the IP header.

4. The 8-bit Type, 8-bit Code, and 16-bit Checksum fields from the ICMP header.

5. The NDP message header, starting from the octet after the ICMP Checksum field and continuing up to but not including NDP options.

6. All NDP options preceding the Proxy Signature option.

The signature value is computed with the RSASSA-PKCS1-v1_5 algorithm and SHA-1 hash, as defined in [RSA] (RSA Laboratories, "RSA Encryption Standard, Version 2.1," November 2002.).

This field starts after the Key Hash field. The length of the Digital Signature field is determined by the length of the RSA

Signature option minus the length of the other fields (including the variable length Pad field.)

Padding
This variable-length field contains padding, as many bytes long as remain after the end of the signature.

6.2. Modified SEND processing rules

TOC

The modifications described in the following section applies when a SEND message contains the Proxy Signature option (PSO), i.e. the message was sent by a Secure Proxy ND.

This specification modifies the sender and receiver processing rules for the following options defined in the SEND specification (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) [RFC3971]: CGA option, RSA option.

6.2.1. Processing rules for senders

TOC

A ICMPv6 message sent by a Secure Proxy ND for a proxied address MUST contain a Proxy Signature option (PSO) and MUST NOT contain CGA and RSA Signature options.

A Secure Proxy ND sending a SEND message with the PSO Signature option MUST construct the message as follows:

1. The SEND message is constructed without the PSO as follow:

   A. If the Secure Proxy ND is locally generating the SEND message for a proxied address, the message is constructed as described in Neighbor Discovery for IP version 6 specification [RFC4861] (Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," September 2007.).

   B. If the Secure Proxy ND is forwarding a SEND message, first the authenticity of the intercepted message is verified as specified in SEND specification [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) Section 5. If the SEND message is valid, any CGA or RSA option MUST be removed from the message. The intercepted message is

> finally modified as described in Section 4 of the ND Proxy specification [RFC4389] (Thaler, D., Talwar, M., and C. Patel, "Neighbor Discovery Proxies (ND Proxy)," April 2006.).

2. The Proxy Signature option is added as the last option in the message.

3. The data is signed as explained in Section 6.1 (Proxy Signature Option).

6.2.2. Processing rules for receivers

TOC

Any SEND message without a Proxy Signature option MUST be treated as specified in the SEND specification (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) [RFC3971].

A SEND message including a Proxy Signature option MUST be processed as specified below:

1. The receiver MUST ignore any RSA and CGA options, as well as any options that might come after the first PSO. The options are ignored for both signature verification and NDP processing purposes.

2. The Key Hash field MUST indicate the use of a known public key. A valid certification path (see [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) Section 6.3) between the receiver's trust anchor and the sender's public key MUST be known. The Secure Proxy ND's X509v3 certificate MUST contain a extended key usage extension including the KeyPurposeId value for the proxy authorization.

3. The Digital Signature field MUST have correct encoding and MUST NOT exceed the length of the Proxy Signature option minus the Padding.

4. The Digital Signature verification MUST show that the signature has been calculated as specified in Section 6.1 (Proxy Signature Option).

Messages that do not pass all the above tests MUST be silently discarded if the host has been configured to accept only secured ND messages.

7. Backward Compatibility with legacy SEND nodes

TOC

The PSO added by a Secure Proxy ND will be ignored by nodes implementing the original SEND specification and hence will not cause any interoperability problems. Since the Secure Proxy ND also removes the original RSA option, these messages will be treated as "unsecured" message as described in Section 8 "Transitions Issues" of the SEND specification (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.) [RFC3971]. Thus, this specification does not introduce any new transition issue compared to the original SEND specification.

8. Security Considerations

TOC

The mechanism described in this document introduce a new Proxy Signature Option (PSO) allowing a Secure Proxy ND to generate or modify a SEND message for a proxied address. A node will only accept such a message if it includes a valid PSO generated by an authorized Secure Proxy ND.
If, on the other hand, a message does not include a PSO, then the Secure Proxy ND support doens't introduce any further security issues since this specification does not modify the SEND processing rules if an ICMPv6 ND message does not contain a PSO. Thus, the same security considerations than that of SEND applies (cf. Section 9 of the SEND specification (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.) [RFC3971].)

9. IANA Considerations

TOC

IANA is requested to allocate:

> A new IPv6 Neighbor Discovery Option types for the PSO, as TBA. The value need to be allocated from the namespace specified in the IANA registry IPv6 NEIGHBOR DISCOVERY OPTION FORMATS located at http://www.iana.org/assignments/icmpv6-parameters.
>
> A new 128-bit value under the CGA Message Type [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) namespace, 0x09F5 2BE5 3B62 4C76 CB96 4E7F CDC9 2804.

10. Normative References

TOC

[I-D.ietf-netlmm-proxymip6]	Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, “Proxy Mobile IPv6,” draft-ietf-netlmm-proxymip6-18 (work in progress), May 2008 (TXT).
[I-D.krishnan-cgaext-send-cert-eku]	Krishnan, S., Kukec, A., and K. Ahmed, “Certificate profile and certificate management for SEND,” draft-krishnan-cgaext-send-cert-eku-03 (work in progress), March 2009 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3775]	Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” RFC 3775, June 2004 (TXT).
[RFC3971]	Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” RFC 3971, March 2005 (TXT).
[RFC3972]	Aura, T., “Cryptographically Generated Addresses (CGA),” RFC 3972, March 2005 (TXT).
[RFC4389]	Thaler, D., Talwar, M., and C. Patel, “Neighbor Discovery Proxies (ND Proxy),” RFC 4389, April 2006 (TXT).
[RFC4861]	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6),” RFC 4861, September 2007 (TXT).
[RSA]	RSA Laboratories, “RSA Encryption Standard, Version 2.1,” PKCS 1 , November 2002.
[SHA1]	National Institute of Standards and Technology, “Secure Hash Standard,” FIPS PUB 180-1 , April 1995.

Authors' Addresses

TOC

	Suresh Krishnan
	Ericsson
	8400 Decarie Blvd.
	Town of Mount Royal, QC
	Canada
Phone:	+1 514 345 7900 x42871
Email:	suresh.krishnan@ericsson.com
	Julien Laganier
	DoCoMo Communications Laboratories Europe GmbH
	Landsberger Strasse 312

	Munich D-80687
	Germany
Phone:	+49 89 56824 231
Email:	julien.ietf@laposte.net
URI:	http://www.docomolab-euro.com/
	Marco Bonola
	Rome Tor Vergata University
	Via del Politecnico, 1
	Rome I-00133
	Italy
Phone:	
Email:	marco.bonola@gmail.com

Full Copyright Statement

TOC

Intellectual Property

standard. Please address the information to the IETF at ietf-ipr@ietf.org.