Network Working Group
Request for Comments: 4877
Updates: 3776
Category: Standards Track

V. Devarapalli
Azaire Networks
F. Dupont
CELAR

April 2007

Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture

Status of This Memo

Copyright Notice

Abstract

This document describes Mobile IPv6 operation with the revised IPsec architecture and IKEv2.

Table of Contents

1. Introduction

RFC 3776 describes how IPsec, as described in RFC 2401 [11], is used with Mobile IPv6 [2] to protect the signaling messages. It also illustrates examples of Security Policy Database and Security Association Database entries that can be used to protect Mobile IPv6 signaling messages.

The IPsec architecture has been revised in RFC 4301 [5]. Among the many changes, the list of selectors has been expanded to include the Mobility Header message type. This has an impact on how security policies and security associations are configured for protecting mobility header messages. It becomes easier to differentiate between the various Mobility Header messages based on the type value instead of checking if a particular mobility header message is being sent on a tunnel interface between the mobile node and the home agent, as it was in RFC 3776. The revised IPsec architecture specification also includes ICMP message type and code as selectors. This makes it possible to protect Mobile Prefix Discovery messages without applying the same security associations to all ICMPv6 messages.

This document discusses new requirements for the home agent and the mobile node to use the revised IPsec architecture and IKEv2. Section 4 lists the requirements. Sections 6 and 7 describe the required Security Policy Database (SPD) and Security Association Database (SAD) entries.

The Internet Key Exchange (IKE) protocol has also been substantially revised and simplified [4]. Section 7.3 of this document describes how IKEv2 can be used to set up security associations for Mobile IPv6.

The use of EAP within IKEv2 is allowed to authenticate the mobile node to the home agent. This is described in Section 8. A method for dynamically configuring a home address from the home agent using the Configuration Payload in IKEv2 is described in Section 9.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

3. Packet Formats

The mobile node and the home agent MUST support the packet formats as defined in Section 3 of RFC 3776.

In case the mobile node reverse tunnels all traffic including Mobile IPv6 signaling messages exchanged between the mobile node and the home agent, then the Home Address Option is not required to be present in the messages sent to the home agent. The packet format for the binding update when sent in the tunnel mode looks as follows.

```
IPv6 hdr (source = care-of address,
          destination = home agent)
ESP header in tunnel mode
IPv6 hdr (source = home address,
          destination = home agent)
Mobility Header
   Binding Update
     Alternate Care-of Address option (care-of address)
```

The binding acknowledgement sent to the mobile node when it is away from the home link looks as follows.

```
IPv6 hdr (source = home agent,
          destination = care-of address)
ESP header in tunnel mode
IPv6 hdr (source = home agent,
          destination = home address)
Mobility Header
   Binding Acknowledgement
```

The packet formats for tunneled mobile prefix discovery messages are very similar to the tunneled Binding Update and Binding Acknowledgment with the with the home address as the source address in the inner IP header.

The support for the above tunneled packet format is optional on the mobile node and the home agent.

4. Requirements

This section describes mandatory rules and requirements for all Mobile IPv6 mobile nodes and home agents so that IPsec, with IKEv2 as the key management protocol, can be used to protect traffic between the mobile node and the home agent. Many of the requirements are repeated from RFC 3776 to make this document self-contained and complete.

4.1. General Requirements

- RFC 3775 states that manual configuration of IPsec security associations MUST be supported, and automated key management MAY be supported. This document does not make any recommendations regarding the support of manual IPsec configuration and dynamic IPsec configuration. This document just describes the use of manually created IPsec security associations and the use of IKEv2 as the automated IPsec key management protocol for protecting Mobile IPv6 signaling messages.

- ESP encapsulation for Binding Updates and Binding Acknowledgements MUST be supported and used.

- ESP encapsulation in tunnel mode for the Home Test Init (HoTi) and Home Test (HoT) messages tunneled between the mobile node and the home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to mobile prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and the 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.

- The home agent and the mobile node MAY support authentication using EAP in IKEv2 as described in Section 8.

- The home agent and the mobile node MAY support remote configuration of the home address as described in Section 9. When the home agent receives a configuration payload with a CFG_REQUEST for INTERNAL_IP6_ADDRESS, it must reply with a valid home address for the mobile node. The home agent can pick a home address from a local database or from a DHCPv6 server on the home link.

4.2. Policy Requirements

The following requirements are related to the configuration of the security policy database on the home agent and the mobile node.

- RFC 3776 required configuration of the security policies per interface in order to be able to differentiate between mobility header messages sent to the home agent and those tunneled through the home agent to the correspondent node. Since the Mobility Header message type is a selector, it is now easy to differentiate between HoTi and HoT messages from other mobility header messages. Therefore per-interface configuration of security policies is not required for protecting mobility header messages. Note that without per-interface security policies, payload packet protection is limited to packets originating/terminating at the home address. Traffic using a link local address within the Mobile IP tunnel cannot be provided IPsec protection without per-interface security policies.

- The home agent MUST be able to prevent a mobile node from using its security association to send a Binding Update on behalf of another mobile node. With manual IPsec configuration, the home agent MUST be able to verify that a security association was created for a particular home address. With dynamic keying, the home agent MUST be able to verify that the identity presented in the IKE_AUTH exchange is allowed to create security associations for a particular home address.

- The home agent uses the Peer Authorization Database (PAD) [5] to store per-mobile node state. More specifically the per-mobile state stores information that is used to authenticate the mobile node and the authorization information that ties the mobile node's identity to the home address of the mobile node. This will allow the home agent to prevent a mobile node from creating IPsec security associations for another mobile node's home address. In case of dynamic home address assignment, the home agent creates a temporary PAD entry linking the authenticated peer identity and the newly allocated home address.

- As required in the base specification [2], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

Similar implementation considerations apply to the Routing header processing as was described above for the Home Address destination option.

- 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 security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent, SHOULD be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are 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 away from home again. The security associations protecting Binding Updates, Binding Acknowledgements and Mobile Prefix Discovery messages SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

- The mobile node MUST use the Home Address destination option in Binding Updates and Mobile Prefix Solicitations when transport mode IPsec protection is used, so that the home address is visible when the IPsec policy checks are made.

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

4.3. IPsec Protocol Processing Requirements

The following lists requirements for IPsec processing at the Home Agent and the mobile node.

- The home agent and mobile node SHOULD support Mobility Header message type as an IPsec selector.

- The home agent and mobile node SHOULD support ICMPv6 message type as an IPsec selector.

- The home agent MUST be able to distinguish between HoTi messages sent to itself (when it is acting as a Correspondent Node) and those sent to Correspondent Nodes (when it is acting as a home agent) based on the destination address of the packet.

- When securing Binding Updates, Binding Acknowledgements, and Mobile Prefix Discovery messages, both the mobile node and the home agent MUST support the use of the Encapsulating Security Payload (ESP) [6] 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. The use of sequence number in the ESP header to provide anti-replay protection is optional because the sequence numbers in the Binding Updates provide anti-replay protection. However, the anti-replay protection fails if the home agent loses the binding cache state, for example, due to a reboot. Since the IPsec security association state can also be assumed to be lost, ESP cannot provide anti-replay protection in this case. Complete anti-replay protection can only be provided by the use of a dynamic keying mechanism, like IKEv2.

  Support for protecting these messages using ESP in tunnel mode is optional.

- 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 a non-null authentication algorithm MUST be applied.

- When ESP is used to protect Binding Updates, there is no protection for the care-of address that 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 with. 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 Binding Updates sent by mobile nodes while away from home. The exception to this is when the mobile node returns home and sends a Binding Update to the home agent in order to de-register.

  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.

- 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 outer header destination address in the security association had changed. Similarly, the home agent starts to expect the new source address in the tunnel packets received from the mobile node.

Such address changes can be implemented, for instance, through an API from the Mobile IPv6 implementation to the IPsec implementation. One such API is described in [12]. It should be noted that the use of such an API and the address changes MUST only be done based on the Binding Updates received by the home agent and protected by the use of IPsec. Address modifications based on other sources, such as Binding Updates to the correspondent nodes protected by return routability, or open access to an API from any application may result in security vulnerabilities.

4.4. Dynamic Keying Requirements

The following requirements are related to the use of a dynamic key management protocol by the mobile node and the home agent. Section 7.3 describes the use of IKEv2 as the dynamic key management protocol.

- o The mobile node MUST use its care-of address as source address in protocol exchanges, when using dynamic keying.

- o The mobile node and the home agent MUST create security associations based on the home address, so that the security associations survive changes in care-of address. When using IKEv2 as the key exchange protocol, the home address should be carried as the initiator IP address in the TSi payload during the CREATE_CHILD_SA exchange [4].

- o If the mobile node has used IKEv2 to establish security associations with its home agent, it should follow the procedures discussed in Sections 11.7.1 and 11.7.3 of the base specification [2] to determine whether the IKE endpoints can be moved or if the SAs, including the IKEv2 SA, have to be re-established.

- o If the home agent has used IKEv2 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 [2] to determine whether the IKE endpoints can be moved or if the SAs, including the IKEv2 SA, have to be re-established.

5. Selector Granularity Considerations

IPsec implementations are compatible with this document even if they do not support fine-grain selectors such as the Mobility Header message type and ICMPv6 message type. Note that such IPsec implementations are not compliant with RFC 4301 [5]. For various reasons, some implementations may choose to support only coarse-grain selectors (i.e., addresses and in some cases the protocol field) for forwarded traffic. As finer-grain selectors give better control, i.e., the protection is only applied when required, the examples in this document always use the finest granularity.

The following describes different ways of setting up IPsec policies for protecting Mobile IPv6 messages:

1. The IPsec implementations on the mobile node and the home agent support fine-grain selectors, including the Mobility Header message type. This is the case assumed in the IPsec SPD and SAD examples in this document.

2. The IPsec implementations only support selectors at a protocol level. Such an IPsec implementation can only identify mobility header traffic and cannot identify the individual mobility header messages. In this case, the protection of Return Routability Messages uses a setup similar to the regular payload packets sent to the correspondent node with the protocol selector set to Mobility Header. All tunneled Mobility Header messages will be protected.

3. The third case is where the protocol selector is not available in the IPsec implementation. In this case, all traffic sent by the mobile node that is reverse tunneled through the home agent is protected using ESP in tunnel mode. This case is also applicable when the mobile node, due to privacy considerations, tunnels all traffic to the home agent. This includes Mobile IPv6 signaling messages exchanged between the mobile node and the home agent and all traffic exchanged between the mobile node and the correspondent node. This case uses IPsec tunnel mode SA with the protocol selector set to 'any'.

The third case where all tunneled traffic is protected introduces some additional considerations:

- o If there is just one IPsec SA providing protection for all traffic, then the SA MUST fulfill the requirements for protecting the Return Routability messages which require confidentiality protection. If the third case is being used for privacy considerations, then there can also be separate tunnel mode SPD entries for protecting the Return Routability messages with a higher priority in the SPD so that the SPD entry with the higher priority gets applied first.

- The receipt of a Binding Update from the new care-of address updates the tunnel endpoint of the IPsec SA as described in Section 4.3. Since the Binding Update that updates the tunnel endpoint is received through the same tunnel interface that needs to be updated, special care should be taken on the home agent to ensure that the Binding Update is not dropped. This can be achieved either by performing the source address check on the outer IPv6 header after the binding update is processed or by having exception handling to check the inner packet for a Binding Update when the source address match on the outer source address fails. Typical IPsec processing does not check the outer source address when the originator of the packet has already been authenticated.

6. Manual Configuration

This section describes the SPD and SAD entries that can be used to protect Mobile IPv6 signaling messages. The SPD and SAD entries are only example configurations. A particular mobile node implementation and a home agent implementation could configure different SPD and SAD entries as long as they provide the required security of the Mobile IPv6 signaling messages.

For the examples described in this document, a mobile node with home address, "home_address_1", primary care-of address, "care_of_address_1", a home agent with address, "home_agent_1" and a user of the mobile node with identity "user_1" are assumed. If the home address of the mobile node changes, the SPD and SAD entries need to be re-created or updated for the new home address.

The Peer Authorization Database is not used when manual IPsec configuration is used for setting up security associations for protecting Mobile IPv6 signaling messages.

6.1. Binding Updates and Acknowledgements

The following are the SPD and SAD entries on the mobile node and the home agent to protect Binding Updates and Acknowledgements.

```
mobile node SPD-S:
  - IF local_address = home_address_1 &
       remote_address = home_agent_1 & proto = MH &
       local_mh_type = BU & remote_mh_type = BAck
    Then use SA SA1 (OUT) and SA2 (IN)

mobile node SAD:
  - SA1(OUT, spi_a, home_agent_1, ESP, TRANSPORT):
    local_address = home_address_1 &
    remote_address = home_agent_1 &
    proto = MH & mh_type = BU
  - SA2(IN, spi_b, home_address_1, ESP, TRANSPORT):
    local_address = home_agent_1 &
    remote_address = home_address_1 &
    proto = MH & mh_type = BAck

home agent SPD-S:
  - IF local_address = home_agent_1 &
       remote_address = home_address_1 & proto = MH &
       local_mh_type = BAck & remote_mh_type = BU
    Then use SA SA2 (OUT) and SA1 (IN)

home agent SAD:
  - SA2(OUT, spi_b, home_address_1, ESP, TRANSPORT):
    local_address = home_agent_1 &
    remote_address = home_address_1 &
    proto = MH & mh_type = BAck
  - SA1(IN, spi_a, home_agent_1, ESP, TRANSPORT):
    local_address = home_address_1 &
    remote_address = home_agent_1 &
    proto = MH & mh_type = BU
```

6.2. Return Routability Messages

The following are the SPD and SAD entries on the mobile node and the home agent to protect Return Routability messages.

```
mobile node SPD-S:
  - IF local_address = home_address_1 & remote_address = any &
    proto = MH & local_mh_type = HoTi & remote_mh_type = HoT
    Then use SA SA3 (OUT) and SA4 (IN)

mobile node SAD:
  - SA3(OUT, spi_c, home_agent_1, ESP, TUNNEL):
    local_address = home_address_1 & remote_address = any &
    proto = MH & mh_type = HoTi
  - SA4(IN, spi_d, care_of_address_1, ESP, TUNNEL):
    local_address = any & remote_address = home_address_1 &
    proto = MH & mh_type = HoT

home agent SPD-S:
  - IF remote_address = home_address_1 & local_address = any &
    proto = MH & local_mh_type = HoT & remote_mh_type = HoTi
    Then use SA SA4 (OUT) and SA3 (IN)

home agent SAD:
  - SA4(OUT, spi_d, care_of_address_1, ESP, TUNNEL):
    local_address = any & remote_address = home_address_1 &
    proto = MH & mh_type = HoT
  - SA3(IN, spi_c, home_agent_1, ESP, TUNNEL):
    local_address = home_address_1 & remote_address = any &
    proto = MH & mh_type = HoTi
```

6.3. Mobile Prefix Discovery Messages

The following are the SPD and SAD entries used to protect Mobile Prefix Discovery messages.

```
      mobile node SPD-S:
        - IF local_address = home_address_1 &
             remote_address = home_agent_1 & proto = ICMPv6 &
             local_icmp6_type = MPS & remote_icmp6_type = MPA
          Then use SA SA5 (OUT) and SA6 (IN)

      mobile node SAD:
        - SA5(OUT, spi_e, home_agent_1, ESP, TRANSPORT):
          local_address = home_address_1 &
          remote_address = home_agent_1 &
          proto = ICMPv6 & icmp6_type = MPS
        - SA6(IN, spi_f, home_address_1, ESP, TRANSPORT):
          local_address = home_agent_1 &
          remote_address = home_address_1 &
          proto = ICMPv6 & icmp6_type = MPA

      home agent SPD-S:
        - IF local_address = home_agent_1 &
             remote_address = home_address_1 & proto = ICMPv6 &
             local_icmp6_type = MPA & remote_icmp6_type = MPS
          Then use SA SA6 (OUT) and SA5 (IN)

      home agent SAD:
        - SA6(OUT, spi_f, home_address_1, ESP, TRANSPORT):
          local_address = home_agent_1 &
          remote_address = home_address_1 &
          proto = ICMPv6 & icmp6_type = MPA
        - SA5(IN, spi_e, home_agent_1, ESP, TRANSPORT):
          local_address = home_address_1 &
          remote_address = home_agent_1 &
          proto = ICMPv6 & icmp6_type = MPS
```

6.4. Payload Packets

Regular payload traffic between the mobile node and the correspondent node tunneled through the home agent can be protected by IPsec, if required. The mobile node and the home agent use ESP in tunnel mode to protect the tunneled traffic. The SPD and SAD entries shown in Section 5.2.4 of [3] are applicable here.

7. Dynamic Configuration

This section describes the use of IKEv2 to set up the required security associations.

7.1. Peer Authorization Database Entries

The following describes PAD entries on the mobile node and the home agent. The PAD entries are only example configurations. Note that the PAD is a logical concept; a particular mobile node and a home agent can implement the PAD in an implementation-specific manner. The PAD state may also be distributed across various databases in a specific implementation.

```
    mobile node PAD:
      - IF remote_identity = home_agent_identity_1
           Then authenticate (shared secret/certificate/)
           and authorize CHILD_SA for remote address home_agent_1

    home agent PAD:
      - IF remote_identity = user_1
           Then authenticate (shared secret/certificate/EAP)
           and authorize CHILD_SAs for remote address home_address_1
```

The list of authentication mechanisms in the above examples is not exhaustive. There could be other credentials used for authentication stored in the PAD.

In case of dynamic home address assignment, the home agent creates a temporary PAD entry linking the authenticated peer identity and the newly allocated home address.

7.2. Security Policy Database Entries

The following sections describe the security policy entries on the mobile node and the home agent. The SPD entries are only example configurations. A particular mobile node implementation and a Home Agent implementation could configure different SPD entries as long as they provide the required security of the Mobile IPv6 signaling messages.

In the examples shown below, the identity of the user of the mobile node is assumed to be user_1, the home address of the mobile node is assumed to be home_address_1, the primary care-of address of the mobile node is assumed to be care_of_address_1, and the IPv6 address of the Home Agent is assumed to be home_agent_1.

7.2.1. Binding Updates and Acknowledgements

The following are the SPD entries on the mobile node and the home agent for protecting Binding Updates and Acknowledgements.

```
    mobile node SPD-S:
      - IF local_address = home_address_1 &
           remote_address = home_agent_1 &
           proto = MH & local_mh_type = BU & remote_mh_type = BAck
        Then use SA ESP transport mode
        Initiate using IDi = user_1 to address home_agent_1

    home agent SPD-S:
      - IF local_address = home_agent_1 &
           remote_address = home_address_1 &
           proto = MH & local_mh_type = BAck & remote_mh_type = BU
        Then use SA ESP transport mode
```

In the examples shown above, the home address of the mobile node might not be available all the time. For instance, the mobile node might not have configured a home address yet. When the mobile node acquires a new home address, it must either add the address to the corresponding SPD entries or create the SPD entries for the home address.

The home agent should have named SPD entries per mobile node, based on the identity of the mobile node. The identity of the mobile node is stored in the "Name" selector in the SPD [5]. The home address presented by the mobile node during the IKE negotiation is stored as the remote IP address in the resultant IPsec security associations. If the mobile node dynamically configures a home agent and the home address, the home agent may not know which mobile nodes it is supposed to be serving. Therefore, the home agent cannot have SPD entries configured per mobile node. Instead, the home agent should have generic SPD entries to prevent mobility header traffic that requires IPsec protection from bypassing the IPsec filters. Once a mobile node authenticates to the home agent and configures a home address, appropriate SPD entries are created for the mobile node.

The Mobility Header message type is negotiated by placing it in the most significant eight bits of the 16-bit local "port" selector during IKEv2 exchange. For more details, refer to [5]. The TSi and TSr payloads in the above examples will contain many other selectors apart from home_address_1. For the sake of brevity, we show only those values that are relevant for Mobile IPv6.

7.2.2. Return Routability Messages

The following are the SPD entries on the mobile node and the home agent for protecting the Return Routability messages.

```
    mobile node SPD-S:
      - IF local_address = home_address_1 & remote_address = any &
           proto = MH & local_mh_type = HoTi & remote_mh_type = HoT
        Then use SA ESP tunnel mode
        Initiate using IDi = user_1 to address home_agent_1

    home agent SPD-S:
      - IF local_address = any & remote_address = home_address_1 &
           proto = MH & local_mh_type = HoT & remote_mh_type = HoTi
        Then use SA ESP tunnel mode
```

When the mobile node's care-of address changes, the SPD entries on both the mobile node and the home agent must be updated. The home agent knows about the change in care-of address of the mobile node when it receives a Binding Update from the mobile node.

7.2.3. Mobile Prefix Discovery Messages

The following are the SPD entries on the mobile node and the home agent for protecting Mobile Prefix Discovery messages.

```
    mobile node SPD-S:
      - IF local_address = home_address_1 &
           remote_address = home_agent_1 &
           proto = ICMPv6 & local_icmp6_type = MPS &
           remote_icmp6_type = MPA
        Then use SA ESP transport mode
        Initiate using IDi = user_1 to address home_agent_1

     home agent SPD-S:
      - IF local_address = home_agent_1 &
           remote_address = home_address_1 &
           proto = ICMPv6 & local_icmp6_type = MPA &
           remote_icmp6_type = MPS
        Then use SA ESP transport mode
```

In the examples shown above, the home address of the mobile node might not be available all the time. When the mobile node acquires a new home address, it must add the address to the corresponding SPD entries.

The TSi and TSr payloads in the above examples will contain many other selectors apart from home_address_1. For brevity, they are not shown here.

7.2.4. Payload Packets

The following are the SPD entries on the mobile node and the home agent if payload traffic exchanged between the mobile node and its Correspondent Node needs to be protected. The SPD entries are similar to the entries for protecting Return Routability messages and have lower priority than the above SPD entries.

```
    mobile node SPD-S:
      - IF interface = IPv6 tunnel to home_agent_1 &
        source = home_address_1 & destination = any & proto = X
        Then use SA ESP tunnel mode
        Initiate using IDi = user_1 to address home_agent_1

    home agent SPD-S:
      - IF interface = IPv6 tunnel to home_address_1 &
        source = any & destination = home_address_1 & proto = X
        Then use SA ESP tunnel mode
```

7.3. Security Association Negotiation Using IKEv2

Mobile IPv6 signaling messages are typically initiated by the mobile node. The mobile node sends a Binding Update to the home agent whenever it moves and acquires a new care-of address.

The mobile node initiates an IKEv2 protocol exchange if the required security associations are not present. A possible mechanism used for mutual authentication is a shared secret between the mobile node and the home agent. The home agent uses the identity of the mobile node to identify the corresponding shared secret. When a public-key-based mechanism is available, it should be the preferred mechanism for mutual authentication.

If a shared secret is being used, the mobile node uses the shared secret to generate the AUTH payload in the IKE_AUTH exchange. If the mobile node is using a public-key-based mechanism, then it uses its private key to generate the AUTH payload in the IKE_AUTH exchange.

```
    Mobile Node                          Home Agent
    -----------                          ----------
    HDR, SAi1, KEi, Ni      -->

                          <--      HDR, SAr1, KEr, Nr, [CERTREQ]

    HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,]
             AUTH, SAi2, TSi, TSr}
                            -->

                          <--      HDR, SK {IDr, [CERT,] AUTH,
                                             SAr2, TSi, TSr}
```

The mobile node always includes its identity in the IDi payload in the IKE_AUTH exchange. The mobile node could use the following different types of identities to identify itself to the home agent.

- o Home Address - The mobile node could use its statically configured home address as its identity. In this case the ID Type field is set to ID_IPV6_ADDR.
- o FQDN - The mobile node can use a Fully Qualified Domain Name as the identifier and set the ID Type field to ID_FQDN.
- o RFC 822 identifier - If the mobile node uses a RFC 822 identifier [9], it sets the ID Type field to ID_RFC822_ADDR.

The above list of identities is not exhaustive.

In the IKE_AUTH exchange, the mobile node includes the home address and the appropriate selectors in the TSi (Traffic Selector-initiator) payload to negotiate IPsec security associations for protecting the Binding Update and Binding Acknowledgement messages. The mobile node MAY use a range of selectors that includes the mobility message types for Binding Update and Binding Acknowledgement to use the same pair of IPsec security associations for both messages.

After the IKE_AUTH exchange completes, the mobile node initiates CREATE_CHILD_SA exchanges to negotiate additional security associations for protecting Return Routability signaling, Mobile Prefix Discovery messages, and (optionally) payload traffic. The CREATE_CHILD_SA exchanges are protected by IKEv2 security associations created during the IKE_SA_INIT exchange. If a correspondent node, that is also a mobile node, initiates the return routability exchange, then the home agent initiates the CREATE_CHILD_SA exchange to negotiate security associations for protecting Return Routabilty messages.

It is important that the security associations are created based on the home address of the mobile node, so that the security associations survive care-of address change. The mobile node MUST use its home address as the initiator IP address in the TSi payload in the CREATE_CHILD_SA exchange in order to create the IPsec security associations for the home address.

```
     Mobile Node                      Home Agent
     -----------                      ----------
     HDR, SK {[N], SA, Ni, [KEi],
              [TSi, TSr]}    -->

                             <--      HDR, SK {SA, Nr, [KEr],
                                               [TSi, TSr]}
```

When PKI-based authentication is used between the mobile node and the Home Agent, the identity presented by the mobile node in the IDi payload MUST correspond to the identity in the certificate obtained by the Home Agent. The home agent uses the identity presented in the IDi payload to lookup the policy and the certificate that corresponds to the mobile node. If the mobile node presents its home address in the IDi payload, then the home agent MUST verify that the home address matches the address in an iPAddress field in the SubjectAltName extension [8].

When the mobile node uses its home address in the IDi field, implementations are not required to match the source address in the outermost IP header with the IP address in the IDi field. According to RFC 4306 [4], the IP header fields in the IKEv2 messages are ignored and used only in the IP headers for IKEv2 messages sent as replies.

7.4. Movements and Dynamic Keying

If the mobile node moves and its care-of address changes, the IKEv2 SA might not be valid. RFC 3775 defines a mechanism based on the successful exchange of Binding Update and Binding Acknowledgement messages. The mobile node establishes the IKE SA with the home agent using its primary care-of address. The IKE SA endpoints are updated on the home agent when it receives the Binding Update from the mobile node's new care-of address and on the mobile node when it sends the Binding Update to the home agent or when it receives the Binding acknowledgement sent by the home agent. This capability to change IKE endpoints is indicated through setting the Key Management Capability (K) flag [2] in the Binding Update and Binding Acknowledgement messages. If the mobile node or the home agent does not support this capability, and has no other means to update the addresses, then an IKEv2 exchange MUST be initiated to re-establish a new IKE SA.

8. The Use of EAP Authentication

In addition to using public key signatures and shared secrets, EAP [10] can be used with IKEv2 for authenticating the mobile node to the home agent.

The mobile node indicates that it wants to use EAP by including the IDi payload but leaving out the AUTH payload in the first message during the IKE_AUTH exchange. The home agent then includes an EAP payload if it is willing to use an extensible authentication method. Security associations are not created until the subsequent IKE_AUTH exchange after successful EAP authentication. The use of EAP adds at least two round trips to the IKE negotiation. The number of round trips depends on the EAP method used.

```
     Mobile Node                            Home Agent
     ------------                           ----------
     HDR, SAi1, KEi, Ni      -->

                             <--     HDR, SAr1, KEr, Nr, [CERTREQ]

     HDR, SK {IDi, [CERTREQ,] [IDr,]
              SAi2, TSi, TSr}-->

                             <--     HDR, SK {IDr, [CERT,] AUTH,
                                              EAP }
                               .
                               .
                               .

     HDR, SK {EAP}           -->

                             <--     HDR, SK {EAP (success)}

     HDR, SK {AUTH}          -->

                             <--     HDR, SK {AUTH, SAr2, TSi,
                                              TSr}
```

When EAP is used, the identity presented by the mobile node in the IDi field may not be the actual identity of the mobile node. It could be set to an identity that is used only for Authentication, Authorization, and Accounting (AAA) routing purposes and selecting the right EAP method. It is possible that the actual identity is carried inside EAP, invisible to the home agent. While IKEv2 does not allow an EAP Identity Request/Response message exchange, EAP methods may exchange identities within themselves. In this case, the home agent MUST acquire the mobile node's identity from the corresponding AAA server. How the home agent acquires the mobile node's identity is out of scope for this document.

Some EAP methods, when used with IKEv2, generate a shared key on the mobile node and the Home Agent once the EAP authentication succeeds. This shared key is used to generate the AUTH payloads in the subsequent IKEv2 messages. The shared key, if used to generate the AUTH payloads, MUST NOT be used for any other purpose. For more details, refer to [4].

The use of EAP between the mobile node and the home agent might require the home agent to contact an authorization server like the AAA Home server, on the home link, to authenticate the mobile node. Please refer to [7] for more details.

9. Dynamic Home Address Configuration

The mobile node can dynamically configure a home address by including a Configuration Payload in the IKE_AUTH exchange, with a request for an address from the home link. The mobile node should include a zero-length INTERNAL_IP6_ADDRESS attribute in the CFG_REQUEST Payload. The mobile node MAY include multiple instances of the INTERNAL_IP6_ADDRESS to request multiple home address to the assigned by the home agent.

When the home agent receives a configuration payload with a CFG_REQUEST for INTERNAL_IP6_ADDRESS, it replies with a valid home address for the mobile node. The INTERNAL_IP6_ADDRESS attribute in the CFG_REPLY contains the prefix length of the home prefix in addition to a 128 bit home address. The home agent could use a local database or contact a DHCPv6 server on the home link to allocate a home address. The duration for which the home address is allocated to the mobile node is the same as the duration for which an IKEv2 security association exists between the mobile node and the home agent. If the IKEv2 security association is rekeyed, the home address lifetime is also extended.

```
    Mobile Node                          Home Agent
    -----------                          ----------
    HDR, SK {IDi, [CERT,] [CERTREQ,]
             [IDr,] AUTH, CP(CFG_REQUEST),
             SAi2, TSi, TSr}
                           -->

                           <--   HDR, SK {IDr, [CERT,] AUTH,
                                          CP(CFG_REPLY), SAr2,
                                          TSi, TSr}
```

The mobile node could suggest a home address that it wants to use in the CFG_REQUEST. For example, this could be a home address that was allocated for the mobile node before or an address that the mobile node auto-configured from the IPv6 prefix on the home link. The Home Agent could let the mobile node use the same home address by setting the INTERNAL_IP6_ADDRESS attribute in the CFG_REPLY payload to the same home address. If the home agent wants the mobile node to use a different home address, it sends a new home address in the INTERNAL_IP6_ADDRESS attribute in the CFG_REPLY payload. The Mobile Node MUST stop using its old home address and start using the newly allocated home address.

In case the home agent is unable to allocate a home address for the mobile node during the IKE_AUTH exchange, it MUST send a Notify Payload with an INTERNAL_ADDRESS_FAILURE message. When the mobile node receives a Notify Payload with an INTERNAL_ADDRESS_FAILURE message, it SHOULD terminate the IKE_AUTH exchange. The mobile node then should initiate a new IKE_SA_INIT and IKE_AUTH exchange and try to auto-configure a home address as described in [13]. The mobile node MAY also switch to another home agent. The new home agent address can be obtained by consulting a home agent list received during a previous home agent discovery phase or, if such list is empty or not available, by attempting a new home agent discovery.

If the mobile node wants to configure a DNS server from the home link, it can request the DNS server information by including an INTERNAL_IP6_DNS attribute in the CFG_REQUEST payload.

10. Security Considerations

This document describes how IPsec can be used to secure Mobile IPv6 signaling messages. Please refer to RFC 3775 [2] for security considerations related to the use of IPsec with Mobile IPv6.

A misbehaving mobile node could create IPsec security associations for a home address that belongs to another mobile node. Therefore, the home agent should check if a particular mobile node is authorized to use a home address before creating IPsec security associations for the home address. If the home address is assigned as described in Section 9, the home agent MUST associate the home address with the identity used in IKE negotiation. The home agent MAY store the assigned home address in the SPD entries created for the mobile node.

The use of EAP for authenticating the mobile node to the home agent is described in Section 8. Security considerations related to the use of EAP with IKEv2 are described in [4].

11. Acknowledgements

The authors would like to thank Mika Joutsenvirta, Pasi Eronen, Jari Arkko, Gerardo Giaretta, Shinta Sugimoto, Tero Kivinen, Steve Bellovin, Kilian Weniger, and Vijay Gurbani for reviewing the document.

Many of the requirements listed in Section 4 are copied from RFC 3776. Therefore, the authors of RFC 3776 are acknowledged.

12. References

12.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[3] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[4] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[5] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[6] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

12.2. Informative References

[7] Giaretta, G., "AAA Goals for Mobile IPv6", Work in Progress, September 2006.

[8] Korver, B., "The Internet IP Security PKI Profile of IKEv1/ ISAKMP, IKEv2, and PKIX", Work in Progress, February 2007.

[9] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[10] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[11] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[12] Sugimoto, S., "PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE", Work in Progress, September 2006.

[13] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", Work in Progress, December 2006.

Authors' Addresses

Vijay Devarapalli
Azaire Networks
3121 Jay Street
Santa Clara, CA 95054
USA

EMail: vijay.devarapalli@azairenet.com

Francis Dupont
CELAR

EMail: Francis.Dupont@fdupont.fr

Full Copyright Statement

Intellectual Property

Acknowledgement

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