Secure Proxy ND Support for SEND
draft-ietf-csi-proxy-send-03

Abstract

Secure Neighbor Discovery (SEND) specifies a method for securing Neighbor Discovery (ND) signaling against specific threats. As defined today, SEND assumes that the node sending a ND message is the owner of the address from which the message is sent, so that it is in possession of the private key used to generate the digital signature on the message. This means that the Proxy ND signaling performed 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 in order to secure Proxy ND operation.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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 September 23, 2010.
1. Requirements notation

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].
2. Introduction

Secure Neighbor Discovery (SEND) [RFC3971] specifies a method for securing Neighbor Discovery (ND) signaling [RFC4861] against specific threats. As defined today, SEND assumes that the node sending a ND message is the owner of the address from which the message is sent, so that it is in possession of the private key used to generate the digital signature on the message. This means that the Proxy ND signaling performed 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

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 does not belong to the Secure Proxy ND and for which the Secure Proxy ND is performing advertisements.

Non-SEND node

An IPv6 node that does not implement the SEND [RFC3971] specification but uses only the ND protocol defined in [RFC4861] and [RFC4862], without security.

RFC3971 node

An IPv6 node that does not implement the specification defined in this document for Secure Proxy ND support, but uses only the SEND specification as defined in [RFC3971].

SPND node

An IPv6 node that implements the specification defined in this document for Secure Proxy ND support.
4. Secure Proxy ND Overview

The original SEND specification [RFC3971] has implicitly assumed that only the node sending a ND message is the owner of the address from which the message is sent. This assumption does not allow proxying of ND messages since the advertiser is required to generate a valid RSA Signature option, which in turns requires possession of the public-private key pair that was used to generate a CGA, or that was associated to a router certificate.

To be able to separate the roles of ownership and advertiser the following extensions to the SEND protocol are defined:

- A Secure Proxy ND certificate, which is a certificate authorizing an entity to act as an ND proxy. It is a X509v3 certificate in which the purpose for which the certificate is issued has been specified explicitly as described in a companion document [I-D.ietf-csi-send-cert]. Briefly, a KeyPurposeId value is defined for authorizing proxies. The inclusion of the proxy authorization value allows the certificate owner to perform proxying of SEND messages for a range of addresses indicated in the same certificate. This certificate can be exchanged through the Authorization Delegation Discovery process defined in [RFC3971].

- A new Neighbor Discovery option called Proxy Signature option (PSO). This option contains the hash value of the public key of the proxy, and the digital signature of the SEND message computed with the private key of the proxy. The hash of the public key of the proxy is computed over the public key contained in the Secure Proxy ND’s certificate. When a ND message contains a PSO, it MUST NOT contain CGA and RSA Signature options. This option can be appended to any ND message: NA, NS, RS, RA and Redirect.

- A modification of the SEND processing rules for all ND messages: NA, NS, RS, RA, and Redirect. When any of these messages containing a valid Proxy Signature option is validated, it is considered as secure.

These extensions are applied in the following way:

- A Secure Proxy ND which proxies ND messages on behalf of a node can use the PSO option to protect the proxied messages. This Secure Proxy ND becomes part of the trusted infrastructure just like a SEND router.

- In order to allow nodes to successfully validate secured proxied messages, the nodes must be aware of the Secure Proxy ND.
certificate (in the format described in [I-D.ietf-csi-send-cert]) and must apply the modified processing rules specified in this document. We call these nodes ‘SPND nodes’. Note that the rules for generating ND messages in SPND nodes do not change, so these nodes behave as defined in [RFC3971] for sending ND messages.

To allow SPND nodes to know the certificate path required to validate the public key of the proxy, devices responding to CPS (Certification Path Solicitation) messages with CPA (Certification Path Advertisements) as defined in Section 6 of SEND specification [RFC3971] must handle the certificate format specified in [I-D.ietf-csi-send-cert], and must be configured with the appropriate certification path.

The proposed approach resolves the incompatibilities between the current SEND specification and the application scenarios described in Section 6.
5. Secure Proxy ND Specification

A Secure Proxy ND performs all the operations described in the SEND specification [RFC3971] 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 ND 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.

5.1. Proxy Signature Option

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:

```
+----------------------------------+
<p>| 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 |
| Type | Length | Reserved |</p>
<table>
<thead>
<tr>
<th>----------------------------------</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Hash</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>Digital Signature</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>Padding</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
</tbody>
</table>

Figure 1: 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] 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 corresponding 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] 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].

This field starts after the Key Hash field. The length of the Digital Signature field is determined by the ASN.1 BER coding of the PKCS#1 v1.5 signature.

Padding

This variable-length field contains padding. The length of the padding field is determined by the length of the Proxy Signature Option minus the length of the other fields.

5.2. Modified SEND processing rules

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 CGA and RSA options defined in the SEND specification [RFC3971].

5.2.1. Processing rules for senders

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 follows:

   A. If the Secure Proxy ND is locally generating the SEND message for a proxied address, the message MUST be constructed as described in Neighbor Discovery for IP version 6 specification [RFC4861].

   B. If the Secure Proxy ND is forwarding a SEND message, first the authenticity of the intercepted message MUST be verified as specified in SEND specification [RFC3971], 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].
C. If the Secure Proxy ND is forwarding a SEND message already containing a PSO, first the authenticity of the intercepted message is verified as specified in Section 5.2.2 of this specification. If the SEND message is valid, the original PSO MUST be removed from the message. The intercepted message is finally modified as described in Section 4 of the ND Proxy specification \[RFC4389\].

2. Timestamp and Nonce options MUST be included according to the rules specified in SEND \[RFC3971\]. The value in the Timestamp option MUST be generated by the Proxy. If the proxy is forwarding a message, the Nonce value in the proxied message MUST be the same as in the forwarded message.

3. The Proxy Signature option MUST be added as the last option in the message.

4. The data MUST be signed as explained in Section 5.1.

5.2.2. Processing rules for receivers

Any SEND message without a Proxy Signature option MUST be treated as specified in the SEND specification \[RFC3971\].

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 \[RFC3971\] 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.

4. The Digital Signature verification MUST show that the signature has been calculated as specified in Section 5.1.

5. Timestamp and Nonce options MUST be processed as specified in \[RFC3971\] Section 5.3.4, except for replacing ‘RSA Signature option’ by ‘PSO option’.
6. Messages with the Override bit [RFC4861] set MUST override an existing cache entry regardless if it was created as a result of a RSA Signature option or a PSO option validation. When the Override bit is not set, the advertisement MUST NOT update a cached link-layer address created securely by means of RSA Signature option or PSO option validation.

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.

5.3. Proxying Link-Local Addresses

Secure Neighbor Discovery [RFC3971] relies on certificates to prove that routers are authorized to announce a certain prefix. However, Neighbor Discovery [RFC4861] states that router does not announce the Link-Local prefix (fe80::/64). Hence, it is not required for a SEND certificate to hold a X.509 extension for IP addresses that authorizes the fe80::/64 prefix. However, some scenarios ([RFC4389], [RFC5213]) impose that the Secure ND proxy provides proxying function for the Link-Local address of a node. When Secure ND proxy functionality for a Link-Local address is required, either a list of link-local addresses, or the fe80::/64 prefix MUST be explicitly authorized to be proxied in the corresponding certificate.
6. Application Scenarios

In this section we describe three different application scenarios for which Secure Proxy ND Support for SEND can be applied. Note that the particular way in which Secure Proxy ND support is applied (which ND messages are proxied, in which directions, how the interaction with non-SEND hosts and RFC3971 hosts is handled, etc.) largely depends on the particular scenario considered. In the first two scenarios presented below, ND messages are synthesized on behalf of off-link nodes. In the third one, ND message generation is triggered by the reception of ND messages in other interfaces of the proxy.

6.1. Scenario 1: Mobile IPv6

The description of the problems for deploying SEND in this scenario can be found in [I-D.ietf-csi-sndp-prob].

The Mobile IPv6 protocol (MIPv6) [RFC3775] 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 MN attaches to a foreign network, all the packets sent to the MN’s HoA by a Correspondent Node (CN) on the home link or a router, are intercepted by the Home Agent (HA) on that home link, encapsulated and tunneled to the MN’s registered Care-of Address (CoA).

The HA intercepts these packets acting as a ND proxy for this MN. When a NS is intercepted on the home link, the HA 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) constructed as described in [RFC4861], containing its own link layer address (HA_LL) as the Target Link Layer Address Option (TLLAO). Then a timestamp (generated by the proxy) and nonce (if appropriate, according to [RFC3971]), MUST be included. Finally, a PSO option signing the message MUST be included as the last option of the message.
Figure 2: Proxy ND role of the Home agent in MIPv6

A node receiving the NA containing the PSO (e.g.: the CN in the home link, or a router) MUST apply the rules defined in Section 5.2.2. Note that in this case the Override bit of the NA message is used to control which messages should prevail each case: the message generated by the proxy once the MN moves from the home network, or the MN if it comes back to the home link, as defined in the MIPv6 specification [RFC3775]

6.2. Scenario 2: Proxy Mobile IPv6

Proxy Mobile IPv6 [RFC5213] 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 completed (it receives a Proxy Binding Ack – PBA), it will reply to the MN with a ICMPv6 Router Advertisement (RA) containing the 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 3).
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.

To provide SEND protection, each MAG is configured to act as a proxy by means of a certificate associated to the PMIPv6 domain, authorizing each MAG to proxy securely ND messages. In addition, the certificate must also authorize the MAG to advertise prefixes. Note that the inclusion of multiple KeyPurposeId values is supported by [I-D.ietf-csi-send-cert].

When a MAG replies to a RS with a RA, the source address MUST be equal to the MAG link-local address associated to the MN in this PMIPv6 domain and its own link layer address as Source link-layer address. Then a timestamp (generated by the proxy) and nonce (if appropriate, according to [RFC3971]), MUST be included. Finally, a PSO option signing the message MUST be included as the last option of the message. This procedure is followed for any other ND message that could be generated by the MAG to a MN.

A node receiving a message from the MAG containing the PSO MUST apply the rules defined in Section 5.2.2.

6.3. Scenario 3: RFC 4389 Neighbor Discovery Proxy

The description of the problems for deploying SEND in this scenario can be found in [I-D.ietf-csi-sndp-prob].
The Neighbor Discovery (ND) Proxy specification [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 Secure ND Proxy shall parse any IPv6 packet it receives on a proxy interface to check whether it contains one of the following secured ICMPv6 messages: NS, NA, RA, or Redirect. The Secure ND Proxy MUST verify the authenticity of the received ND message, according to [RFC3971]. If the SEND message is valid, then it proxies the original message with the following changes:

1. The message MUST be processed according to [RFC4389]. This includes changing the source link layer address to the address of

---

**Figure 4: Proxy ND operations**

<table>
<thead>
<tr>
<th>Link 1</th>
<th>Link 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host A</td>
<td>ND Proxy (P)</td>
</tr>
<tr>
<td>SRC = A</td>
<td>DST = solicited_node(B)</td>
</tr>
<tr>
<td>DST = solicited_node(B)</td>
<td>ICMPv6 NS</td>
</tr>
<tr>
<td>ICMPv6 NS</td>
<td>TARGET = B</td>
</tr>
<tr>
<td>TARGET = B</td>
<td>SLLAO = A_LL</td>
</tr>
<tr>
<td>SLLAO = A_LL</td>
<td>------------------------&gt;</td>
</tr>
<tr>
<td>SRC = B</td>
<td>DST = A</td>
</tr>
<tr>
<td>DST = A</td>
<td>ICMPv6 NA</td>
</tr>
<tr>
<td>ICMPv6 NA</td>
<td>TARGET = B</td>
</tr>
<tr>
<td>TARGET = B</td>
<td>TLLAO = B_LL</td>
</tr>
<tr>
<td>TLLAO = B_LL</td>
<td>&lt;-------------------------</td>
</tr>
<tr>
<td>SRC = B</td>
<td>DST = A</td>
</tr>
<tr>
<td>DST = A</td>
<td>ICMPv6 NA</td>
</tr>
<tr>
<td>ICMPv6 NA</td>
<td>TARGET = B</td>
</tr>
<tr>
<td>TARGET = B</td>
<td>TLLAO = P_LL</td>
</tr>
<tr>
<td>TLLAO = P_LL</td>
<td>&lt;-------------------------</td>
</tr>
</tbody>
</table>
the outgoing interface, maintaining the destination link layer address as the address in the neighbor entry corresponding to the destination IPv6 address, etc. In particular any 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.

2. Any CGA or RSA option MUST be removed.

3. If a Nonce option existed in the original message, its value MUST be preserved in the proxied message. The Timestamp MUST be generated by the proxy.

4. The PSO option MUST be added as the last option in the message, signing all the information contained so far in the message.

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.

In order to deploy this scenario, nodes in proxied segments MUST know the certificate authorizing proxy operation. To do so it could be required to configure at least one device per each proxied segment (may be the proxy itself) to propagate the required certification path to authorize proxy operation by means of a CPS CPA exchange.

While more robust mechanisms could be developed for securing the scenario described in [RFC4389], if hosts have been upgraded to apply the rules stated in Section 5.2.2, for example to benefit from secure support for other scenarios, the application of this mechanism is straightforward.
7. Backward Compatibility with RFC3971 nodes and non-SEND nodes

In this section we discuss the interaction of Secure Proxy ND nodes and SPND nodes with RFC3971 nodes and non-SEND nodes.

7.1. Backward Compatibility with RFC3971 nodes

RFC3971 nodes, i.e. SEND nodes not compliant with the modifications required in Section 5 cannot interpret correctly a PSO option received in a proxied ND message. These SEND nodes silently discard the PSO option, as specified in [RFC4861] for any unknown option. As a result, these messages will be treated as unsecured as described in Section 8 "Transitions Issues" of the SEND specification [RFC3971].

When RFC3971 nodes and SPND nodes exchange ND messages (without proxy intervention), in either direction, messages are generated according to the SEND specification [RFC3971], so these nodes interoperate seamlessly.

In the scenarios in which the proxy translates ND messages, the messages to translate can either be originated in a RFC3971 node or in an SPND node, without interoperability issues.

7.2. Backward Compatibility with non-SEND nodes

Non-SEND nodes receiving NDP packets silently discard PSO options, as specified in [RFC4861] for any unknown option. Therefore, these node interpret messages proxied by a Secure Proxy ND as any other ND message.

When non-SEND nodes and SPND nodes exchange ND messages (without proxy intervention), in either direction, the rules specified in section 8 of [RFC3971] apply.

A secure Proxy ND SHOULD support the use of secured and unsecured NDP messages at the same time, although it MAY have a configuration that causes not to perform proxing for unsecured NDP messages. A secure Proxy ND MAY also have a configuration option whereby it disables secure ND proxying completely. This configuration SHOULD be switched off by default, that is SEND is used. In the next paragraphs we discuss the recommended behavior of the Secure Proxy ND regarding to the protection level to provide to proxied messages in a mixed scenario involving SPND/RFC3971 nodes and non-SEND nodes. In particular, two different situations occur depending on if the proxied nodes are RFC3971 or SPND, or if they are non-SEND nodes.

As a rule of thumb, if the proxied nodes can return to the link in which the proxy operates, the Secure Proxy ND MUST only generate PSO
options on behalf of nodes with SEND capabilities (i.e. that they could use SEND to defend their messages if being in the same link than the proxy, either RFC3971 nodes or SPND nodes). This is relevant to allow nodes preferring secured information over unsecured one, and for executing the DAD procedure, as specified in [RFC3971]. Therefore, the Secure Proxy ND MUST generate messages containing the PSO option for SPND and RFC3971 hosts, and MUST NOT generate messages containing the PSO option for non-SEND nodes. Note that ND advertisements in response to solicitations generated by a Secure Proxy ND must be secured or not according to the previous considerations (i.e. to the nature of the proxied node), and not according to the secure or unsecure nature of the solicitation message.

To apply this rule, we have to consider that depending on the application scenario the proxy may translate ND messages generated by a node or synthetise ND messages on behalf of a node that can return to the link in which the Secure Proxy ND operates.

- For translating ND messages for nodes that can arrive to the link in which the proxy operates, the rule can be easily applied: only messages validated in the Secure Proxy ND according to the SEND specification [RFC3971] MUST be proxied securely by the inclusion of a PSO option. Unsecured ND messages could be proxied if unsecured operation is enabled in the proxy, but the message generated by the Secure Proxy ND for the received message MUST NOT include a PSO option.

- For synthesizing ND messages on behalf of remote nodes, different considerations should be made according to the particular application scenario.

* For MIPv6, if the MN can return to the home link, it is required for the proxy to know if the node could use SEND to defend its address or not. A mismatch between the proxy and proxied node behavior regarding to SEND operation would result in unappropriate operation. A HA including the PSO option for proxying a non-SEND MN would make ND messages sent by the proxy to be more preferred than ND message of the non-SEND MN when the MN returns to the home link (even if the proxied messages have the Override bit set to 1). Not using the PSO option for a RFC3971 or SPND MN would make more vulnerable the address in the home link when the MN is away than when it is in the home link (and would defeat the purpose of the Secure Proxy ND mechanism). Therefore, in this case the HA MUST know the SEND capabilities of the MN, and MUST use PSO if the MN is a SPND or RFC3971 host, and MUST NOT use PSO for non-SEND hosts.
For the Proxy Mobile IPv6 scenario, we have to note that a node moving from a link in which PSO has been used to protect a link-layer address to a link in which ND messages are not protected by SEND would prevent the MN from acquiring the new information until the cached information expires. However, in this case it is reasonable to consider that all MAGs provide the same security for protecting ND messages, and that either all MAGs will behave as Secure Proxy ND, or none, so configuration could be easier.
8. Security Considerations

The mechanism described in this document introduces a new Proxy Signature Option (PSO) allowing a Secure Proxy ND to generate or modify a SEND message for a proxied address. A SPND node will only accept such a message if it includes a valid PSO generated by an authorized Secure Proxy ND. Such a message has equivalent protection to the threats presented in section 9 of [RFC3971] as a message signed with a RSA Signature option.

The security of proxied ND messages not including a PSO option is the same as an unsecured ND message. The security of a proxied ND message received by a non-SEND host or RFC3971 host is the same of an unsecured ND message.

Thanks to the authorization certificate it is provisioned with, a proxy ND is authorized to issue ND signaling on behalf of nodes on the subnet. Thus, a compromised proxy is able, like a compromised router, to siphon off traffic from the host, or mount a man-in-the-middle attack. However, when two on-link hosts communicate using their respective link-local addresses, the threats involved with a compromised router and a compromised proxy ND differs because the router is not able to siphon off traffic exchanged between the hosts or mount a man-in-the-middle attack, while the proxy ND can, even if the hosts use SEND.

The messages for which a Secure Proxy ND performs its function, and the link for which this function is performed MUST be configured appropriately for each proxy and scenario. This configuration is specially relevant if Secure Proxy ND is used for translating ND messages from one link to another.

Proper configuration of when the PSO option must or must not be included, depending on the proxied nodes being SEND or non-SEND may result in security considerations which are discussed in Section 7.

Attacks to the timestamp of the secured ND message can be performed as described in section 7.3 of [I-D.ietf-csi-sndp-prob].
9. IANA Considerations

IANA is requested to allocate:

A new IPv6 Neighbor Discovery Option type 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] namespace, 0x09F5 2BE5 3B62 4C76 CB96 4E7F CDC9 2804.
10. References

10.1. Normative References

[I-D.ietf-csi-send-cert]
Gagliano, R., Krishnan, S., and A. Kukec, "Certificate profile and certificate management for SEND",
draft-ietf-csi-send-cert-03 (work in progress), March 2010.


10.2. Informative References

[I-D.ietf-csi-sndp-prob]
draft-ietf-csi-sndp-prob-04 (work in progress), January 2010.
Authors’ Addresses

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
QUALCOMM Incorporated
5775 Morehouse Dr
San Diego, CA  92121
USA
Phone: +1 858 658 3538
Email: julienl@qualcomm.com

Marco Bonola
Rome Tor Vergata University
Via del Politecnico, 1
Rome  I-00133
Italy
Phone:
Email: marco.bonola@gmail.com

Alberto Garcia-Martinez
U. Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid  28911
Spain
Phone: +34 91 6248782
Email: alberto@it.uc3m.es
URI:  http://www.it.uc3m.es/