MIP6 WG
Internet Draft
Expires: April 21, 2006

G. Giaretta, Editor
Tilab
J. Kempf
DoCoMo Labs USA
V. Devarapalli
Nokia

October 21, 2005

Mobile IPv6 bootstrapping in split scenario
draft-ietf-mip6-bootstrapping-split-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

This Internet-Draft will expire on April 21, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

A Mobile IPv6 node requires a Home Agent address, a home address, and IPsec security associations with its Home Agent before it can start utilizing Mobile IPv6 service. RFC 3775 requires that some

or all of these are statically configured. This document defines how a Mobile IPv6 node can bootstrap this information from non-

topological information and security credentials preconfigured on the Mobile Node. The solution defined in this document solves the bootstrapping problem from draft-ietf-mip6-bootstrapping-ps-02 when the Mobile Node's mobility service is authorized by a different service provider than basic network access, and is therefore generically applicable to any bootstrapping case.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].

Table of Contents

1. Introduction

Mobile IPv6 [2] requires the Mobile Node to know its Home Agent Address, its own Home Address and the cryptographic materials (e.g. shared keys or certificates) needed to set-up IPsec security associations with the Home Agent in order to protect MIPv6 signaling. This is generally referred to as the Mobile IPv6 bootstrapping problem [4].

Mobile IPv6 base protocol does not specify any method to automatically acquire this information, which means that network administrators are normally required to manually set configuration data on MNs and HAs. However, in real deployments, manual configuration does not scale as the Mobile Nodes increase in number.

As discussed in [4], several bootstrapping scenarios can be identified depending on the relationship between the network operator that authenticates a mobile host for granting network access service (Access Service Authorizer, ASA) and the service provider that authorizes Mobile IPv6 service (Mobility Service

Authorizer, MSA). This document describes a solution to the bootstrapping problem that is applicable in a scenario where the MSA and the ASA are different entities (i.e. split scenario).

2. Terminology

General mobility terminology can be found in [8]. The following additional terms are used here:

ASA
: Access Service Authorizer. A network operator that authenticates a mobile host and establishes the mobile host's authorization to receive Internet service.

ASP
: Access Service Provider. A network operator that provides

direct IP packet forwarding to and from the end host.

MSA
: Mobility Service Authorizer. A service provider that authorizes Mobile IPv6 service.

MSP
: Mobility Service Provider. A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile host must be authenticated and prove authorization to obtain the service.

Split scenario
: A scenario where mobility service and network access service are authorized by different entities. This implies that MSA is different from ASA.

3. Split scenario

In the problem statement draft [4] there is a clear assumption

that mobility service and network access service can be separate. This assumption implies that mobility service and network access service may be authorized by different entities. As an example, the service model defined in [4] allows an enterprise network to deploy a Home Agent and offer Mobile IPv6 service to a user, even if the user is accessing the Internet independent of its enterprise account (e.g., by using his personal WiFi hotspot account at a coffee shop).

Therefore, in this document it is assumed that network access and mobility service are authorized by different entities, which means that authentication and authorization for mobility service and network access will be considered separately. This scenario is called split scenario.

Moreover, the model defined in [4] separates the entity providing the service from the entity that authenticates and authorizes the user. This is similar to the roaming model for network access. Therefore, in the split scenario, two different cases can be identified depending on the relationship between the entity that provides the mobility service (i.e. Mobility Service Provider, MSP) and the entity that authenticates and authorizes the user (i.e. Mobility Service Authorizer, MSA).

Figure 1 depicts the split scenario when the MSP and the MSA are the same entity. This means that the network operator that provides the Home Agent authenticates and authorizes the user for mobility service.

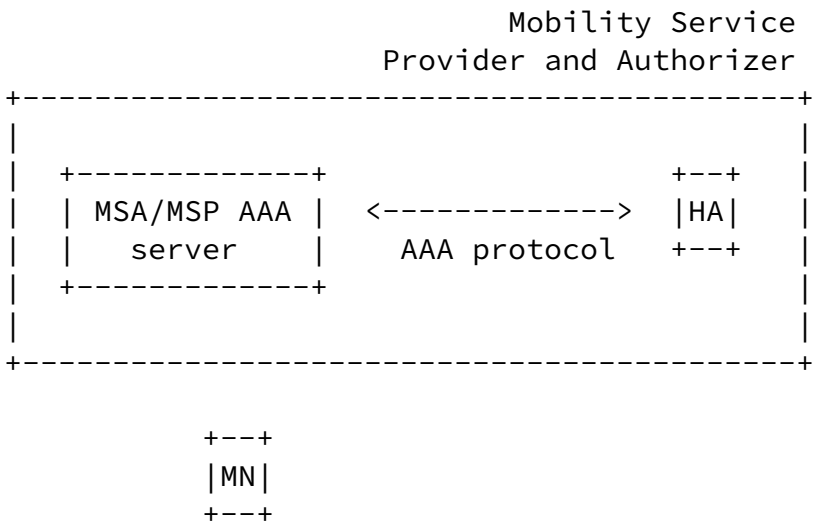


Figure 1 - Split Scenario (MSA == MSP)

Figure 2 shows the split scenario in case the MSA and the MSP are two different entities. This might happen if the Mobile Node is

far from its MSA network and is assigned a closer HA to optimize performance or if the MSA cannot provide any Home Agent and relies on a third party (i.e. the MSP) to grant mobility service to its users. Notice that the MSP might be or might not be also the network operator that is providing network access (i.e. ASP, Access Service Provider).

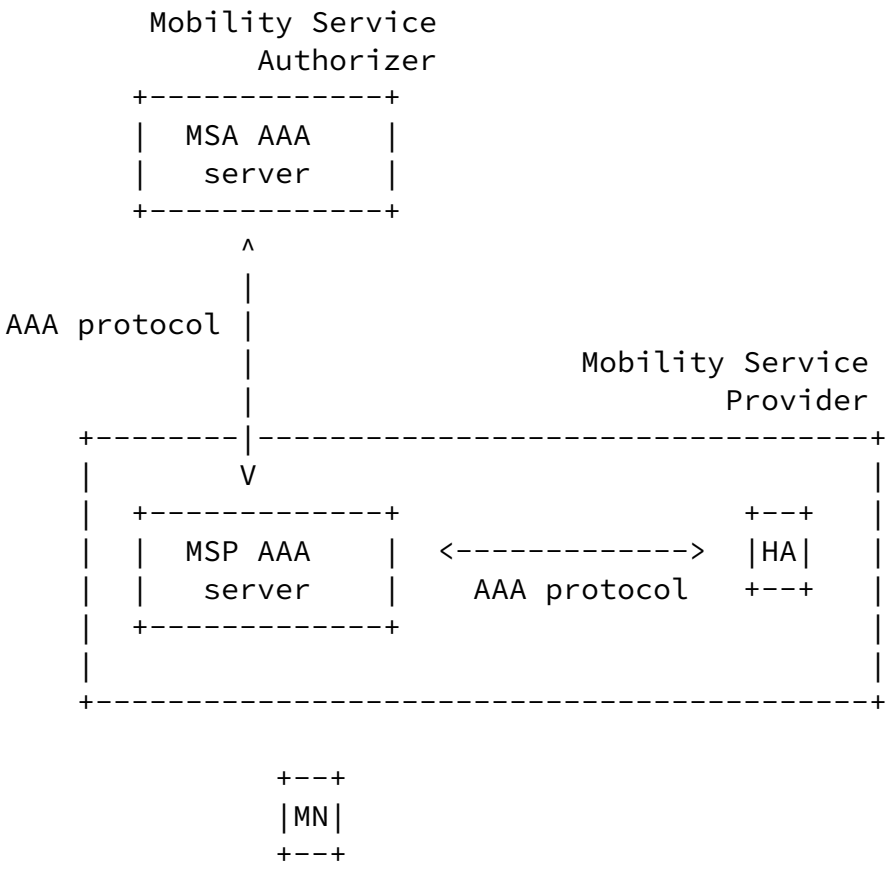


Figure 2 - Split Scenario (MSA != MSP)

Note that Figure 1 and Figure 2 assume the use of an AAA protocol to authenticate and authorize the MN for mobility service. If, instead, a PKI is used, the MN and HA exchange certificates and there is no AAA server involved. This is conceptually similar to Figure 1, since the MSP == MSA, except the HA may require a certificate revocation list check (CRL check) with the Certificate Authority (CA). The CA may be either internal or external to the MSP. Figure 3 illustrates.

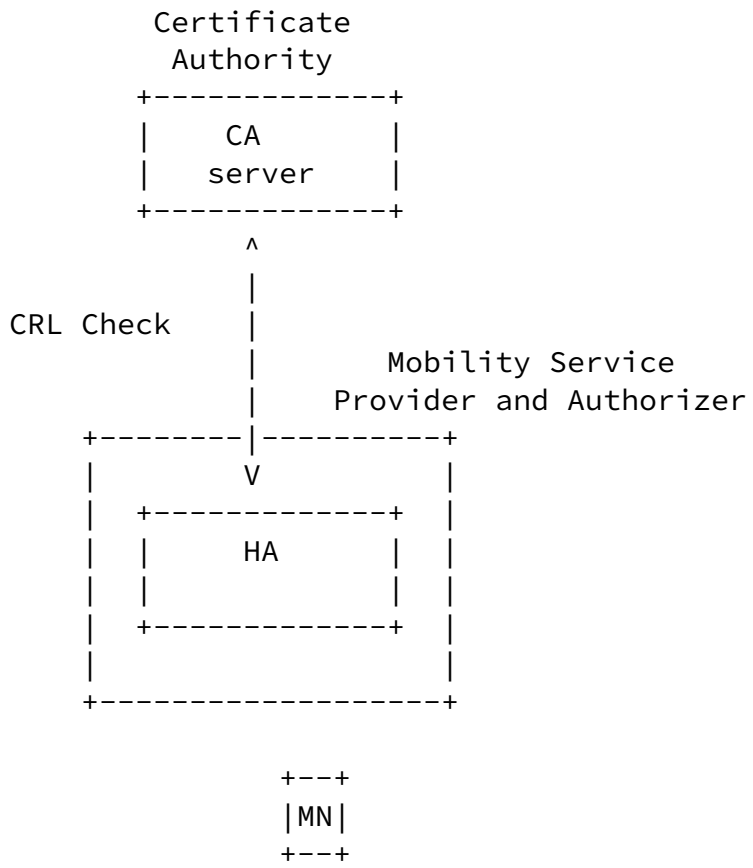


Figure 3 - Split Scenario with PKI

The split scenario is the simplest model that can be identified, since no assumptions about the access network are made. This implies that the mobility service is bootstrapped independently from the authentication protocol for network access used (e.g. PANA, EAP). For this reason, the solution described in this document and developed for this scenario could also be applied to the integrated access network deployment model [4], even if it might not be optimized.

4. Components of the solution

The bootstrapping problem is composed of different sub-problems that can be solved independently in a modular way. The components identified and a brief overview of their solution follow.

- HA address discovery. The Mobile Node needs to discover the address of its Home Agent. The main objective of a bootstrapping solution is to minimize the data pre-configured on the Mobile Node. For this reason, the DHAAD defined in [2] may not be applicable in real deployments since it is required that the Mobile Node is pre-configured with the home network prefix and it does not allow an operator to load balance by having Mobile Nodes dynamically assigned to Home Agents located in different subnets. This document defines a solution for Home Agent address discovery that is based on Domain Name Service (DNS), introducing a new DNS SRV record [5]. The unique information that needs to be pre-configured on the Mobile Node is the domain name of the MSP.

- IPsec Security Associations setup. MIPv6 requires that a Mobile Node and its Home Agent share an IPsec SA in order to protect binding updates and other MIPv6 signaling. This document provides a solution that is based on IKEv2 and follows what is specified in [6]. The IKEv2 peer authentication can be performed both using certificates and using EAP, depending on the network operator's deployment model.

- o HoA assignment. The Mobile Node needs to know its Home Address in order to bootstrap Mobile IPv6 operation. The Home Address is assigned by the Home Agent during the IKEv2 exchange (as described in [6]). The solution defined in this draft also allows the Mobile Node to auto-configure its Home Address based on stateless auto-configuration ([20]), Cryptographically Generated Addresses ([9]) or privacy addresses ([10]).

- o Authentication and Authorization with MSA. The user must be authenticated in order for the MSP to grant the service. Since the user credentials can be verified only by the MSA, this authorization step is performed by the MSA. Moreover, the mobility service must be explicitly authorized by the MSA based on the user's profile. These operations are performed in different ways depending on the credentials used by the Mobile Node during the IKEv2 peer authentication and on the backend infrastructure (PKI or AAA).

An optional part of bootstrapping involves providing a way for the Mobile Node to have its FQDN updated in the DNS with a dynamically assigned home address. While not all applications will require this service, many networking applications use the FQDN to obtain an address for a node prior to starting IP traffic with it. The

solution defined in this document specifies that the dynamic DNS update is performed by the Home Agent or through the AAA infrastructure, depending on the trust relationship in place.

5. Protocol Operations

This section describes in detail the procedures needed to perform Mobile IPv6 bootstrapping based on the components identified in the previous section.

5.1. Home Agent Address Discovery

Once a Mobile Node has obtained network access, it can perform Mobile IPv6 bootstrapping. For this purpose, the Mobile Node queries the DNS server to request information on Home Agent service. As mentioned before in the document, the only information that needs to be pre-configured on the Mobile Node is the domain name of the Mobility Service Provider.

The Mobile Node needs to obtain the IP address of the DNS server before it can send a DNS request. This can be pre-configured on the Mobile Node or obtained through DHCPv6 from the visited link [11]. In any case, it is assumed that there is some kind of mechanism by which the Mobile Node is configured with a DNS server since a DNS server is needed for many other reasons.

Two options for DNS lookup for a Home Agent address are identified in this document: DNS lookup by Home Agent Name and DNS lookup by service name.

This document does not provide a specific mechanism to load balance different Mobile Nodes among Home Agents. It is possible for an MSP to achieve coarse-grained load balancing by dynamically updating the SRV RR priorities to reflect the current load on the MSP's collection of Home Agents. Mobile Nodes then use the priority mechanism to preferentially select the least loaded HA. The effectiveness of this technique depends on how much of a load it will place on the DNS servers, particularly if dynamic DNS is used for frequent updates.

While this document specifies a Home Agent Address Discovery solution based on DNS, when the ASP and the MSP are the same entity DHCP may be used. See [15] for details.

5.1.1. DNS lookup by Home Agent Name

In this case, the Mobile Node is configured with the Fully Qualified Domain Name of the Home Agent. As an example, the Mobile Node could be configured with the name "ha1.example.com", where "example.com" is the domain name of the MSP granting the mobility service.

The Mobile Node constructs a DNS request, by setting the QNAME to

the name of the Home Agent. The request has QTYPE set to 'AAAA', so that the DNS server sends the IPv6 address of the Home Agent. Once the DNS server replies to this query, the Mobile Node knows its Home Agent address and can run IKEv2 in order to set up the IPsec SAs and get a Home Address.

Additionally, the ability to provide a mobile node with a localized home agent (e.g. on the visited link) can help to optimize handover signaling and improve routing efficiency in bi-directional tunneling mode. There are a variety of ways this can be achieved in an interoperable way. One way is to provision the mobile node with an FQDN for a local home agent when it configures for the local link. Another way is to specify an interoperable naming convention for constructing home agent FQDNs based on location. For example, an operator might assign the FQDN "ha.locationA.operator.com" to the Home Agent located in "location A" and the FQDN "ha.locationB.operator.com" to the Home Agent located in "location B". If the Mobile Node wants to use a Home Agent located in "location A", it will set the QNAME to "ha.locationA.operator.com" in the DNS request. The exact way in which localized Home Agents are configured is out of scope for this draft.

5.1.2. DNS lookup by service name

RFC 2782 [5] defines the service resource record (SRV RR), that allows an operator to use several servers for a single domain, to move services from host to host, and to designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service/protocol for a specific domain and get back the names of any available servers.

RFC 2782[5] describes also the policies to choose a service agent based on the preference and weight values. The DNS SRV record may contain the preference and weight values for multiple Home Agents available to the Mobile Node in addition to the Home Agent FQDNs. If multiple Home Agents are available in the DNS SRV record then Mobile Node is responsible for processing the information as per policy and for picking one Home Agent. If the Home Agent of choice does not respond for some reason or the IKEv2 authentication fails, the Mobile Node SHOULD try other Home Agents on the list.

The service name for Mobile IPv6 Home Agent service as required by RFC 2782 is "mip6" and the protocol name is "ipv6". Note that a transport name cannot be used here because Mobile IPv6 does not run over a transport protocol.

The SRV RR has a DNS type code of 33. As an example, the Mobile constructs a request with QNAME set to "_mip6_ipv6.example.com" and QTYPE to SRV. The reply contains the FQDNs of one or more

servers, that can then be resolved in a separate DNS transaction to the IP addresses. However, it is RECOMMENDED that the DNS server also return the IP addresses of the Home Agents in AAAA records as part of the additional data section in order to avoid requiring an additional DNS round trip to resolve the FQDNs, if there is room in the SRV reply.

5.2. IPsec Security Associations setup

As soon as the Mobile Node has discovered the Home Agent Address, it establishes an IPsec Security Association with the Home Agent itself through IKEv2. The detailed description of this procedure is provided in [6]. If the Mobile Node wants the HA to register the Home Address in the DNS, it MUST use the FQDN as the initiator identity in IKE_AUTH step of the IKEv2 exchange (IDi). This is needed because the Mobile Node has to provide it is the owner of the FQDN provided in the subsequent DNS Update Option. See section 6 and section 9 for a more detailed analysis on this issue.

The IKEv2 Mobile Node to Home Agent authentication can be performed using either IKEv2 public key signatures or the Extensible Authentication Protocol (EAP). The details about how IKEv2 authentication is done are described in [6] and [7]. Choice of an IKEv2 peer authentication method depends on the deployment. However, IKEv2 restricts the Home Agent to Mobile Node authentication to use public key signature based authentication.

5.3. Home Address assignment

Home Address assignment is performed during the IKEv2 exchange. The Home Address can be assigned directly by the Home Agent or can be auto-configured by the Mobile Node.

5.3.1. Home Address assignment by the Home Agent

When the Mobile Node runs IKEv2 with its Home Agent, it can request a HoA through the Configuration Payload in the IKE_AUTH exchange by including an INTERNAL_IP6_ADDRESS attribute. When the Home Agent processes the message, it allocates a HoA and sends it

a CFG_REPLY message. The Home Agent could consult a DHCP server on the home link for the actual home address allocation. This is explained in detail in [6].

5.3.2. Home Address auto-configuration by the Mobile Node

With the type of assignment described in the previous section, the Home Address cannot be generated based on Cryptographically

Generated Addresses (CGAs) [9] or based on the privacy extensions for stateless autoconfiguration [10]. However, the Mobile Node might want to have an auto-configured HoA based on these mechanisms. It is worthwhile to mention that the auto-configuration procedure described in this section cannot be used in some possible deployment, since the Home Agents might be provisioned with pools of allowed Home Addresses.

In the simplest case, the Mobile Node is provided with a pre-configured home prefix and home prefix length. In this case the Mobile Node creates a Home Address based on the pre-configured prefix and sends it to the Home Agent including an INTERNAL_IP6_ADDRESS attribute in a Configuration Payload of type CFG_REQUEST. If the Home Address is valid, the Home Agent replies with a CFG_REPLY, including an INTERNAL_IP6_ADDRESS with the same address. If the Home Address provided by the Mobile Node is not valid, the Home Agent assigns a different Home Address including an INTERNAL_IP6_ADDRESS attribute with a new value. According to [7] the Mobile Node MUST use the address sent by the Home Agent. Later, if the Mobile Node wants to use an auto-configured Home Address (e.g. based on CGA), it can run Mobile Prefix Discovery, obtain a prefix, auto-configure a new Home Address and then perform a new CREATE_CHILD_SA exchange.

If the Mobile Node is not provided with a pre-configured Home Prefix, the Mobile cannot simply propose an auto-configured HoA in the Configuration Payload since the Mobile Node does not know the home prefix before the start of the IKEv2 exchange. The Mobile Node must obtain the home prefix and the home prefix length before it can configure a home address.

One simple solution would be for the Mobile Node to just assume that the prefix length on the home link is 64 bits and extract the home prefix from the Home Agent's address. The disadvantage with

this solution is that the home prefix cannot be anything other than /64. Moreover, this ties the prefix on the home link and the Home Agent's address, but, in general, a Home Agent with a particular address should be able to serve a number of prefixes on the home link, not just the prefix from which its address is configured.

Another solution would be for the Mobile Node to assume that the prefix length on the home link is 64 bits and send its interface identifier to the Home Agent in the IP6_INTERNAL_ADDRESS attribute within the CFG_REQ payload. Even though this approach does not tie the prefix on the home link and the Home Agent's address, it still requires that the home prefix length is 64 bits.

For this reason the Mobile Node needs to obtain the home link prefixes through the IKEv2 exchange. In the Configuration Payload during the IKE_AUTH exchange, the Mobile Node includes the

MIP6_HOME_PREFIX attribute in the CFG_REQUEST message. The Home Agent, when it processes this message, should include in the CFG_REPLY payload prefix information for one prefix on the home link. This prefix information includes the prefix length (see section 8.2). The Mobile Node auto-configures a Home Address from the prefix returned in the CFG_REPLY message and runs a CREATE_CHILD_SA exchange to create security associations for the new Home Address.

As mentioned before in this document, there are deployments where auto-configuration of the Home Address cannot be used. In this case, when the Home Agent receives a CFG_REQUEST including a MIP6_HOME_PREFIX attribute, in the subsequent IKE response it includes a Notify Payload type "USE_ASSIGNED_HoA" and the related Home Address in a INTERNAL_IP6_ADDRESS attribute. If the Mobile Node gets a "USE_ASSIGNED_HoA" Notify Payload in response to the Configuration Payload containing the MIP6_HOME_PREFIX attribute, it looks for an INTERNAL_IP6_ADDRESS attribute and MUST use the address contained in it in the subsequent CREATE_CHILD_SA exchange.

When the Home Agent receives a Binding Update for the Mobile Node, it performs proxy DAD for the auto-configured Home Address. If DAD fails, the Home Agent rejects the Binding Update. If the Mobile Node receives a Binding Acknowledgement with status 134 (DAD

failed), it MUST stop using the current Home Address, configure a new HoA, and then run IKEv2 CREATE_CHILD_SA exchange to create security associations based on the new HoA. The Mobile Node does not need to run IKE_INIT and IKE_AUTH exchanges again. Once the necessary security associations are created, the Mobile Node sends a Binding Update for the new Home Address.

It is worth noting that with this mechanism, the prefix information carried in MIP6_HOME_PREFIX attribute includes only one prefix and does not carry all the information that is typically present when received through a IPv6 router advertisement. Mobile Prefix Discovery, specified in RFC 3775 [2], is the mechanism through which the Mobile Node can get all prefixes on the home link and all related information. That means that MIP6_HOME_PREFIX attribute is only used for Home Address auto-configuration and does not replace the usage of Mobile Prefix Discovery for the purposes detailed in RFC 3775.

5.4. Authorization and Authentication with MSA

In a scenario where the Home Agent is discovered dynamically by the Mobile Node, it is very likely that the Home Agent is not able to verify by its own the credentials provided by the Mobile Node during the IKEv2 exchange. Moreover, the mobility service needs to

be explicitly authorized based on the user's profile. As an example, the Home Agent might not be aware if the mobility service can be granted at a particular time of the day or if the credit of the Mobile Node is going to expire.

Due to all these reasons, the Home Agent may need to contact the MSA in order to authenticate the Mobile Node and authorize mobility service. This can be accomplished based on a Public Key Infrastructure if certificates are used and a PKI is deployed by the MSP and MSA. On the other hand, if the Mobile Node is provided with other types of credentials, the AAA infrastructure must be used.

The definition of this backend communication is out of the scope of this document. In [12] a list of goals for such a communication is provided.

6. Home Address registration in the DNS

In order that the Mobile Node is reachable through its dynamically assigned Home Address, the DNS needs to be updated with the new Home Address. Since applications make use of DNS lookups on FQDN to find a node, the DNS update is essential for providing IP reachability to the Mobile Node, which is the main purpose of the

Mobile IPv6 protocol. The need of DNS update is not discussed in RFC 3775 since it assumes that the Mobile Node is provisioned with a static home address. However, when a dynamic Home Address is assigned to the Mobile Node, any existing DNS entry becomes invalid and the Mobile Node becomes unreachable unless a DNS update is performed.

Since the DNS update must be performed securely in order to prevent attacks or modifications from malicious nodes, the node performing this update must share a security association with the DNS server. Having all possible Mobile Nodes sharing a security association with the DNS servers of the MSP might be cumbersome from an administrative perspective. Moreover, even if a Mobile Node has a security association with a DNS server of its MSP, an address authorization issue comes into the picture. A detailed analysis of possible threats against DNS update is provided in section 9.5.

Therefore, due to security and administrative reasons, it is RECOMMENDED that the Home Agent perform DNS entry update for the Mobile Node. For this purpose the Mobile Node MAY include a new mobility option, the DNS Update option, with the flag R not set in the Binding Update. This option is defined in section 8 and includes the FQDN that needs to be updated. After receiving the Binding Update, the Home Agent MUST update the DNS entry with the identifier provided by the Mobile Node and the Home Address included in the Home Address Option. The procedure for sending a dynamic DNS update message is specified in [14]. The dynamic DNS update SHOULD be performed in a secure way; for this reason, the usage of TKEY and TSEC or DNSSEC is recommended (see section 9.5. for details). As soon as the Home Agent has updated the DNS, it MUST send a Binding Acknowledgement message to the Mobile Node including the DNS Update mobility option with the correct value in the Status field (see section 8.1).

This procedure can be performed directly by the Home Agent if the Home Agent has a security association with the domain specified in the Mobile Node's FQDN.

On the other hand, if the Mobile Node wants to be reachable through a FQDN that belongs to the MSA, the Home Agent and the DNS server that must be updated belong to different administrative domain. In this case the Home Agent may not share a security association with the DNS server and the DNS entry update can be

performed by the AAA server of the MSA. In order to accomplish this, the Home Agent sends to the AAA server the FQDN-HoA pair through the AAA protocol. This message is proxied by the AAA infrastructure of the MSP and is received by the AAA server of the MSA. The AAA server of the MSA perform the DNS update based on [14]. The detailed description of the communication between Home Agent and AAA is out of the scope of this draft. More details are provided in [12].

A mechanism to remove stale DNS entries is needed. A DNS entry becomes stale when the related Home Address is no more used by the Mobile Node. To remove a DNS entry, the MN includes the DNS Update mobility option, with the flag R set in the Binding Update. After receiving the Binding Update, the Home Agent MUST remove the DNS entry identified by the FQDN provided by the Mobile Node and the Home Address included in the Home Address Option. The procedure for sending a dynamic DNS update message is specified in [14]. As mentioned above, the dynamic DNS update SHOULD be performed in a secure way; for this reason, the usage of TKEY and TSEC or DNSSEC is recommended (see section 9.5. for details).

This approach does not work if the Mobile Node stops using the Home Address without sending a Binding Update message (e.g. in case of crash). In this case, an additional mechanism to trigger the DNS entry removal is needed. For this purpose, the Home Agent has a timer related to the DNS entry of the Mobile Node. This timer is initialized when the Mobile Node sends a Binding Update with R==0 (i.e. when the MN asks the Home Agent to bind the FQDN to the Home Address). The initial value of this timer is configurable by the network operator.

If the Home Agent receives a Binding Update with R==1, it removes the DNS entry as described in the previous paragraph and removes the timer associated to that entry. If the timer expires without receiving a Binding Update with R==1, the HA checks the Binding Cache. If there is an existing Binding Cache entry for the HoA, the HA does not remove the DNS entry and re-initialize the timer. If there is not a Binding Cache entry, it sends a Neighbor Solicitation message to check if the MN is at home and is using the HoA. If the HA gets a Neighbor Advertisement message, it does not remove the DNS entry and re-initialize the timer. If it does not receive a NA, it removes the DNS entry and the timer associated to it.

7. Summary of Bootstrapping Protocol Flow

The message flow of the whole bootstrapping procedure when the dynamic DNS update is performed by the Home Agent is depicted in Figure 3.

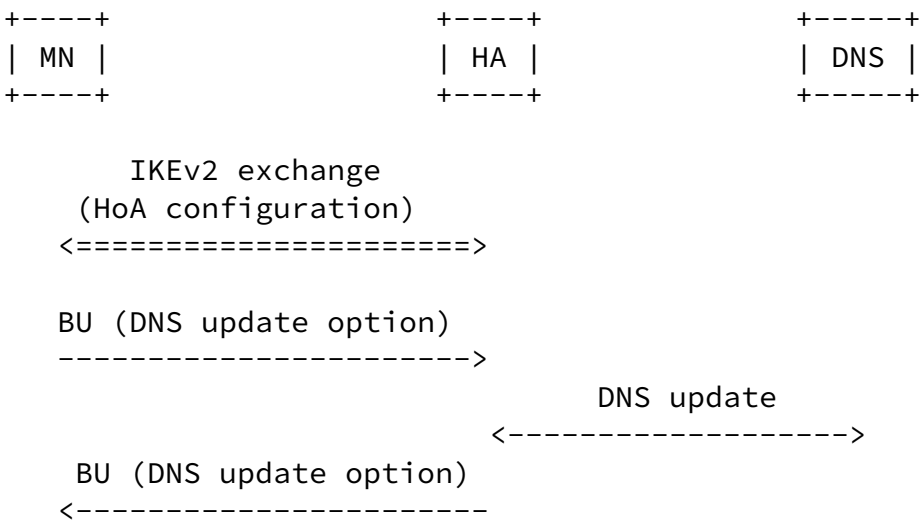


Figure 3 - Dynamic DNS update by the HA

Figure 4 shows the message flow of the whole bootstrapping procedure when the dynamic DNS update is performed by the AAA server of the MSA.

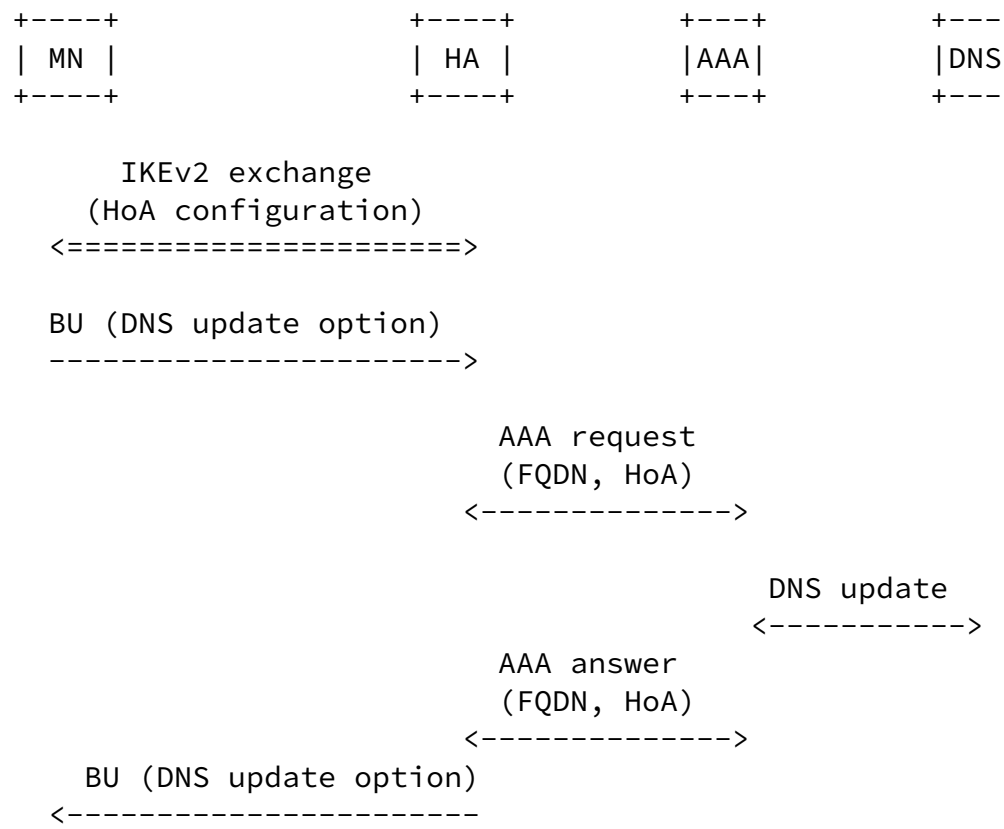
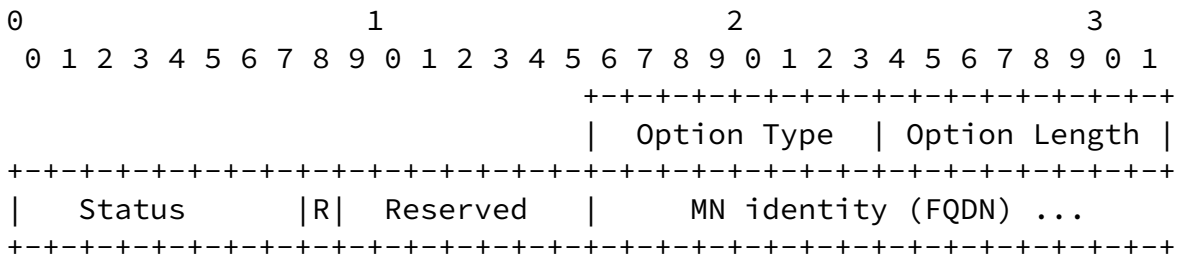


Figure 4 - Dynamic DNS update by the AAA

Notice that, even in this last case, the Home Agent is always required to perform a DNS update for the reverse entry, since this is always performed in the DNS server of the MSP. This is not depicted in Figure 4.

8. Option and Attribute Format

8.1. DNS Update mobility option



- Option Type - DNS-UPDATE-TYPE to be defined by IANA
- Option Length - 8 bit unsigned integer indicating the length of the option excluding the type and length fields
- Status - 8 bit unsigned integer indicating the result of the dynamic DNS update procedure. This field MUST be set to 0 and ignored by the receiver when the DNS Update mobility option is included in a Binding Update message. When the DNS Update

mobility option is included in the Binding Acknowledgement message, values of the Status field less than 128 indicate that the dynamic DNS update was performed successfully by the Home Agent. Values greater than or equal to 128 indicate that the dynamic DNS update was not completed by the HA. The following Status values are currently defined:

0 DNS update performed

128 Reason unspecified

129 Administratively prohibited

130 DNS Update Failed

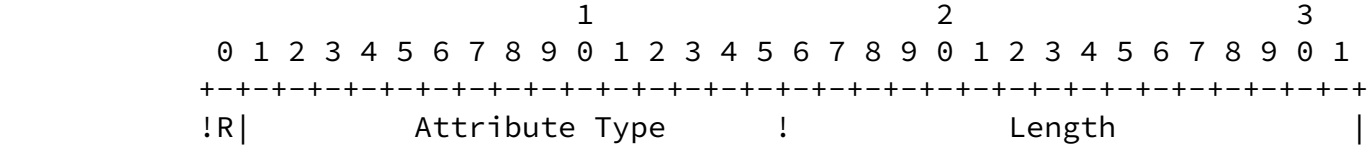
- R flag - if set the MN is requesting the HA to remove the DNS entry identified by the FQDN specified in this option and the HoA of the MN. If not set, the MN is requesting the HA to create or update a DNS entry with its HoA and the FQDN specified in the option.

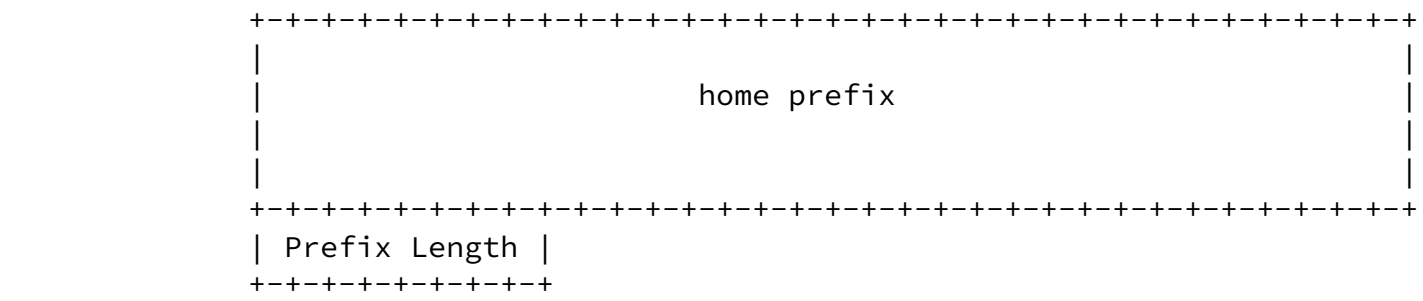
- Reserved - these bits are reserved for future purposes and MUST be set to 0.

- MN identity - the identity of the Mobile Node to be used by the Home Agent to send a Dynamic DNS update. It is a variable length field.

8.2. MIP6_HOME_PREFIX attribute

The MIP6_HOME_PREFIX attribute is included in the IKEv2 CFG_REQUEST by the Mobile Node to ask the Home Agent for the home prefix and is included in the CFG_REPLY by the Home Agent to provide the Mobile Node with home prefix and home prefix length. The format of this attribute is equal to the format of the Configuration Attributes defined in [7] and is depicted below.





- Reserved (1 bit) - This bit MUST be set to zero and MUST be ignored on receipt.
- Attribute Type (7 bits) - A unique identifier for the MIP6_HOME_PREFIX attribute. To be assigned by IANA.
- Length (2 octets) - Length in octets of Value field (home prefix and Prefix Length). This is multi-valued and can be 0 or 17.
- Home Prefix (16 octets) - The prefix of the home link through which the Mobile Node must auto-configure its Home Address.
- Prefix Length (1 octet) - The length of the home prefix specified in the field Home Prefix.

When the MIP6_HOME_PREFIX attribute is included by the Mobile Node in the CFG_REQUEST payload, the value of the Length field is 0. On the other hand, when the MIP6_HOME_PREFIX attribute is included in the CFG_REPLY payload by the Home Agent, the value of the Length field is 17 and the attribute contains also the Home Prefix and the Prefix Length fields.

9. Security Considerations

9.1. HA Address Discovery

Use of DNS for address discovery carries certain security risks. DNS transactions in the Internet are typically done without any authentication of the DNS server by the client or of the client by the server. There are two risks involved:

1) A legitimate client obtains a bogus Home Agent address from a bogus DNS server. This is sometimes called a "pharming" attack,

2) An attacking client obtains a legitimate Home Agent address from a legitimate server.

The risk in Case 1 is mitigated because the Mobile Node is required to conduct an IKE transaction with the Home Agent prior to performing a Binding Update to establish Mobile IPv6 service. According to the IKEv2 specification [7], the responder must present the initiator with a valid certificate containing the responder's public key, and the responder to initiator IKE_AUTH message must be protected with an authenticator calculated using the public key in the certificate. Thus, an attacker would have to set up both a bogus DNS server and a bogus Home Agent, and provision the Home Agent with a certificate that a victim Mobile Node could verify. If the Mobile Node can detect that the certificate is not trustworthy, the attack will be foiled when the Mobile Node attempts to set up the IKE SA.

The risk in Case 2 is limited for a single Mobile Node to Home Agent transaction if the attacker does not possess proper credentials to authenticate with the Home Agent. The IKE SA establishment will fail when the attacking Mobile Node attempts to authenticate itself with the Home Agent. Regardless of whether the Home Agent utilizes EAP or host-side certificates to authenticate the Mobile Node, the authentication will fail unless the Mobile Node has valid credentials.

Another risk exists in Case 2 because the attacker may be attempting to propagate a DoS attack on the Home Agent. In that case, the attacker obtains the Home Agent address from the DNS, then propagates the address to a network of attacking hosts that bombard the Home Agent with traffic. This attack is not unique to the bootstrapping solution, however, it is actually a risk that any Mobile IPv6 Home Agent installation faces. In fact, the risk is faced by any service in the Internet that distributes a unicast globally routable address to clients. Since Mobile IPv6 requires that the Mobile Node communicate through a globally routable unicast address of a Home Agent, it is possible that the Home Agent address could be propagated to an attacker by various means (theft of the Mobile Node, malware installed on the Mobile Node,

evil intent of the Mobile Node owner him/herself, etc.) even if the home address is manually configured on the Mobile Node. Consequently, every Mobile IPv6 Home Agent installation will likely be required to mount anti-DoS measures. Such measures include overprovisioning of links to and from Home Agents and of Home Agent processing capacity, vigilant monitoring of traffic on the Home Agent networks to detect when traffic volume increases abnormally indicating a possible DoS attack, and hot spares that can quickly be switched on in the event an attack is mounted on an operating collection of Home Agents. DoS attacks of moderate intensity should be foiled during the IKEv2 transaction. IKEv2 implementations are expected to generate their cookies without any saved state, and to time out cookie generation parameters frequently, with the timeout value increasing if a DoS attack is suspected. This should prevent state depletion attacks, and should assure continued service to legitimate clients until the practical limits on the network bandwith and processing capacity of the Home Agent network are reached.

Explicit security measures between the DNS server and host, such DNSSEC [16] or TSIG/TKEY [17] [18] can mitigate the risk of 1) and 2), but these security measures are not widely deployed on end nodes. These security measures are not sufficient to protect the Home Agent address against DoS attack, however, because a node having a legitimate security association with the DNS server could nevertheless intentionally or inadvertently cause the Home Agent address to become the target of DoS.

Finally notice that assignment of an home agent from the serving network access provider's (local home agent) or a home agent from a nearby network (nearby home agent) may set up the potential to compromise a MN's location privacy. However, since a standardized mechanism of assigning local or nearby home agents is out of scope for this document, it is not possible to present detailed security considerations. Please see other drafts that contain detailed mechanisms for localized home agent assignment, such as [15], for information on the location privacy properties of particular home agent assignment mechanisms.

Security considerations for discovering HA using DHCP are covered in draft-jang-dhc-haopt-01 [15].

9.2. Home Address Assignment through IKEv2

Mobile IPv6 bootstrapping assigns the home address through the IKEv2 transaction. The Mobile Node can either choose to request an address, similar to DHCP, or the Mobile Node can request a prefix

on the home link then autoconfigure an address.

RFC 3775 [2] and 3776 [3] require that a Home Agent check authorization on a home address received during a Binding Update.

The Home Agent MUST set up authorization by linking the home address to the identity of the IPsec SAs used to authenticate the Binding Update message. The linking MUST be done either during the IKE_AUTH phase or CREATE_CHILD_SA phase when the IPsec SAs are constructed.

If the address is autoconfigured, RFC 3775 requires the Home Agent to proxy-defend the address on the home link after the Mobile Node performs the initial Binding Update. Since it is not currently possible to securely proxy CGAs using SEND, attacks on address resolution for Neighbor Discovery listed in RFC 3756 are possible on dynamically assigned home addresses that are proxied by the Home Agent.

9.3. SA Establishment Using EAP Through IKEv2

Security considerations for authentication of the IKE transaction using EAP are covered in draft-ietf-mip6-ikev2-ipsec [6].

9.4. Back End Security Between the HA and AAA Server

Some deployments of Mobile IPv6 bootstrapping may use an AAA server to handle authorization for mobility service. This process has its own security requirements, but the back end protocol for Home Agent to AAA server interface is not covered in this draft. Please see draft-ietf-mip6-aaa-ha-goals [12] for a discussion of this interface.

9.5. Dynamic DNS Update

Mobile IPv6 bootstrapping recommends the Home Agent to update the Mobile Node's FQDN with a dynamically assigned home address rather than have the Mobile Node itself do it (see Section 6 above). This choice was motivated by a concern for preventing redirection-based flooding attacks (see draft-ietf-mip6-ro-sec [19] for more information about redirection-based flooding attacks and the role preventing them played in the design of Mobile IPv6 route optimization security). Exactly as for route optimization, it is

possible for a node that is the legitimate owner of a DNS FQDN - in the sense that it has a security association with the DNS server allowing it to perform dynamic DNS update of its FQDN - to bind its FQDN to the address of a victim, then redirect large volumes of traffic at the victim. The attack may be propagated without the owner's knowledge, for example, if the node is compromised by malware, or it may be intentional if the node itself is the attacker.

While it is possible to prevent redirection attacks through ingress filtering on access routers, ISPs have little or no incentive to deploy ingress filtering. In some cases, if an attack could result in substantial financial gain, it is even possible

that a corrupt ISP may have an incentive not to deploy ingress filters such as has been the case for spam. Consequently, the security for dynamic Mobile Node FQDN update has been assigned to the Home Agent, where active network administration and vigilant defense measures are more likely to (but are not assured of) mitigating problems, and the owner of the Mobile Node is more likely to detect a problem if it occurs.

If a Home Agent performs dynamic DNS update on behalf of the Mobile Node directly with the DNS server, the Home Agent MUST have a security association of some type with the DNS server. The security association MAY be established either using DNSSEC [16] or TSIG/TKEY [17][18]. A security association is required even if the DNS server is in the same administrative domain as the Home Agent. The security association SHOULD be separate from the security associations used for other purposes, such as AAA.

In the case where the Mobility Service Provider is different from the Mobility Service Authorizer, the network administrators may want to limit the number of cross-administrative domain security associations. If the Mobile Node's FQDN is in the Mobility Service Authorizer's domain, since a security association for AAA signaling involved in mobility service authorization is required in any case, the Home Agent can send the Mobile Node's FQDN to the AAA server under the HA-AAA server security association, and the AAA server can perform the update. In that case, a security association is required between the AAA server and DNS server for the dynamic DNS update. See draft-ietf-mip6-aaa-ha-goals [12] for a deeper discussion of the Home Agent to AAA server interface.

Regardless of whether the AAA server or Home Agent performs DNS update, the authorization of the Mobile Node to update a FQDN MUST be checked prior to the performance of the update. It is an implementation issue as to how authorization is determined. However, in order to allow this authorization step, the Mobile Node MUST use a FQDN as the IDi in IKE_AUTH step of the IKEv2 exchange. The FQDN MUST be the same that will be provided by the MN in the DNS Update Option. This allows the Home Agent to get authorization information about the Mobile Node's FQDN via the AAA back end communication performed during IKEv2 exchange. The outcome of this step will give the Home Agent the necessary information to authorize the DNS update request of the Mobile Node. See draft-ietf-mip6-aaa-ha-goals [12] for details about the communication between the AAA server and the Home Agent needed to perform the authorization. Notice that if certificates are used in IKEv2, the authorization information about the FQDN for DNS update MUST be present in the certificate provided by the Mobile Node.

10. IANA Considerations

This document defines a new Mobility Option and a new IKEv2 Configuration Attribute Type.

The following values should be assigned:

- from "Mobility Option" namespace ([2]): DNS-UPDATE-TYPE (section 8.1)
- from "IKEv2 Configuration Payload Attribute Types" namespace ([7]): MIP6_HOME_PREFIX attribute (section 8.2)
- from "IKEv2 Notify Payload Error Types" namespace ([7]): USE_ASSIGNED_HoA error type (section 5.3.2)

11. Contributors

This contribution is a joint effort of the bootstrapping solution design team of the MIP6 WG. The contributors include Basavaraj Patil, Alpesh Patel, Jari Arkko, James Kempf, Yoshihiro Ohba, Gopal Dommety, Alper Yegin, Junghoon Jee, Vijay Devarapalli, Kuntal Chowdury, Julien Bournelle.

The design team members can be reached at:

Gerardo Giaretta gerardo.giaretta@tilab.com

Basavaraj Patil	basavaraj.patil@nokia.com
Alpesh Patel	alpesh@cisco.com
Jari Arkko	jari.arkko@kolumbus.fi
James Kempf	kempf@docomolabs-usa.com
Yoshihiro Ohba	yohba@tari.toshiba.com
Gopal Dommety	gdommety@cisco.com
Alper Yegin	alper.yegin@samsung.com
Vijay Devarapalli	vijayd@iprg.nokia.com
Kuntal Chowdury	kchowdury@starentnetworks.com
Junghoon Jee	jhjee@etri.re.kr
Julien Bournelle	julien.bournelle@int-evry.fr

12. Acknowledgments

The authors would like to thank Rafa Lopez, Francis Dupont, Basavaraj Patil, Jari Arkko, Kilian Weniger for their valuable comments.

13. References

13.1. 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., Dupont, F., "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", RFC 3776, June 2004

[4] Patel, A., "Problem Statement for bootstrapping Mobile IPv6", Internet-Draft draft-ietf-mip6-bootstrap-ps-03, July 2005.

[5] Gulbrandsen, A., Vixie, P. and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[6] Devarapalli, V., " Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", Internet-Draft draft-ietf-mip6-ikev2-ipsec-03, September 2005.

[7] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", Internet-Draft draft-ietf-ipsec-ikev2-17, October 2004

13.2. Informative References

[8] Manner, J., Kojo, M. "Mobility Related Terminology", RFC 3753, June 2004.

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

[10] Narten, T., Draves, R., Krishnan, S., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", Internet-Draft draft-ietf-ipv6-privacy-addrs-v2-04, May 2005.

[11] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646,

December 2003.

[12] Giaretta, G., Ed. "Goals for AAA-HA interface", Internet-Draft draft-ietf-mip6-aaa-ha-goals-00, April 2005.

[13] Koodli, R., Devarapalli, V., Perkins, C., Flinck, H., "Solutions for IP Address Location Privacy in the presence of IP Mobility", Internet-Draft, draft-koodli-mip6-location-privacy-solutions-00, February 2005.

[14] P. Vixie, Ed., S. Thomson, Y. Rekhter, and J. Bound. "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[15] Chowdhury, K., Yegin, A., Choi, J., "MIP6-bootstrapping via DHCPv6 for the Integrated Scenario", Internet-Draft, draft-ietf-mip6-bootstrapping-integrated-dhc-00, October 2005.

[16] Arends, R., Austein, R., Larson, M., Massey, D., Rose, S., "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[17] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., Wellington, B., "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[18] Eastlake 3rd, D., " Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[19] Nikander, P., Arkko, J., Aura, T., Montenegro, G., Nordmark, E., "Mobile IP version 6 Route Optimization Security Design Background", Internet-Draft, draft-ietf-mip6-ro-sec-02, October 2004.

[20] Narten, T., Nordmark, E., Simpson, W., Soliman, H., "Neighbor Discovery for IP version 6 (IPv6)"`, Internet-Draft, draft-ietf-ipv6-2461bis-03, May 2005.

Authors' Addresses

Gerardo Giaretta
Telecom Italia Lab
via Reiss Romoli 274
10148 Torino
Italy

Phone: +39 011 228 6904
Email: gerardo.giaretta@tilab.com

James Kempf
DoCoMo Labs USA
181 Metro Drive
Suite 300
San Jose, CA, 95110
USA

Phone: +1 408 451 4711
Email: kempf@docomolabs-usa.com

Vijay Devarapalli
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043
USA

Email: vijay.devarapalli@nokia.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository

at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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