Network Working Group	J. Arkko
Internet-Draft	Ericsson
Expires: August 19, 2003	V. Devarapalli
	Nokia Research Center
	F. Dupont
	ENST Bretagne
	February 18, 2003

TOC

Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents

draft-ietf-mobileip-mipv6-ha-ipsec-03.txt

Abstract

Mobile IPv6 uses IPsec to protect signaling between the home agent and the mobile node. Mobile IPv6 base document defines the main requirements these nodes must follow. This document discusses these requirements in more depth, illustrates the used packet formats, describes suitable configuration procedures, and shows how implementations can process the packets in the right order.

TOC

Table of Contents

TOC

1. Introduction

This document illustrates the use of IPsec in securing control traffic relating to Mobile IPv6[8]. In Mobile IPv6, a mobile node is always expected to be addressable at its home address, whether it is currently attached to its home link or is away from home. The "home address" is an IP address assigned to the mobile node within its home subnet prefix on its home link. While a mobile node is at home, packets addressed to its home address are routed to the mobile node's home link.

While a mobile node is attached to some foreign link away from home, it is also addressable at a care-of addresses. A care-of address is an IP address associated with a mobile node that has the subnet prefix of a particular foreign link. The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. While away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function as the "home agent" for the mobile node. The mobile node performs this binding registration by sending a "Binding Update" message to the home agent. The home agent replies to the mobile node by returning a "Binding Acknowledgement" message.

Any other nodes communicating with a mobile node are referred to as "correspondent nodes". Mobile nodes can provide information about their current location to correspondent nodes, again using Binding Updates and Acknowledgements. Additionally, return routability test is performed between the mobile node, home agent, and the correspondent node in order to authorize the establishment of the binding. Packets between the mobile node and the correspondent node are either tunneled via the home agent, or sent directly if a binding exists in the correspondent node for the current location of the mobile node.

Mobile IPv6 tunnels payload packets between the mobile node and the home agent in both directions. This tunneling uses IPv6 encapsulation[7]. Where these tunnels need to be secured, they are replaced by IPsec tunnels[2].

Mobile IPv6 also provides support for the reconfiguration of the home network. Here the home subnet prefixes may change over time. Mobile nodes can learn new information about home subnet prefixes through the "prefix discovery" mechanism.

This document discusses security mechanisms for the control traffic between the mobile node and the home agent. If this traffic is not protected, mobile nodes and correspondent nodes are vulnerable to Man-in-the-Middle, Hijacking, Confidentiality, Impersonation, and Denial-of-Service attacks. Any third parties are also vulnerable to Denial-of-Service attacks. These threats are discussed in more detail in Section 15.1 of the Mobile IPv6 base specification[8].

In order to avoid these attacks, the base specification uses IPsec[2] to protect control traffic between the home agent and the mobile node. This control traffic consists of

various messages carried by the Mobility Header protocol in IPv6[6]. The traffic takes the following forms:

*Binding Update and Acknowledgement messages exchanged between the mobile node and the home agent, as described in Sections 10.3.1, 10.3.2, 11.7.1, and 11.7.3 of the base specification[8].

*Return routability messages Home Test Init and Home Test that pass through the home agent on their way to a correspondent node, as described in Section 10.4.6 of the base specification[8].

*ICMPv6 messages exchanged between the mobile node and the home agent for the purposes of prefix discovery, as described in Sections 10.6 and 11.4 of the base specification[8].

The nodes may also optionally protect payload traffic passing through the home agent, as described in Section 5.3 of the base specification[8]. If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection support is required.
The control traffic between the mobile node and the home agent requires message authentication, integrity, correct ordering and replay protection. The mobile node and the home agent must have a security association to protect this traffic. Furthermore, great care is needed when using IKE[5] to establish security associations to Mobile IPv6 home agents. The right kind of addresses must be used for transporting IKE. This is necessary to avoid circular dependencies in which the use of a Binding Update triggers the need for an IKE exchange that cannot complete prior to the Binding Update having been completed.
The mobile IPv6 base document defines the main requirements the mobile nodes and home agents must follow when securing the above traffic. This document discusses these requirements in more depth, illustrates the used packet formats, describes suitable configuration procedures, and shows how implementations can process the packets in the right order.
We begin our description by showing the required wire formats for the protected packets in Packet Formats. Requirements describes rules which associated Mobile IPv6, IPsec, and IKE implementations must observe. Example Configurations discusses how IPsec can be configured to use either manual or automatically established security associations. Processing Steps within a Node shows examples of how packets are processed within the nodes.
All implementations of Mobile IPv6 mobile node and home agent MUST support at least the formats described in Packet Formats and obey the rules in Requirements. The configuration and processing sections are informative, and should only be considered as one possible way of providing the required functionality.

TOC

2. Terminology

The keywords "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[1].

TOC

3. Packet Formats

3.1 Binding Updates and Acknowledgements

When the mobile node is away from its home, the BUs sent by it to the home agent MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header
Mobility header
   Binding Update
      Alternative Care-of Address option (care-of address)
```

Note that the Alternative Care-of Address option is used to ensure that the care-of address is protected by ESP. The home agent considers the address within this option as the current care-of address for the mobile node.
The Binding Acknowledgements sent back to the mobile node when it is away from home MUST have at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header
Mobility header
   Binding Acknowledgement
```

When the mobile node is at home, the above rules are different as the mobile node can use its home address as a source address. This typically happens for the de-registration Binding Update when the mobile is returning home. In this situation, the Binding Updates MUST support at least the following headers in the following order:

```
IPv6 header (source = home address,
             destination = home agent)
ESP header
Mobility header
   Binding Update
      Alternative Care-of Address option (care-of address)
```

The Binding Acknowledgement messages sent to the home address MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = home address)
ESP header
Mobility header
   Binding Acknowledgement
```

3.2 Return Routability Signaling

When the Home Test Init messages tunneled to the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header
IPv6 header (source = home address,
             destination = correspondent node)
Mobility Header
   Home Test Init
```

This format assumes that the mobile node's current care-of address is used as one of the gateway addresses in the security association. As discussed in IPsec Protocol Processing, this requires the home agent to update the gateway address when the mobile node moves. Policy entries and security association selectors stay the same, however, as the inner packets do not change upon movements.
Similarly, when the Home Test messages tunneled from the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test
```

The format used to protect return routability packets relies on the destination of the tunnel packets to change for the mobile node as it moves. The home agent's address stays the same, but the mobile node's address changes upon movements, as if the security association's tunnel gateway address had changed. When the mobile node adopts a new care-of address, its source address selection rules will automatically adopt a new source address for outgoing tunnel packets. (The home agent accepts packets sent like this, as the outer source address in tunnel packets is not checked.)
The process is more complicated in the home agent side, as the home agent has stored the previous care-of address in its Security Association Database as the gateway address. When IKE is being used, the mobile node runs it on top of its then current care-of address, and the resulting tunnel-mode security associations will use the same addresses as IKE was transported on. In order for the home agent to be able to tunnel a Home Test message to the mobile node, it uses the current care-of address as the destination of the tunnel packets, as if the home agent had modified the gateway address of the security association used for this protection. This implies that the same security

association can be used in multiple locations, and no new configuration or IKE rekeying is needed per movement.

3.3 Prefix Discovery

If IPsec is used to protect prefix discovery, requests for prefixes from the mobile node to the home agent MUST support at least the following headers in the following order.

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header
ICMPv6
   Mobile Prefix Solicitation
```

Again if IPsec is used, solicited and unsolicited prefix information advertisements from the home agent to the mobile node MUST support at least the following headers in the following order.

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header
ICMPv6
   Mobile Prefix Advertisement
```

3.4 Payload Packets

If IPsec is used to protect payload packets tunneled to the home agent from the mobile node, a similar format is used as in the case of tunneled Home Test Init messages. However, instead of the Mobility Header these packets may contain any legal IPv6 protocol(s):

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header
IPv6 header (source = home address,
             destination = correspondent node)
Any protocol
```

Similarly, when the payload packets are tunneled from the home agent to the mobile node with IPsec protection, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header
IPv6 header (source = correspondent node,
             destination = home address)
Any protocol
```

TOC

4. Requirements

This section describes mandatory rules for all Mobile IPv6 mobile nodes and home agents. These rules are necessary in order for it to be possible to enable IPsec communications despite movements, guarantee sufficient security, and to ensure correct processing order of packets.
The rules in the following sections apply only to the communications between home agents and mobile nodes. They should not be taken as requirements on how IPsec in general is used by mobile nodes.

4.1 Mandatory Support

The following requirements apply to both home agents and mobile nodes:

*Manual configuration of security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

*Automatic key management with IKE[5] MAY be supported. Only IKEv1 is discussed in this document, even if it is expected that the next version of IKE can also be used and that it offers several improvements in this specific application.

*IPsec protection for Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

*IPsec protection for the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

*IPsec protection for the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

*IPsec protection of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

*If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

4.2 Policy Requirements

The following requirements apply to both home agents and mobile nodes:

*When a packet is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option MUST be considered as the source address of the packet.

*Similarly, a home address within a Type 2 Routing header MUST be considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

*When IPsec is used to protect return routability signaling or payload packets, the security policy database entries SHOULD be defined specifically for the tunnel interface between the mobile node and the home agent. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

*The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

*When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The SPD entries, which were used for protecting tunneled traffic between the mobile node and the home agent become inactive. The corresponding security associations could be stored or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves aways from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD not be deleted as they do not depend on care-of addresses and can be used again.

The following rules apply to mobile nodes:

*The mobile node MUST use the Home Address destination option in Binding Updates and Mobile Prefix Solicitations, sent to the home agent from a care-of address.

*When the mobile node receives a changed set of prefixes from the home agent during prefix discovery, there is a need to configure new security policy entries, and there may be a need to configure new security associations. It is outside the scope of this specification to discuss automatic methods for this.

The following rules apply to home agents:

*The home agent MUST use the Type 2 Routing header in Binding Acknowledgements and Mobile Prefix Advertisements sent to the mobile node, again due to the need to have the home address visible when the policy checks are made.

*It is necessary to avoid the possibility that a mobile node could use its security association to send a Binding Update on behalf of another mobile node using the same home agent. In order to do this, the security policy database entries MUST unequivocally identify a single security association for any given home address and home agent when manual keying is used. When dynamic keying is used, the security policy database entries MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for a particular home address. How these mappings are maintained is outside the scope of this specification, but they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a FQDN, secure forms of DNS may also be used.

*When the set of prefixes advertised by the home agent changes, there is a need to configure new security policy entries, and there may be a need to configure new security associations. It is outside the scope of this specification to discuss automatic methods for this, if new home addresses are required.

4.3 IPsec Protocol Processing

The following requirements apply to both home agents and mobile nodes:

*When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents SHOULD use the Encapsulating Security Payload (ESP)[4] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection. Note that Authentication Header (AH)[3] is also possible but for brevity is not discussed in this specification.

Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401[2], RFC 2402[3], and RFC 2406[4]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when security associations are configured manually, as the same key is used for a long time.

*Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and authentication algorithm MUST be applied.

*IPsec AH[3] authenticator calculation MUST be performed as if a packet with a Type 2 Routing header would have the home address in the IPv6 destination address field and the care-of address in the Routing header. Type 2 Routing header should be treated by IPsec in the same manner as Type 0 Routing header.

*Similarly, the authenticator calculation MUST be performed as if a packet with a Home Address destination option would have the home address in the IPv6 source address field and the care-of address in the destination option.

The following rules apply to mobile nodes:

*When ESP is used to protect Binding Updates, there is no protection for the care-of address which appears in the IPv6 header outside the area protected by ESP. It is important for the home agent to verify that the care-of address has not been tampered. As a result, the attacker would have redirected the mobile node's traffic to another address. In order to prevent this, Mobile IPv6 implementations MUST use the Alternate Care-of Address mobility option in all Binding Updates sent to the home agent. (Note that AH protects also the IPv6 header, and some implementations might avoid the option if they know AH is being used.)

*When IPsec is used to protect return routability signaling or payload packets, the mobile node MUST set the source address it uses for the outgoing tunnel packets to the current primary care-of address. The mobile node starts to use a new primary care-of address immediately after sending a Binding Update to the home agent to register this new address.

The following rules apply to home agents:

*When IPsec is used to protect return routability signaling or payload packets, IPsec security associations are needed to provide this protection. When the care-of address for the mobile node changes as a result of an accepted Binding Update, special treatment is needed for the next packets sent using these security associations. The home agent MUST set the new care-of address as the destination address of these packets, as if the destination gateway address in the security association had changed.

4.4 Dynamic Keying

The following requirements apply to both home agents and mobile nodes:

*If replay protection is required, dynamic keying MUST be used. IPsec can provide replay protection only if dynamic keying is used. This may not always be possible, and manual keying would be preferred in some cases. IPsec also does not guarantee correct ordering of packets, only that they have not been replayed. Because of this, sequence numbers within the Mobile IPv6 messages ensure correct ordering. However, if a home agent reboots and loses its state regarding the sequence numbers, replay attacks become possible. The use of a key management mechanism together with IPsec can be used to prevent such replay attacks.

*If IKE version 1 is used with preshared secrets in main mode, it determines the shared secret to use from the IP address of the peer. With Mobile IPv6, however, this may be a care-of address and does not indicate which mobile node attempts to contact the home agent. Therefore, if preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used. Note also that care needs to be taken with phase 1 identity selection. Where the ID_IPV6_ADDR Identity Payloads is used, unambiguous

mapping of identities to keys is not possible. (The next version of IKE may not have these limitations.)

The following rules apply to mobile nodes:

*Where dynamic keying is used, the key management protocol MUST use the care-of address as the source address in the protocol exchanges with the mobile node's home agent.

*Conversely, the IPsec security associations with the mobile node's home agent MUST be requested from the key management protocol with the home address as the mobile node's address.

The security associations for protecting Binding Updates and Acknowledgements are requested for the Mobility header protocol in transport mode and for specific IP addresses as endpoints. Similarly, the security associations for protecting prefix discovery are requested for the ICMPv6 protocol. Payload and return routability protection requests security associations for a specific tunnel interface and either the payload protocol or the Mobility header protocol, in tunnel mode. In this case one requested endpoint is an IP address and another one is a wildcard.

*If the mobile node has used IKE to establish security associations with its home agent, it should follow the procedures discussed in Section 11.7.1 and 11.7.3 of the base specification to determine whether the IKE endpoints can be moved or if rekeying is needed.

The following rules apply to home agents:

*If the home agent has used IKE to establish security associations with the mobile node, it should follow the procedures discussed in Section 10.3.1 and 10.3.2 of the base specification to determine whether the IKE endpoints can be moved or if rekeying is needed.

TOC

5. Example Configurations

In the following we describe the Security Policy Database (SPD) and Security Association Database (SAD) entries necessary to protect Binding Updates and Binding Acknowledgements exchanged between the mobile node and the home agent. Our examples assume the use of ESP, but a similar configuration could also be used to protect the messages with AH.
Format introduces the format we use in the description of the SPD and the SAD. Manual Configuration describes how to configure manually keyed security associations, and Dynamic Keying describes how to use dynamic keying.

5.1 Format

The format used in the examples is as follows. The SPD description has the format

```
<node> "SPD OUT:"
  "-" <spdentry>
  "-" <spdentry>
  ...
  "-" <spdentry>

<node> "SPD IN:"
  "-" <spdentry>
  "-" <spdentry>
  ...
  "-" <spdentry>
```

Where <node> represents the name of the node, and <spdentry> has the following format:

```
"IF" <condition> "THEN USE" <sa> |
"IF" <condition> "THEN CREATE" <pattern> |
```

Where <condition> is an boolean expression about the fields of the IPv6 packet, <sa> is the name of a security association, and <pattern> is a specification for a security association to be negotiated via IKE[5]. The SAD description has the format

```
<node> "SAD:"
  "-" <sadentry>
  "-" <sadentry>
  ...
  "-" <sadentry>
```

Where <node> represents the name of the node, and <sadentry> has the following format:

```
<sa> "(" <dir> ","
         <spi> ","
         <destination> ","
         <ahesp> ","
         <mode> ")" ":"
     <selectors>
```

Where <dir> is "IN" or "OUT", <spi> is the SPI of the security association, <destination> is its destination, <ahesp> is normally "ESP" in our case but could also be "AH", <mode> is either "TUNNEL" or "TRANSPORT", and <selectors> is a boolean expression about the fields of the IPv6 packet.
We will be using an example mobile node in this section with the home address "home_address_1". The user's identity in this mobile node is "user_1". The home agent's address is "home_agent_1".

5.2 Manual Configuration

5.2.1 Binding Updates and Acknowledgements

Here are the contents of the SPD and SAD for protecting Binding Updates and Acknowledgements:

```
mobile node SPD OUT:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = MH
    THEN USE SA1

mobile node SPD IN:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = MH
    THEN USE SA2

mobile node SAD:
  - SA1(OUT, spi_a, home_agent_1, ESP, TRANSPORT):
    source = home_address_1 & destination = home_agent_1 &
    proto = MH
  - SA2(IN, spi_b, home_address_1, ESP, TRANSPORT):
    source = home_agent_1 & destination = home_address_1 &
    proto = MH

home agent SPD OUT:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = MH
    THEN USE SA2

home agent SPD IN:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = MH
    THEN USE SA1

home agent SAD:
  - SA2(OUT, spi_b, home_address_1, ESP, TRANSPORT):
    source = home_agent_1 & destination = home_address_1 &
    proto = MH
  - SA1(IN, spi_a, home_agent_1, ESP, TRANSPORT):
    source = home_address_1 & destination = home_agent_1 &
    proto = MH
```

In the above, "MH" refers to the protocol number for the Mobility Header[8].

5.2.2 Return Routability Signaling

In the following we describe the necessary SPD and SAD entries to protect return routability signaling between the mobile node and the home agent. Note that the rules in the SPD are ordered, and the ones in the previous section must take precedence over these ones:

```
mobile node SPD OUT:
  - IF interface = tunnel to home_agent_1 &
       source = home_address_1 & destination = any &
       proto = MH
    THEN USE SA3

mobile node SPD IN:
  - IF interface = tunnel from home_agent_1 &
       source = any & destination = home_address_1 &
       proto = MH
    THEN USE SA4

mobile node SAD:
  - SA3(OUT, spi_c, home_agent_1, ESP, TUNNEL):
    source = home_address_1 & destination = any & proto = MH
  - SA4(IN, spi_d, home_address_1, ESP, TUNNEL):
    source = any & destination = home_address_1 & proto = MH

home agent SPD OUT:
  - IF interface = tunnel to home_address_1 &
       source = any & destination = home_address_1 &
       proto = MH
    THEN USE SA4

home agent SPD IN:
  - IF interface = tunnel from home_address_1 &
       source = home_address_1 & destination = any &
       proto = MH
    THEN USE SA3

home agent SAD:
  - SA4(OUT, spi_d, home_address_1, ESP, TUNNEL):
    source = any & destination = home_address_1 & proto = MH
  - SA3(IN, spi_c, home_agent_1, ESP, TUNNEL):
    source = home_address_1 & destination = any & proto = MH
```

5.2.3 Prefix Discovery

In the following we describe some additional SPD and SAD entries to protect prefix discovery.

```
mobile node SPD OUT:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = ICMPv6
    THEN USE SA5.

mobile node SPD IN:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = ICMPv6
    THEN USE SA6

mobile node SAD:
  - SA5(OUT, spi_e, home_agent_1, ESP, TRANSPORT):
    source = home_address_1 & destination = home_agent_1 &
    proto = ICMPv6
  - SA6(IN, spi_f, home_address_1, ESP, TRANSPORT):
    source = home_agent_1 & destination = home_address_1 &
    proto = ICMPv6

home agent SPD OUT:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = ICMPv6
    THEN USE SA6

home agent SPD IN:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = ICMPv6
    THEN USE SA5

home agent SAD:
  - SA6(OUT, spi_f, home_address_1, ESP, TRANSPORT):
    source = home_agent_1 & destination = home_address_1 &
    proto = ICMPv6
  - SA5(IN, spi_e, home_agent_1, ESP, TRANSPORT):
    source = home_address_1 & destination = home_agent_1 &
    proto = ICMPv6
```

Note that the SPDs described above protect all ICMPv6 traffic between the mobile node and the home agent.

5.2.4 Payload Packets

It is also possible to perform some additional, optional, protection of tunneled payload packets. This protection takes place in a similar manner to the return routability protection above, but requires a different value for the protocol field. The necessary SPD and SAD entries are shown below. It is assumed that the entries for protecting Binding Updates and Acknowledgements, and the entries to protect Home Test Init and Home Test messages take precedence over these entries.

```
mobile node SPD OUT:
  - IF interface = tunnel to home_agent_1 &
       source = home_address_1 & destination = any &
       proto = X
    THEN USE SA7

mobile node SPD IN:
  - IF interface = tunnel from home_agent_1 &
       source = any & destination = home_address_1 &
       proto = X
    THEN USE SA8

mobile node SAD:
  - SA7(OUT, spi_g, home_agent_1, ESP, TUNNEL):
    source = home_address_1 & destination = any & proto = X
  - SA8(IN, spi_h, home_address_1, ESP, TUNNEL):
    source = any & destination = home_address_1 & proto = X

home agent SPD OUT:
  - IF interface = tunnel to home_address_1 &
       source = any & destination = home_address_1 &
       proto = X
    THEN USE SA8

home agent SPD IN:
  - IF interface = tunnel from home_address_1 &
       source = home_address_1 & destination = any &
       proto = X
    THEN USE SA7

home agent SAD:
  - SA8(OUT, spi_h, home_address_1, ESP, TUNNEL):
    source = any & destination = home_address_1 & proto = X
  - SA7(IN, spi_g, home_agent_1, ESP, TUNNEL):
    source = home_address_1 & destination = any & proto = X
```

If multicast group membership control protocols such as MLDv1[9] or MLDv2[12] need to be protected, these packets may use a link-local address rather than the home address of the mobile node. In this case the source and destination can be left as a wildcard and the SPD entries will work solely based on the used interface and the protocol, which is ICMPv6 for both MLDv1 and MLDv2.
Similar problems are encountered when stateful address autoconfiguration protocols such as DHCPv6[10] are used. The same approach is applicable for DHCPv6 as well. DHCPv6 uses the UDP protocol.
Support for multiple layers of encapsulation (such as ESP encapsulated in ESP) is not required by RFC 2401[2] and is also otherwise often problematic. It is therefore useful to avoid setting the protocol X in the above entries to either AH or ESP.

5.3 Dynamic Keying

In this section we show an example configuration that uses IKE to negotiate security associations.

5.3.1 Binding Updates and Acknowledgements

Here are the contents of the SPD for protecting Binding Updates and Acknowledgements:

```
mobile node SPD OUT:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = MH
    THEN CREATE ESP TRANSPORT SA: local phase 1 identity = user_1

mobile node SPD IN:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = MH
    THEN CREATE ESP TRANSPORT SA: local phase 1 identity = user_1

home agent SPD OUT:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = MH
    THEN CREATE ESP TRANSPORT SA: peer phase 1 identity = user_1

home agent SPD IN:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = MH
    THEN CREATE ESP TRANSPORT SA: peer phase 1 identity = user_1
```

We have omitted details of the proposed transforms in the above, and all details related to the particular authentication method such as certificates beyond listing a specific identity that must be used.
We require IKE to be run using the care-of addresses but still negotiate IPsec SAs that use home addresses. The extra conditions set by the home agent SPD for the peer phase 1 identity to be "user_1" must be verified by the home agent. The purpose of the condition is to ensure that the IKE phase 2 negotiation for a given user's home address can't be requested by another user. In the mobile node, we simply set our local identity to be "user_1".
These checks also imply that the configuration of the home agent is user-specific: every user or home address requires a specific configuration entry. It would be possible to alleviate the configuration tasks by using certificates that have home addresses in the Subject AltName field. However, it isn't clear if all IKE implementations allow one address to be used for carrying the IKE negotiations when another address is mentioned in the used certificates. In any case, even this approach would have required user-specific tasks in the certificate authority.

5.3.2 Return Routability Signaling

Protection for the return routability signaling can be configured in a similar manner as above.

```
mobile node SPD OUT:
  - IF interface = tunnel to home_agent_1 &
       source = home_address_1 & destination = any &
       proto = MH
    THEN CREATE ESP TUNNEL SA: gateway = home_agent_1 &
                               local phase 1 identity = user_1

mobile node SPD IN:
  - IF interface = tunnel from home_agent_1 &
       source = any & destination = home_address_1 &
       proto = MH
    THEN CREATE ESP TUNNEL SA: gateway = home_agent_1 &
                               local phase 1 identity = user_1

home agent SPD OUT:
  - IF interface = tunnel to home_address_1 &
       source = any & destination = home_address_1 &
       proto = MH
    THEN CREATE ESP TUNNEL SA: gateway = home_address_1 &
                               peer phase 1 identity = user_1

home agent SPD IN:
  - IF interface = tunnel from home_address_1 &
       source = home_address_1 & destination = any &
       proto = MH
    THEN CREATE ESP TUNNEL SA: gateway = home_address_1 &
                               peer phase 1 identity = user_1
```

Here we specified the gateway address for the security association as the home address for the mobile node. However, as required by IPsec Protocol Processing the packets will actually be sent to the current care-of address. In order to avoid writing dynamically changing information to the SPD entries, the above has been written with the home address as the gateway.

5.3.3 Prefix Discovery

In the following we describe some additional SPD entries to protect prefix discovery with IKE. (Note that when actual new prefixes are discovered, there may be a need to enter new manually configured SPD entries to specify the authorization policy for the resulting new home addresses.)

```
mobile node SPD OUT:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = ICMPv6
    THEN CREATE ESP TRANSPORT SA: local phase 1 identity = user_1

mobile node SPD IN:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = ICMPv6
    THEN CREATE ESP TRANSPORT SA: local phase 1 identity = user_1

home agent SPD OUT:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = ICMPv6
    THEN CREATE ESP TRANSPORT SA: peer phase 1 identity = user_1

home agent SPD IN:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = ICMPv6
    THEN CREATE ESP TRANSPORT SA: peer phase 1 identity = user_1
```

5.3.4 Payload Packets

Protection for the payload packets happens similarly to the protection of return routability signaling. As in the manually keyed case, these SPD entries have lower priority than the above ones.

```
mobile node SPD OUT:
  - IF interface = tunnel to home_agent_1 &
       source = home_address_1 & destination = any &
       proto = X
    THEN CREATE ESP TUNNEL SA: gateway = home_agent_1 &
                               local phase 1 identity = user_1

mobile node SPD IN:
  - IF interface = tunnel from home_agent_1 &
       source = any & destination = home_address_1 &
       proto = X
    THEN CREATE ESP TUNNEL SA: gateway = home_agent_1 &
                               local phase 1 identity = user_1

home agent SPD OUT:
  - IF interface = tunnel to home_address_1 &
       source = any & destination = home_address_1 &
       proto = X
    THEN CREATE ESP TUNNEL SA: gateway = home_address_1 &
                               peer phase 1 identity = user_1

home agent SPD IN:
  - IF interface = tunnel from home_address_1 &
       source = home_address_1 & destination = any &
       proto = X
    THEN CREATE ESP TUNNEL SA: gateway = home_address_1 &
                               peer phase 1 identity = user_1
```

TOC

6. Processing Steps within a Node

6.1 Binding Update to the Home Agent

Step 1. At the mobile node, Mobile IPv6 module first produces the following packet:

```
IPv6 header (source = home address,
             destination = home agent)
Mobility header
   Binding Update
```

Step 2. This packet is matched against the IPsec policy data base on the mobile node and we make a note that IPsec must be applied.
Step 3. Then, we add the necessary Mobile IPv6 options but do not change the addresses yet, as described in Section 11.2.2 of the base specification[8]. This results in:

```
IPv6 header (source = home address,
             destination = home agent)
Destination Options header
   Home Address option (care-of address)
Mobility header
   Binding Update
```

Step 4. Finally, IPsec headers are added and the necessary authenticator values are calculated:

```
IPv6 header (source = home address,
             destination = home agent)
Destination Options header
   Home Address option (care-of address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

Step 5. Before sending the packet, the addresses in the IPv6 header and the Destination Options header are changed:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

6.2 Binding Update from the Mobile Node

Step 1. The following packet is received at the home agent:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

Step 2. The home address option is processed first, which results in

```
IPv6 header (source = home address,
             destination = home agent)
Destination Options header
   Home Address option (care-of address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

Step 3. ESP header is processed next, resulting in

```
 IPv6 header (source = home address,
              destination = home agent)
 Destination Options header
    Home Address option (care-of address)
 Mobility header
    Binding Update
```

Step 4. This packet matches the security association selectors (source = home address, destination = home agent, proto = MH).
Step 5. Mobile IPv6 processes the Binding Update. The Binding Update is delivered to the Mobile IPv6 module.

6.3 Binding Acknowledgement to the Mobile Node

Step 1. Mobile IPv6 produces the following packet:

```
IPv6 header (source = home agent,
             destination = home address)
Mobility header
   Binding Acknowledgement
```

Step 2. This packet matches the IPsec policy entries, and we remember that IPsec has to be applied.
Step 3. Then, we add the necessary Route Headers but do not change the addresses yet, as described in Section 9.6 of the base specification[8]. This results in:

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
Mobility header
   Binding Acknowledgement
```

Step 4. We apply IPsec:

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

Step 5. Finally, before sending the packet out we change the addresses in the IPv6 header and the Route header:

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

6.4 Binding Acknowledgement from the Home Agent

Step 1. The following packet is received at the mobile node

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

Step 2. After the routing header is processed the packet becomes

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

Step 3. ESP header is processed next, resulting in:

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
Mobility header
   Binding Acknowledgement
```

Step 4. This packet matches the security association selectors (source = home agent, destination = home address, proto = MH).
Step 5. The Binding Acknowledgement is delivered to the Mobile IPv6 module.

6.5 Home Test Init to the Home Agent

Step 1. The mobile node constructs a Home Test Init message:

```
IPv6 header (source = home address,
             destination = correspondent node)
Mobility header
   Home Test Init
```

Step 2. Mobile IPv6 determines that this packet should go to the tunnel to the home agent.
Step 3. The packet is matched against IPsec policy entries for the interface, and we find that IPsec needs to be applied.
Step 4. IPsec tunnel mode headers are added. Note that we use a care-of address as a source address for the tunnel packet.

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header (SPI = spi_c)
IPv6 header (source = home address,
             destination = correspondent node)
Mobility header
   Home Test Init
```

Step 5. The packet no longer satisfies the criteria that made it enter the tunnel, and it is sent directly to the home agent.

6.6 Home Test Init from the Mobile Node

Step 1. The home agent receives the following packet:

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header (SPI = spi_c)
IPv6 header (source = home address,
             destination = correspondent node)
Mobility Header
   Home Test Init
```

Step 2. IPsec processing is performed, resulting in:

```
IPv6 header (source = home address,
             destination = correspondent node)
Mobility Header
   Home Test Init
```

Step 3. The resulting packet matches the selectors and the packet can be processed further.
Step 4. The packet is then forwarded to the correspondent node.

6.7 Home Test to the Mobile Node

Step 1. The home agent receives a Home Test packet from the correspondent node:

```
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test Init
```

Step 2. The home agent determines that this packet is destined to a mobile node that is away from home, and decides to tunnel it.
Step 3. The packet matches the IPsec policy entries for the tunnel interface, and we note that IPsec needs to be applied.
Step 4. IPsec is applied, resulting in a new packet. Note that the home agent must keep track of the location of the mobile node, and update the tunnel gateway address in the security association(s) accordingly.

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header (SPI = spi_d)
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test Init
```

Step 5. The packet no longer satisfies the criteria that made it enter the tunnel, and it is sent directly to the care-of address.

6.8 Home Test from the Home Agent

Step 1. The mobile node receives the following packet:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header (SPI = spi_d)
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test Init
```

Step 2. IPsec is processed, resulting in:

```
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test Init
```

Step 3. This matches the security association selectors (source = any, destination = home address).
Step 4. The packet is given to Mobile IPv6 processing.

6.9 Prefix Solicitation Message to the Home Agent

This procedure is similar to the one presented in Binding Update to the Home Agent.

6.10 Prefix Solicitation Message from the Mobile Node

This procedure is similar to the one presented in Binding Update from the Mobile Node.

6.11 Prefix Advertisement Message to the Mobile Node

This procedure is similar to the one presented in Binding Acknowledgement to the Mobile Node.

6.12 Prefix Advertisement Message from the Home Agent

This procedure is similar to the one presented in Binding Acknowledgement from the Home Agent.

6.13 Payload Packet to the Home Agent

This procedure is similar to the one presented in Home Test Init to the Home Agent.

6.14 Payload Packet from the Mobile Node

This procedure is similar to the one presented in Home Test Init from the Mobile Node.

6.15 Payload Packet to the Mobile Node

This procedure is similar to the one presented in Home Test to the Mobile Node.

6.16 Payload Packet from the Home Agent

This procedure is similar to the one presented in Home Test from the Home Agent.

6.17 Establishing New Security Associations

Step 1. The mobile node wishes to send a Binding Update to the home agent.

```
IPv6 header (source = home address,
             destination = home agent)
Mobility header
   Binding Update
```

Step 2. There is no existing security association to protect the Binding Update, so IKE is initiated. The IKE packets are sent as shown in the following examples. The first packet is an example of an IKE packet sent from the mobile node, and the second one is from

the home agent. The examples shows also that the phase 1 identity used for the mobile node is a FQDN.

```
IPv6 header (source = care-of address,
             destination = home agent)
   UDP
   IKE
      ... IDii = ID_FQDN mn123.ha.net ...


IPv6 header (source = home agent
             destination = care-of address)
   UDP
   IKE
      ... IDir = ID_FQDN ha.net ...
```

Step 3. IKE phase 1 completes, and phase 2 is initiated to request security associations for protecting traffic between the mobile node's home address and the home agent. This involves sending and receiving additional IKE packets. The below example shows again one packet sent by the mobile node and another sent by the home agent. The example shows also that the phase 2 identity used for the mobile node is the mobile node's home address.

```
IPv6 header (source = care-of address,
             destination = home agent)
   UDP
   IKE
      ... IDci = ID_IPV6_ADDR home address ...

IPv6 header (source = home agent,
             destination = care-of address)
   UDP
   IKE
      ... IDcr = ID_IPV6_ADDR home agent ...
```

Step 4. The remaining steps are as shown in Binding Update to the Home Agent.

6.18 Rekeying Security Associations

Step 1. The mobile node and the home agent have existing security associations. Either side may decide at any time that the security associations need to be rekeyed, for instance, because the specified lifetime is approaching.
Step 2. Mobility header packets sent during rekey may be protected by the existing security associations.
Step 3. When the rekeying is finished, new security associations are established. In practice there is a time interval during which an old, about-to-expire security association and newly established security association will both exist. The new ones should be used as soon as they become available.
Step 4. A notification of the deletion of the old security associations is received. After this, only the new security associations can be used.

Note that there is no requirement that the existence of the IPsec and IKE security associations is tied to the existence of bindings. It is not necessary to delete a security association if a binding is removed, as a new binding may soon be established after this. Since cryptographic acceleration hardware may only be able to handle a limited number of active security associations, security associations may be deleted via IKE in order to keep the number of active cryptographic contexts to a minimum. Such deletions should not be interpreted as a sign of losing a contact to the peer or as a reason to remove a binding. Rather, if additional traffic needs to be sent, it is preferable to bring up another security association to protect it.

6.19 Movements and Dynamic Keying

In this section we describe the sequence of events that relate to movement with IKE-based security associations. In the initial state, the mobile node is not registered in any location and has no security associations with the home agent. Depending on whether the peers will be able to move IKE endpoints to new care-of addresses, the actions taken in Step 9 and 10 are different.
Step 1. Mobile node with the home address A moves to care-of address B.
Step 2. Mobile node runs IKE from care-of address B to the home agent, establishing a phase 1.
Step 3. Protected by this phase 1, mobile node establishes a pair of security associations for protecting Mobility Header traffic to and from the home address A.
Step 4. Mobile node sends a Binding Update and receives a Binding Acknowledgement using the security associations created in Step 3.
Step 5. Mobile node establishes a pair of security associations for protecting return routability packets. These security associations are in tunnel mode and their endpoint in the mobile node side is care-of address B. For the purposes of our example, this step uses the phase 1 connection established in Step 2. Multiple phase 1 connections are also possible.
Step 6. The mobile node uses the security associations created in Step 5 to run return routability.
Step 7. The mobile node moves to a new location and adopts a new care-of address C.
Step 8. Mobile node sends a Binding Update and receives a Binding Acknowledgement using the security associations created in Step 3. The home agent ensures that the next packets sent using the security associations created in Step 5 will have the new care-of address as their destination address, as if the destination gateway address in the security association had changed.
Step 9. If the mobile node and the HA have the capability to change the IKE endpoints, they change the address to C. If they dont have the capability, both nodes remove their phase 1 connections created on top of the care-of address B and establish a new IKE phase 1 on top of the care-of address C. This capability to change the IKE phase 1 end points is indicated through setting the Key Management Mobility Capability (K) flag[8] in the Binding Update and Binding Acknowledgement messages.
Step 10. If a new IKE phase 1 connection was setup after movement, the MN will not be able to receive any notifications delivered on top of the old IKE phase 1 security association. Notifications delivered on top of the new security association are received and processed normally. If the mobile node and HA were able to update the IKE endpoints, they can continue using the same IKE phase 1 connection.

TOC

7. Implementation Considerations

We have chosen to require an encapsulation format for return routability and payload packet protection which can only be realized if the destination of the IPsec packets sent from the home agent can be changed as the mobile node moves. One of the main reasons for choosing such a format is that it removes the overhead of twenty four bytes when a home address option or routing header is added to the tunneled packet. What is needed is that the home agent must act as if the gateway address of a security association to the mobile node would have changed. Implementations are free to choose any particular method to make this change, such as using an API to the IPsec implementation to change the parameters of the security association, removing the security association and installing a new one, or modification of the packet after it has gone through IPsec processing. The only requirement is that after registering a new binding at the home agent, the next IPsec packets sent on this security association will be addressed to the new care-of address.
We have also chosen to require that a dynamic key management protocol must be able to make an authorization decision for IPsec security association creation with different addresses than with what the key management protocol is run. We expect this to be done typically by configuring the allowed combinations of phase 1 user identities and home addresses.
The base Mobile IPv6 specification sets high requirements for a so-called Bump-In-The-Stack (BITS) implementation model of IPsec. As Mobile IPv6 specific modifications of the packets are required after IPsec processing, the BITS implementation has to perform also some tasks related to mobility. This may increase the complexity of the implementation, even if it already performs some tasks of the IP layer (such as fragmentation).
We have chosen to require policy entries that are specific to a tunnel interface. This means that implementations have to regard the Home Agent - Mobile Node tunnel as a separate interface on which IPsec SPDs can be based.
A further complication of the IPsec processing on a tunnel interface is that this requires access to the BITS implementation before the packet actually goes out.
When certificate authentication is used, IKE fragmentation can be encountered. This can occur when certificate chains are used, or even with single certificates if they are large. Many firewalls do not handle fragments properly, and may drop them. Routers in the path may also discard fragments after the initial one, since they typically will not contain full IP headers that can be compared against an access list. Where fragmentation occurs, the endpoints will not always be able to establish a security association.
Fortunately, typical Mobile IPv6 deployment uses short certificate chains, as the mobile node is communicating directly with its home network. Nevertheless, where the problem appears, one solution is to replace the firewalls or routers with equipment that can properly support fragments. If this cannot be done, it may help to store the peer certificates locally, or to obtain them through other means.

TOC

8. Security Considerations

The Mobile IPv6 base specification[8] requires strong security between the mobile node and the home agent. This memo discusses how that security can be arranged in practice, using IPsec.

Normative References

TOC

[1]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[2]	Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998 (TXT, HTML, XML).
[3]	Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998 (TXT, HTML, XML).
[4]	Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998 (TXT, HTML, XML).
[5]	Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998 (TXT, HTML, XML).
[6]	Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998 (TXT, HTML, XML).
[7]	Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998 (TXT, HTML, XML).
[8]	Perkins, C., Johnson, D. and J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-21 (work in progress), February 2003.

Informative References

TOC

[9]	Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
[10]	Droms, R., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-dhcpv6-28 (work in progress), November 2002.
[11]	Kivinen, T., Huttunen, A., Swander, B. and V. Volpe, "Negotiation of NAT-Traversal in the IKE", draft-ietf-ipsec-nat-t-ike-04 (work in progress), November 2002.
[12]	Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", draft-vida-mld-v2-06 (work in progress), December 2002.

Authors' Addresses

TOC

	Jari Arkko
	Ericsson
	Jorvas 02420
	Finland
EMail:	jari.arkko@ericsson.com

	Vijay Devarapalli
	Nokia Research Center
	313 Fairchild Drive
	Mountain View CA 94043
	USA
EMail:	vijayd@iprg.nokia.com
	Francis Dupont
	ENST Bretagne
	Campus de Rennes 2, rue de la Chataigneraie
	BP 78
	Cesson-Sevigne Cedex 35512
	France
EMail:	Francis.Dupont@enst-bretagne.fr

TOC

Appendix A. Acknowledgements

The authors would like to thank Greg O'Shea, Michael Thomas, Kevin Miles, Cheryl Madson, Bernard Aboba, Erik Nordmark, and Gabriel Montenegro for interesting discussions in this problem space.

TOC

Appendix B. Changes from Previous Version

The following changes have been made to this document from version 02:

*It is now better explained why the mobile node can change its source address in security associations before such a change is told to the home agent (tracked issue 249).

*The support for protecting prefix discovery with IPsec has been made mandatory, but use is still a SHOULD (tracked issue 249).

*Requirements for security association and policy configuration for new home addresses received through prefix discovery have been specified (tracked issue 243).

*IPsec protocol and mode requirements have now been stated as minimal requirements and no longer prevent the use of other protocols (AH) and modes (tracked issue 228).

*The specification explicitly discourages the use of nested IPsec encapsulation (tracked issue 219).

*The different types of requests for phase 2 security associations have been explained in the requirements section. This relates to using IKE for creating security associations for Binding Update protection or other tasks (tracked issue 219).

*Many editorial modifications have been performed.

TOC

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

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