AAA WG
INTERNET-DRAFT
Date: November 2004
Expires: May 2005

Franck Le
Basavaraj Patil
Charles E. Perkins
Stefano Faccin
Nokia

Diameter Mobile IPv6 Application
<draft-le-aaa-diameter-mobileipv6-04.txt>

Status of This Memo

Abstract

Mobile IPv6 capable mobile nodes can roam between networks that belong to their home service provider as well as others. Roaming in foreign networks is enabled as a result of the service level and roaming agreements that exist between operators. One of the key protocols that allows this kind of a roaming mechanism to be enabled is Diameter. This Internet Draft specifies a new application to Diameter that enables Mobile IPv6 roaming in networks other than its home.

Table of Contents

1. Introduction

Mobile IP defines a method that allows a Mobile Node to change its point of attachment to the Internet with minimal service disruption. Mobile IP in itself does not provide any specific support for mobility across different administrative domains, which limits the applicability of Mobile IP in a large scale commercial deployment.

AAA protocols such as Diameter precisely enable mobile users to roam and obtain service in networks that may not necessarily be owned by their home service provider. For Mobile IP to be deployed in commercial networks, there therefore has to be AAA support for the protocol.

Diameter extensions for Mobile IPv4 [1] have already been specified allowing a MIPv4 node to receive services from service providers (home and foreign) and allowing the Diameter servers to authenticate, authorize and collect accounting information for those MIPv4 nodes.

Even though MIPv4 and MIPv6 are similar when observed at high level, the two protocols are actually quite different when considering the support for Inter Domain deployment. Mobile IPv6 e.g. does not have the equivalent of a Foreign Agent as defined in Mobile IPv4, and as a result does not define any mechanism by which the visited network can authenticate and authorize access to the network and use of resources. In addition, extending the Diameter Mobile IPv4 Application [1] to support Mobile IPv6 will reduce the flexibility and result in some AAA capability exchange issues: it will be difficult to differentiate which AAA nodes support only Mobile IPv4, which ones support only Mobile IPv6 and which ones support both. This document therefore provides a solution for Mobile IPv6 and AAA interworking and e.g. defines the IPv6 specific solution to support roaming of an IPv6 mobile node between different administrative domains.

In order to give access to a mobile node to network resources, the mobile node needs to be authenticated and authorized. Besides supporting mobile node authentication and authorization, the AAA infrastructure can also be used for distributing the security keys needed to support the mobile node roaming. Optionally, the AAA infrastructure can be used to support mobility procedures and to optimize authentication, authorization and mobility in a common procedure.

This internet draft defines the Diameter Mobile IPv6 application. It identifies the information that needs to be exchanged between the MN and the AAA Client but it does not specify any particular mechanism to convey information between the mobile node and the AAA Client: the

set of information identified in the following internet draft, can be conveyed between the mobile node and the AAA client in a different suitable manner outside the scope of this document (e.g. ICMP, the protocol defined by the PANA WG, etc.). The extensions defined for Diameter allow for any of these alternatives, thus enabling such extensions to be deployed independently of the choice of the protocol used between the MN and the AAA client in the visited or access network.

The basic AAA model for inter domain roaming and the assumptions behind the model are described first. The basic features supported by the Diameter Mobile IPv6 application are described next, with the definition of the Diameter messages and AVPs and with the behavior of the various elements. Finally, enhanced features are described and the AVPs and the behavior of the various elements is described.

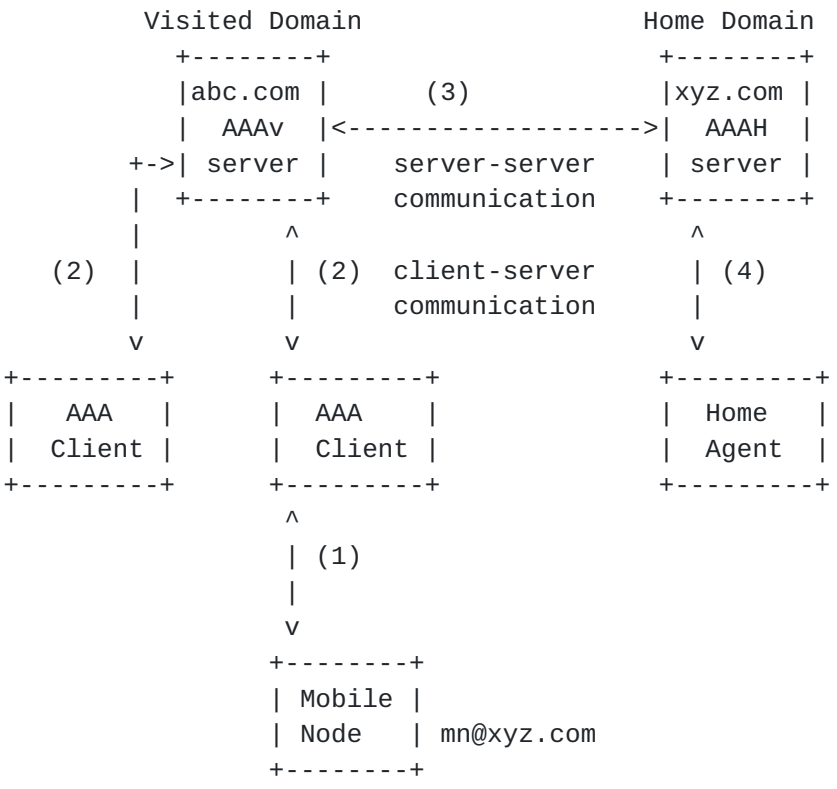
2. Advertising Application support

Diameter nodes conforming to this specification MAY advertise support by including the value of (TBD) in the Auth-Application-Id or the Acct-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command [7].

3. The model and assumptions

3.1. The model

The following entities are involved in the model:



* The Mobile Node

* The AAA Client: it is the function that allows the MN to register and be authenticated by the network service provider, by providing identity and authentication information to the local network which then uses a AAA infrastructure to validate the user, generate accounting data for network usage and, authorize use of resources. In addition to authorization and authentication, the MN may provide the AAA Client with mobility management information (e.g. embedded Binding Updates) to perform Mobile IP procedures. The AAA Client can be an attendant, e.g. located in an Access Router, or can be an AA Agent (Auth/Authorization agent) as the one identified in UNAP.

* AAAv: is the AAA server in the visited network

* AAAh: is the AAA server in the home network of the MN

* HA: is a Home Agent

3.2. Assumptions

1) Mobile nodes are identified by their Network Access Identifier (NAI) in an unique manner:

RFC2794 specifies an identifier for mobile nodes, the MN-NAI. The MN-NAI is used by the AAA infrastructure to authenticate mobile IPv4 nodes.

The Mobile IPv6 specification mandates the existence of a security association between the MN and its Home Agent (HA). In certain scenarios and future deployments a MN may not have any Home Agent or a home address assigned to it. A MN may instead have a security association with the home AAA network element and may use this to obtain a home address, and an HA.

In this document it is assumed that an IPv6 mobile node SHOULD identified by a MN-NAI in a unique manner, and that an IPv6 mobile node SHOULD be able to use its NAI instead of its home address to get authenticated/authorized by the AAA infrastructure when roaming to foreign domains. In fact, in general the network needs to authenticate the user that is roaming, not the specific device, and in the future there may be cases where a specific user is accessing the network through several devices, or several users are accessing the network through the same device.

In general, anyway, it is better to allow identification of an IPv6 mobile node also through the use of its IPv6 home address: this allows users that have not been provided with a NAI by their home domain to get authenticated and authorized by the AAA infrastructure.

The assumption made in this document is that:

* When the identifier associated with a mobile is the MN-NAI, it SHOULD use the MN_NAI to get authenticated/authorized by the AAA infrastructure, independently of whether the MN has or not a home address

* when the MN does not have a MN-NAI but only a home address, the MN MAY use the IPv6 home address to get authenticated/authorized by the AAA infrastructure

2) Mobile Node and AAAh share a long-term key:

This long-term key provides network authentication and user authentication; it can also be used in order to derive session keys

or local security associations as explained in the following sections.

3) Communications between AAAv and AAAh are secure

This inter AAA security association allows the home and visited domain to trust each other, and to exchange information in an authenticated and protected manner.

4. Basic features supported in this Internet Draft

4.1. Authentication/authorization

Before giving access to the network, the visited network wants to authenticate the user. The IPv6 mobile node may also want to authenticate the network to prevent network impersonation such as false BTS attacks.

The IPv6 mobile nodes SHOULD have the capability to use many different authentication methods: The IPv6 mobile nodes could e.g. use EAP at layer 3 for authentication: This document does not define how the authentication information are exchanged between the Mobile nodes and the network (it could be performed using the protocol defined by the PANA WG, ICMPv6 messages) but the AAA infrastructure allows that authentication and authorization; and the defined Diameter messages support many round trips if the authentication method adopted requires it.

4.2. Dynamic Home Agent assignment in Home domain

It is possible that when the mobile node needs to send a Binding Update to its home agent to register its new primary care-of address, the mobile node may not know the address of any router on its home link that can serve as a home agent for it. For example, some nodes on its home link may have been reconfigured while the mobile node has been away from home, such that the router that was operating as the mobile node's home agent has been replaced by a different router serving this role.

The dynamic Home agent assignment feature also provides more flexibility to the service provider: in general, a mobile node home network may not assign statically a home agent to the mobile node to maintain flexibility in the allocation of the home agent to achieve better load sharing and fault tolerance.

In this case, the mobile node MAY use the dynamic home agent address discovery mechanism to find the address of a suitable home agent on its home link.

The current Mobile IPv6 specification describes a dynamic Home Agent discovery procedure; as an alternative, this document describes another home agent assignment procedure relying on the present AAA infrastructure.

Whereas the current dynamic home agent address discovery mechanism requires many round trips between the mobile node and its home domain thus resulting in additional signaling over the access link and between the home and visited domains; and also adding more delay in the procedure, the solution relying on the AAA infrastructure only requires one round trip.

And instead of sending specific IP address to request for a Home address/Home agent in the Home/Visited domain, the proposed solution is based on flags: less data thus needs to be sent over the access link, and the AAAh (AAAv) instead creates the binding update message when assigning the home agent.

4.3. Key distribution

Many security associations need to be dynamically established such as:

* the security association between the mobile node and the visited network to protect data (e.g. confidentiality and integrity protection) over the access link

* the security association between the mobile node and the home agent, to authenticate the binding update/acknowledgement messages. According to the current specifications, after the dynamic home agent address discovery is performed, the mobile node sends a Binding Update to the selected Home agent to create the to create a forwarding entry in the route table for the home address associated with the MN. This Binding Update MUST be authenticated, therefore a key distribution, e.g. IKE, may need to be executed. This requires many messages to be exchanged between the mobile node and the Home Agent.

As an alternative, after the authentication and authorization steps, the AAA servers can be involved and play a role in the key generation and/or the key distribution.

Diameter Mobile IPv4 Application defines one key distribution mechanism; for Mobile IPv6, many different schemes could be applied thus providing more flexibility and different properties as outlined in the following sections.

4.4. Optimization of Binding Updates

As previously explained, in addition to authentication, authorization and key distribution functionalities, the AAA servers can perform mobility procedures such as dynamic home agent assignment. In case, the IPv6 mobile node already has a pre-configured Home Agent, some optimization can also be achieved by having the mobile node encapsulating the binding update to its Home agent in the AAA request message.

4.5. Summary

MN authentication is in general required to grant access to a MN to the foreign domain. In fact, this may be needed in most of the cases even if access to the foreign domain resources is free. Due to the fact that the MN is away from its home network and hence considered roaming the MN needs to perform also mobility procedures to obtain reachability in the new location. Optionally, key distribution may be need to take place. Using the AAA infrastructure to achieve these functions can significantly reduce inter domain signaling and time delay of the overall procedure performed by a MN to get access to the foreign domain.

Currently the mobile node first gets authenticated using the AAA infrastructure to obtain network access, then it may perform dynamic home agent address discovery [4] and set up a security association (using e.g. Internet Key Exchange [5]) with the selected Home agent before sending a Binding Update. This will require many round trips between the foreign domain and the home domain, whereas the use of the AAA infrastructure provides a more efficient and quicker alternative.

5. Mobile IPv6 Application Diameter messages

This memo introduces some new Command codes (AA-Registration-Request, AA-Registration-Answer, Home-Agent-MIPv6-Request, Home-Agent-MIPv6-Answer) and AVPs (MIP-Binding-Update AVP, MIP-Binding-acknowledgement AVP, MIPv6-Mobile-Node-Address AVP, MIPv6-Home-Agent-Address AVP, MIPv6-Feature-Vector AVP, Key-Request AVP, MN-Key-

Distribution AVP, Key-Distribution AVP) to achieve all the previously identified functionalities.

5.1. Command Codes

This document introduces four new Command Codes:

* AA-Registration-Request Command (ARR) (Code TBD)
* AA-Registration-Answer Command(ARA) (Code TBD)
* Home-Agent-MIPv6-Request Command (HOR) (Code TBD)
* Home-Agent-MIPv6-Answer Command (HOA) (Code TBD)

5.2. AVPs

5.2.1. MIP-Binding-Update AVP

The MIP-Binding-Update AVP (AVP Code TBD) is of type OctetString and contains the Mobile IP Binding Update message.

5.2.2. MIP-Binding-acknowledgement AVP

The MIP-Binding-acknowledgement AVP (AVP Code TBD) is of type OctetString and contains the Mobile IP Binding Acknowledgement message sent by the Home Agent to the MN.

5.2.3. MIPv6-Mobile-Node-Address AVP

The Mobile-Node-Address AVP (AVP Code TBD) is of type IPAddress and contains the Mobile Node's Home Address.

5.2.4. MIPv6-Home-Agent-Address AVP

The Home-Agent-Address AVP (AVP Code TBD) is of type IPAddress and contains the Mobile Node's Home Agent Address.

5.2.5. MIPv6-Feature-Vector AVP

The MIPv6-Feature-Vector AVP (AVP Code TBD) is of type Unsigned32 and allows for dynamic Home Agent assignment in Home Domain. In the basic proposal, only one flag is defined; the other ones are reserved for the enhanced version and for future utilization.

Flag values currently defined include:

1 Home-Agent-Requested: This flag is set to 1 when the mobile node requests for a dynamic home agent assignment. When this flag is set to 1, a dynamic session key to be shared between the MN and the HA is also required in order to authenticate BUs from the MN to the HA: the MN may indicate through some Security Key Request the methods it supports to compute it; or a default method known to the MN and the AAAh should exist(e.g. pre-set by the home domain and communicated to the MN at subscription time).

5.2.6. Security Key AVPs

The AAA servers can play a role in key distribution and many methods can be used with their own properties and characteristics. The security keys AVPs format and utilization will be described in more details in the next versions as well as the AAA servers' behaviors.

6. Information exchange between the mobile node and the AAA Client

Although this document is not intended to specify any particular mechanism to convey information between the mobile node and the AAA Client, the information that needs to be exchanged is described. The set of information identified in the follow can actually be conveyed between the mobile node and the network in a different suitable manner outside the scope of this document (e.g. ICMP, the protocol defined by the PANA WG, etc.). The extensions defined for Diameter allow for any of these alternatives, thus enabling such extensions to be deployed independently of the choice of the protocol used between the MN and the network.

6.1. MIP Feature Data

Contrary to Mobile IPv4 where the Mobile nodes send a Registration Request with specific IP addresses values to request for dynamic home

agent assignment in home/visited networks; the IPv6 mobiles nodes SHOULD use some MIP Feature data whose content includes the information required in the previously defined MIPv6 Feature Vector AVP: The IPv6 mobile nodes will not use specific IPv6 addresses values but use flags and this will significantly reduces the amount of data to be sent over the access link. In addition, the attendant will only need to encapsulate that data in the corresponding MIPv6-Feature-Vector AVP.

The MIP Feature data could be sent as an extension to ICMPv6 messages, a new Destination Option or carried in any other way.

6.2. EAP Data

The IPv6 Mobile Node should be able to use different authentication methods such as the different EAP types.

The EAP Data could be sent as an extension to ICMPv6 messages, carried using the protocol defined by the PANA WG or any other protocol.

6.3. Security Key Data

This document does not defines the protocol between the mobile nodes and the network but the mobile node SHOULD use some key request to indicate the keys it needs, but also the methods it supports to generate them.

Those Security Key data SHOULD contain the relevant information so the AAA client can create the corresponding Security Keys AVPs.

6.4. Embedded Data

The embedded data enables the mobile node to send a binding update at the same time the mobile node gets authorized/authenticated by the network (e.g. by mechanism that the protocol defined by the PANA WG will provide) thus saving round trips between the home and the visited domains.

7. Basic Protocol Overview

7.1. Authentication

Authentication is required before providing network access to the user.

Different authentication should be supported to allow more flexibility; but as demonstrated in [6], both network and user authentication should be supported.

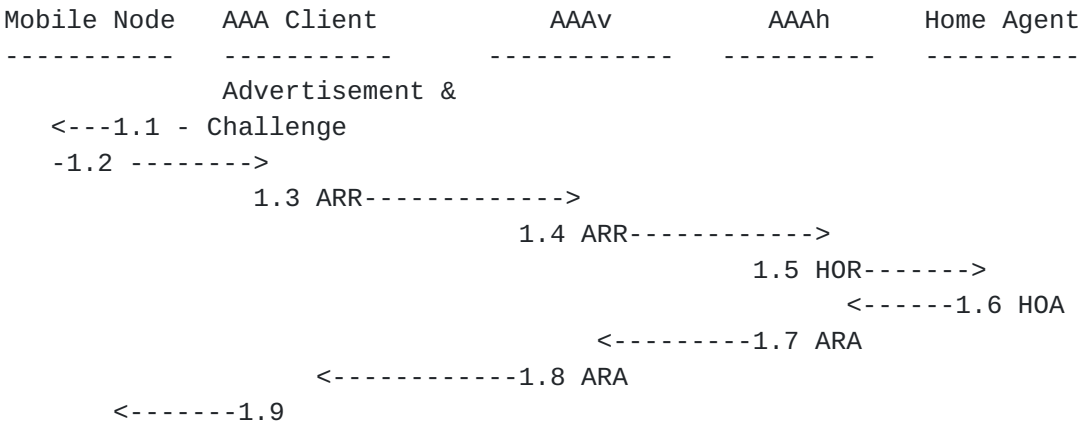
And current authentication mechanisms, even those recently specified in different standardization fora (e.g. CAVE based security functions in IS41 Systems) have security flaws.

For these reasons, even as previously mentioned any existing authentication could be used, in the following illustrations and procedures, a mutual challenge response based authentication method will be suggested and used as default.

The authentication mechanism assumed here assumes that a Local Challenge is broadcast over the access link e.g. in Router Advertisement messages.

7.2. Information flows

Basic Procedure with dynamic Home Agent assignment in the Home network or pre-configured Home Agent



7.3. MN Considerations

7.3.1. Generation of information in MN

1) When entering a new network or at power up, the MN listens to the router advertisements and retrieves:

The Local Challenge
The visited network identifier
The information to derive the CoA

2) It computes the CoA, and based on the following information,

* The NAI
* The long-term security key shared with its AAAh
* The Home Address: in the basic mode, the mobile node is assumed to have a pre-configured Home IP address
* The Home Agent (if any), otherwise MN can request to have one assigned

creates a message with the CoA as the Source IP address and the AAA Client address as the Destination IP address. (The MN can learn the IP address of the AAA Client through router advertisements or others mechanisms outside the scope of this document.) As previously explained, the mobile node also sends its NAI.

3) The MN optionally generates a Host Challenge that it will send to the network for both network authentication and anti replay attacks. Then the MN computes the MN authentication data using the long-term key, the host challenge, the visited network identifier, the local challenge, and an authentication algorithm it shares with its home network. The MN authentication data is then sent to the AAA Client,

4) If the MN does not have a Home Agent and requests one, the MN includes some MIP Feature data with the Home-Agent-Requested flag set to 1. The home agent will then be assigned by the home AAA server, and the binding update will be sent by the AAA server to the Home Agent on behalf of the mobile node that, in turn, does not need to send any.

If the MN have a pre configured Home Agent, it may creates the binding update message and sends it encapsulated to the AAA client. The Binding Update message will be forwarded to the designated home agent via the AAA infrastructure. This binding update message has the MN IP CoA as the source IP address, the pre-configured HA as the destination IP address and the BU option with the pre-configured Home IP address in the Home address option.

5) The MN may also requests for some security keys thanks to the Security Key Request.

The MN SHOULD perform authentication in the following cases:

* When changing visited domain: MN can know that by listening the router advertisements
* When requesting session keys
* When requesting a Home Agent assignment

7.3.2. Replies to MN

When receiving the reply from the AAA Client, the MN:

* Authenticates the network thanks to the network authentication data sent by the AAA Client

* If the MN requested a Home agent, it will learn and store the Home Agent address from the source IP address of the Home Binding Acknowledgement.

The MN creates the security associations from the keying material received.

7.4. AAA Client Operation

As indicated above, the mobile node may interact with the AAA Client to perform authentication/authorization and optionally Mobile IP procedures. Thus, the AAA client may perform authentication functions and optionally Mobile IP functions

When the AAA Client receives an authentication request message from a IPv6 Mobile node:

The AAA Client first verifies the freshness of the request thanks to the Local Challenge contained in it (i.e. the MN may use an older Local Challenge) and if successful, performs Duplicate Address Detection and creates a Diameter ARR (AA-Registration-Request) [7] message carrying the following information to the AAAh:

* User Name AVP [7] carrying the user's NAI

* EAP AVP to carry the authentication data for mutual authentication derived from the content of the received authentication data

* if some MIP feature data were received from the MN, a MIPv6-Feature-Vector AVP whose content is derived from the MIP feature data, sent within the ARR message it sends to the AAAv

* MIP-Binding Update AVP if the MN sent a Home Binding Update as Embedded data

* MIPv6-Home-Agent-Address AVP if the MN sent a binding update message: the Home agent address value is extracted from the Destination IP address field of the embedded home binding update. This AVP enables the AAAh to know where to send the MIP-Home-binding-Update AVP if one was present.

* if the MN provides some Key Request data, some Security Key AVPs whose content is derived from the Key Request data.

When receiving an ARA [7] (AA-Registration-Answer) message from AAAv, the AAA Client converts the message to the appropriate protocol to the MN; this message carries:

* the authentication data

* Binding Acknowledgement as Embedded Data if MN sent a home Binding Update or requested for a dynamic home agent assignement.

The message may also include:

* Keying material to set up the different session keys, converted and conveyed in the appropriate protocol by the AAA Client from the Security Key AVPs. When the MN asks for a dynamic Home Agent, AAAh SHOULD compute the security key to be shared between MN and the HA for authenticating subsequent Binding Updates, and sends the corresponding keying material to the MN.

7.5. AAAv Operation

When AAAv receives an ARR message [7]:

First the AAAv verifies the message is coming from a valid AAA Client and then, checks the MIPv6 Feature Vector AVP, and then sends it to the MN's home AAA server.

When receiving a ARA message from the AAAh, the AAAv MAY optionally, according to the behaviour specific for speficic EAPs or other mechanisms defined elsewhere, store locally information contained in the AVPs of the message received from the AAAh (e.g. session keys, etc.) and then forwards the message to the AAA Client.

7.6. AAAh operations

* When receiving an ARR message from an AAAv, the AAAh first verifies the message is coming from a valid AAAv. Security associations between AAA server are outside the scope of the present document.

The AAAh then authenticates the user using the NAI provided by the MN as MN identity. If the mobile Node is successfully authenticated:

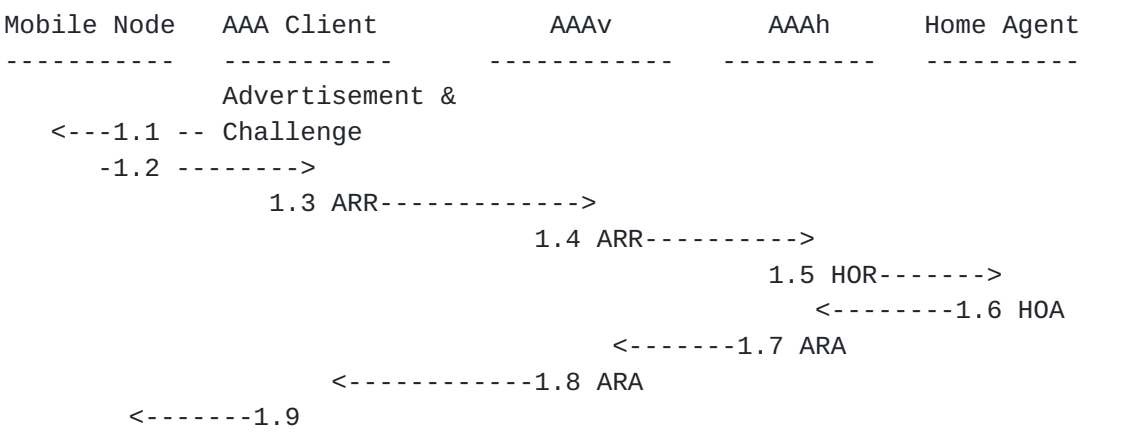
* AAAh also computes some network authentication data based on the Host Challenge and eventually other information depending on the authentication algorithm adopted.

Depending on the authentication method requirements, the AAAh may exchange many messages with the MN via the AAAv (e.g. for a user authentication mechanism that requires more than one round-trip): AAAh may send a ARA Command with the appropriate authentication information and indication, which will be converted to EAP data by the AAA Client to the MN and conveyed to the MN in a suitable manner (outside the scope of this document). The number of round trips varies depending on the authentication mechanism used.

* If the MN asks for some security keys, the AAAh performs the appropriate steps and eventually sends the corresponding messages to achieve the key distribution: many mechanisms exist and some of them will be described later on. Such steps may require the AAAh to distribute keys and keying material to the MN, to other AAA servers or other nodes.

* If a MIPv6-Home-Agent-Address AVP is present: the AAAh checks that the address is that of a known and valid Home Agent, and one that the Mobile Node is allowed to request. AAAh then forwards the MIP-Home-Binding-Update AVP to the Home Agent in a HOR (Home-Agent-MIP-Request) message.

* If no MIPv6-Home-Agent-Address AVP is present, AAAh looks at the MIPv6-Feature-Vector AVP if any. If present, AAAh performs the dynamic home agent assignment in the Home network:



(1.5) AAAh allocates a Home agent on behalf of the MN: this can be done in a variety of ways, including using a load balancing algorithm in order to keep the load on all HAs equal.

* AAAh sends a HOR message to the HA including a newly created binding update.

* AAAh sends some security keying material to allow the Home Agent to comupte the key(s) for the security association between the MN and the Home Agent to authenticate future Binding Updates.

(1.6) the Home Agent creates the Binding Cache and computes the key(s) for the security association with the MN from the data received. It also generates a Binding Acknowledgement message to be sent encapsulated to the MN.

* The HA sends a HOA message to the AAAh including the Binding Ack.

(1.7) AAAh may also compute other keying material according to the keys requested by the MN and send it to the MN passing through the AAAv.

* AAAh then send an ARA message to the AAAv including the MIP-Binding-acknowledgement AVP if the MN sent an embedded BU or request for a HA.

7.7. Home Agent Behavior

Upon receipt of the HOR, the Home Agent first processes the DIAMETER message: if the HOR is invalid, a HOA is returned with the Result-Code AVP set to DIAMETER_ERROR_BAD_HOR. Otherwise, the Home Agent processes the MIP-Binding-update AVP and creates the Binding

Acknowledgement, encapsulating it within the MIP-binding-acknowledgement AVP.

HA also creates the Binding Cache and computes the key(s) for the security association with the MN from the data received.

8. Enhanced features

In addition to the previously described features, additional features can be supported by the AAA infrastructure for the inter-domain roaming of an IPv6 mobile node, thus providing more flexibility and allowing new options to the services providers to develop business models.

A IPv6 mobile node can have a pre-configured home address, may have a pre-configured home agent or request for one and, as explained in the previous section, the basic features of the Mobile IPv6 Diameter Application allow an optimization of the authentication, the binding update, the optional home agent assignment in the home domain and the key distribution procedures.

Optionally, two enhanced features are suggested:

* The dynamic Home agent assignment in the Visited Domain
* The dynamic Home address assignment

8.1. Dynamic Home Agent/ Home Address assignment in Visited domain

The Dynamic Home Agent assignment in visited networks allows more flexibility and allows new business scenarios. As an example, service providers may just own a AAA server for accounting purposes and, thanks to roaming agreements, they may offer Mobile IP services to its subscribers. Another scenario where this can be applied is when IPv6 mobile nodes need to obtain reachability from other CN only at the application level, i.e. through a SIP infrastructure. This may be the case of a basic IPv6 MN supporting only voice services through SIP. In such cases, when a CN needs to reach the MN an identifier at the application level (e.g. MN SIP URL) is used, and the CN does not need to know the home address of the MN. Somebody may argue that Mobile IP is not needed at all in such cases, but it may instead be used to support mobility between the initial point of attachment (i.e. when the MN powered up in the foreign domain) and following points of attachment in the foreign domain.

8.2. Dynamic Home address assignment in Home Domain

The mobile node may not always have a pre-configured IPv6 address and may need to have one dynamically assigned. In addition since the Home Agent and the mobile node home address need to be on the same link, to support dynamic home agent assignment in visited networks, dynamic home address assignment in visited networks is supported.

Finally, this dynamic Home address feature provides more flexibility to the service provider even when the Home agent is to be assigned in the Home network since the Home agent and the home address should be on the same subnet. Additionally, the scenario described in section 7.2 of a MN node needing reachability only at the application layer applies to this case too.

8.3. Enhanced AVPs

In addition to the Command Codes and AVPs described in section 4, some new AVP need to be defined to support the enhanced features.

8.3.1. MIPv6-Feature-Vector AVP

In the extended mode, dynamic home agent assignment in the visited network is feasible.Additional flags of the MIPv6-Feature-Vector AVP are therefore defined.

The following flags allow the Visited AAA server, AAAv, to inform of its capabilities and if the Home agent is assigned in the visited network, the Home address must also be assigned in the visited network.

The AAA Client includes a MIPv6-Feature-Vector AVP within the ARR message it sends to the AAAv if the MN sent some MIP Feature data.

Flag values currently defined include:

1 Home-Agent-Requested: This flag is set to 1 when the mobile node requests for a dynamic home agent assignment. When this flag is set to 1, a dynamic session key to be shared between the MN and the HA is also required in order to authenticate BUs from the MN to the HA: the MN may indicate through some Security Key Request the methods it supports to compute it; or a default method known to the MN and the AAAh should exist(e.g. pre-set by the home domain and communicated

to the MN at subscription time).

2 Mobile-Node-Home-Address-Requested flag: This flag is set to 1 if the mobile node does not have any Home address and requires one. Default value is 0.

4 Home-Address-Allocatable-Only-in-Home-Domain flag: This flags is set to 1 if the mobile node requests for one Home address and wants it to be assigned by its home network. Default value is 0 and means that the MN does not have any preference on whether the Home Address shall be allocated in the home domain and visited domain.

8 Home-Agent-in-Visited-Domain flag: The mobile node indicates its preference to have its Home Agent allocated in the visited domain by having this flag set to 1

16 Visited-Home-Agent-Available flag: The Visited Domain sets this flag to 1 if the MN asks a dynamic Home Agent assignment in the Visited Domain and the Visited Domain agrees to allocate one to the MN.

9. Enhanced Protocol Overview

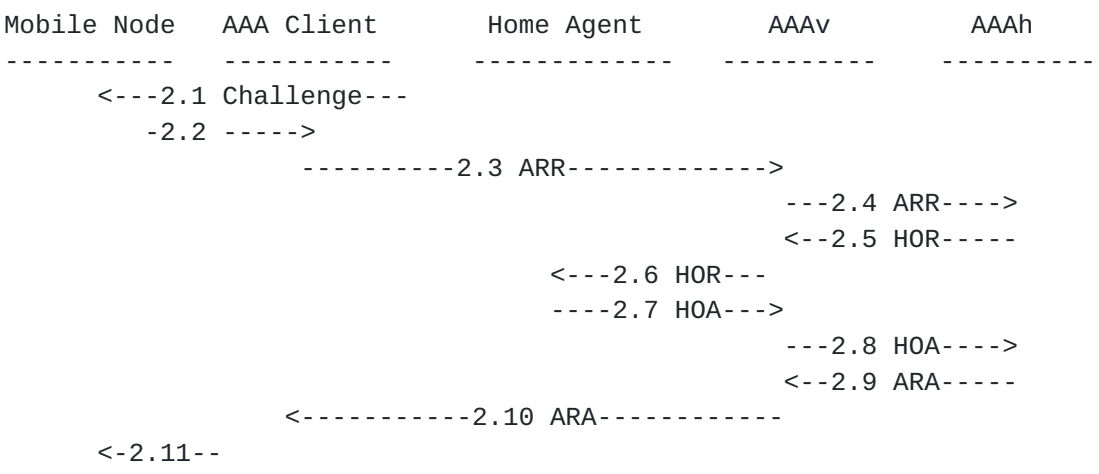
The enhanced mode allows dynamic home agent assignment in the visited network and dynamic home address assignment. The mobile node may not have any preconfigured home address nor any home agent. The following text describes the different entities' behaviors in the Enhanced mode.

The authentication procedure is the same than the one described above.

All the functionalities (key distribution, optimization of Binding Upate, dynamic Home Agent assignment in Home network) of the basic mode are present but in addition the Home agent can be assigned in the visited network and the home address can be dynamically assigned either in the home or visited domain: the entities behaviours and the way the corresponding AVPs are processed, are explained

9.1. Information flow

Enhanced Procedure with dynamic Home agent assignment in the visited network and dynamic home address assignment in home or visited domain



9.2. MN Considerations

9.2.1. Generation of information in MN

The mobile node performs the same steps as in the basic mode (steps (1), (2), (3) section 6.3.1) and then

4) If the MN does not have a Home Address and requests one, the MN also includes some MIP Feature data with the Mobile-Node-Home-Address-Requested flag set to 1:

* If MN wants its Home address to be allocated by its home network, it also sets the value of Home-Address-Allocatable-Only-in-Home-Domain flag to 1.

If the MN does not have a Home Agent and requests one, the MN also includes some MIP Feature data with the Home-Agent-Requested flag set to 1. The home agent will then be assigned by the AAA server, and the binding update will be sent by the AAA server to the Home Agent on behalf of the mobile node that, in turn, does not need to send any.

* If MN wants its Home agent to be allocated by the visited network, it also sets the Home-Agent-in-Visited-Network flag to 1.

The following table describes the different supported cases and the flags that need to be set according to the needs:

HD means Home Domain
VD means Visited Domain
NP means MN has No Preference
X means not supported

P: Mobile-Node-Home-Address-Requested flag
H: Home-Address-Allocatable-Only-in-Home-Domain
A: Home-Agent-Requested
V: Home-Agent-In-Visited-Network

		Home agent Requested				
		YES			NO	
		HD	VD	NP		
Home addr Requested	HD	PAH	x	x	PH	
	YES	VD	x	PAV	x	x
	NP	x	x	PA	P	
	NO	A*	x	x	no MIP Feature data	

A*: MN already has a home address in its Home network and may request for a Home Agent. The HA can thus only be assigned in the Home Network.

While the MN gets authenticated and authorized, if the MN already has a home address and a home agent, it can send a Home Binding Update together with the request to be authorized and authenticated to save one round trip over the access link and between the visited and home networks. This binding update is in this case sent as Embedded Data:

The Home Binding Update has:

* The H flag set to 1.
* The source IP address equals to the CoA
* The destination IP address set to the Home agent address
* The Home Address option set to the MN Home address

5) The MN may also requests for some security keys thanks to the Security Key Request.

The MN SHOULD perform authentication in the following cases:

* When changing visited domain: MN can know that by listening the router advertisements
* When requesting session keys
* When requesting a Home Agent assignment
* When requesting a home address assignment

9.2.2. Replies to MN

When receiving the reply from the AAA Client, the MN:

* Authenticates the network thanks to the network authentication data sent by the AAA Client

* If the MN requested a Home agent, it will learn and store the Home Agent address from the source IP address of the Home Binding Acknowledgement.

* If the MN did not have a Home IP address and requested for one, the MN will learn and store the assigned home address from the home address option of the Home Binding Acknowledgement (embedded data).

The MN creates the security associations from the keying material received.

9.3. AAA Client Operation

As indicated above, the mobile node may interact with the AAA Client to perform authentication/authorization and optionally Mobile IP procedures. Thus, the AAA client may perform authentication functions and optionally Mobile IP functions

When the AAA Client receives an authentication request message from a IPv6 Mobile node:

The AAA Client first verifies the freshness of the request thanks to the Local Challenge contained in it (i.e. the MN may use an older Local Challenge) and if successful, performs Duplicate Address Detection and creates a Diameter ARR (AA-Registration-Request) [7] message carrying the following information to the AAAh:

* User Name AVP [7] carrying the user's NAI

* EAP AVP to carry the authentication data for mutual authentication derived from the content of the received authentication data

* if some MIP feature data were received from the MN, a MIPv6-Feature-Vector AVP whose content is derived from the MIP feature data, sent within the ARR message it sends to the AAAv

* MIP-Binding Update AVP if the MN sent a Home Binding Update as Embedded data

* MIPv6-Home-Agent-Address AVP if the MN sent a Home binding update: the Home agent address value is extracted from the Destination IP address field of the embedded home binding update. This AVP enables the AAAh to know where to send the MIP-Home-binding-Update AVP if one was present.

* if the MN provides a Key Request, some Security Key AVPs whose content is derived from the Key Request.

When receiving an ARA [7] (AA-Registration-Answer) message from AAAv, the AAA Client converts the message to appropriate protocol to the MN; this message carries:

* the authentication data

* Binding Acknowledgement as Embedded Data if MN sent a home Binding Update or requested for a dynamic home agent assignment.

The message may also include:

* Keying material to set up the different session keys, in different Security Key Data created by the AAA Client from the Security Key AVPs. When the MN asks for a dynamic Home Agent, AAAh must compute the security key to be shared between MN and the HA for authenticating subsequent Binding Updates, and sends the corresponding keying material to the MN.

9.4. AAAv Operation

When AAAv receives an ARR message [7]:

First the AAAv verifies the message is coming from a valid AAA Client and then, checks the MIPv6 Feature Vector AVP:

* If the MN requested a Home Agent by setting the Home-Agent-Requested flag to 1, and does not specify that this one should be assigned only in its Home domain by setting the Home-Address-Allocatable-Only-in-Home-Domain flag to 1, the AAAv checks if it can allocate a Home Agent for the mobile node in the visited domain. If AAAv can allocate a Home Agent in the visited domain, it indicates this to the AAAh by setting the Visited-Home-Agent-Available flag to 1 of the MIPv6 Feature Vector AVP forwarded to the AAAh.

When receiving a HOR message from the AAAh for a dynamic Home Agent assignment in the visited network, the AAAv performs the dynamic Home agent assignment and MAY perform some key distribution depending on the mechanisms.

When receiving a ARA message from the AAAh, the AAAv MAY optionally, according to the behavior specific for speficic EAPs or other mechanisms defined elsewhere, store locally information contained in the AVPs of the message received from the AAAh (e.g. session keys, etc.) and then forwards the message to the AAA Client.

9.5. AAAh operations

* When receiving an ARR message from an AAAv, the AAAh first verifies the message is coming from a valid AAAv. Security associations between AAA server are outside the scope of the present document.

The AAAh then authenticates the user using the NAI provided by the MN as MN identity. If the mobile Node is successfully authenticated:

* AAAh also computes some network authentication data based on the Host Challenge and eventually other information depending on the authentication algorithm adopted.

Depending on the authentication method requirements, the AAAh may exchange many messages with the MN via the AAAv (e.g. for a user authentication mechanism that requires more than one round-trip): AAAh may send a ARA Command with the appropriate authentication information and indication, which will be converted to EAP data by the AAA Client to the MN or conveyed to the MN in other suitable manner (outside the scope of this document). The number of round trips varies depending on the authentication mechanism used.

* If the MN asks for some security keys, the AAAh performs the appropriate steps and eventually sends the corresponding messages

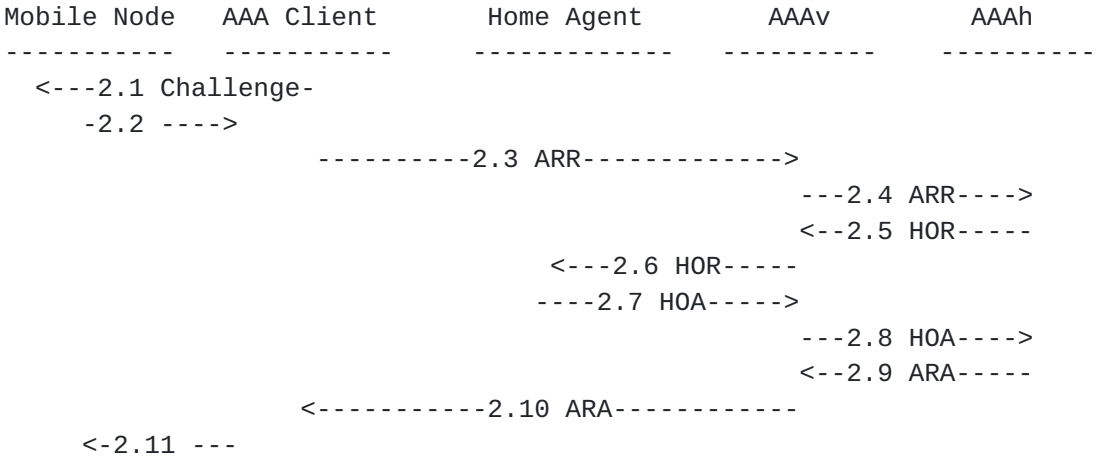
to achieve the key distribution: many mechanisms exist and will be described later on. Such steps may require the AAAh to distribute keys and keying material to the MN, to other AAA servers or other nodes.

* If a MIPv6-Home-Agent-Address AVP is present: the AAAh checks that the address is that of a known and valid Home Agent, and one that the Mobile Node is allowed to request. AAAh then forwards the MIP-Home-Binding-Update AVP to the Home Agent in a HOR (Home-Agent-MIP-Request) message including the appropriate key material to set up the security association between the MN and the Home Agent.

* If no MIPv6-Home-Agent-Address AVP is present, AAAh looks at the MIPv6-Feature-Vector AVP if any. Depending on the mobile node request (Home-Agent-in-Visited-Network flag, Home-Address-Allocatable-Only-in-Home-Domain), the visited network capabilities (Visited-Agent-Available AVP) and the local policy, the AAAh decides whether to assign the HA in the home or visited network:

9.5.1. Home Agent Assignement in Visited Network

If the AAAh accepts the HA to be assigned in the visited domain, the following exchange of messages takes place:



(2.5): AAAh sends a HOR message to the AAAv with neither any MIPv6-Mobile-Node-Address AVP nor any MIPv6-Home-Agent-Address AVP.

* AAAh may send some keying material for HA to derive the key(s) for the security association between the MN and the Home Agent to authenticate future Binding Updates depending on the key distribution mechanism chosen

* AAAh may also send other keying material according to the keys requested by the MN

(2.6): AAAv assigns a Home agent and then creates and sends it a newly created Binding Update encapsulated in the HOR message.

* AAAv may assign Home IP address for the MN and informs the Home Agent by adding a MIPv6-Mobile-Node-Address AVP in the HOR message; or let the Home Agent assigns the Home address by not providing a MIPv6-Mobile-Node-Address AVP in the HOR message.

* AAAv may forward to the Home Agent some keying material depending on the key distribution mechanism adopted to set up the security association between the MN and the Home Agent

(2.7): The Home agent assigns a Home IP address if requested and creates a Binding Cache for the MN.

* The Home agent creates the Security Association according to the mechanism adopted

* The Home Agent creates the Binding Acknowledgement to be sent encapsulated to the MN.

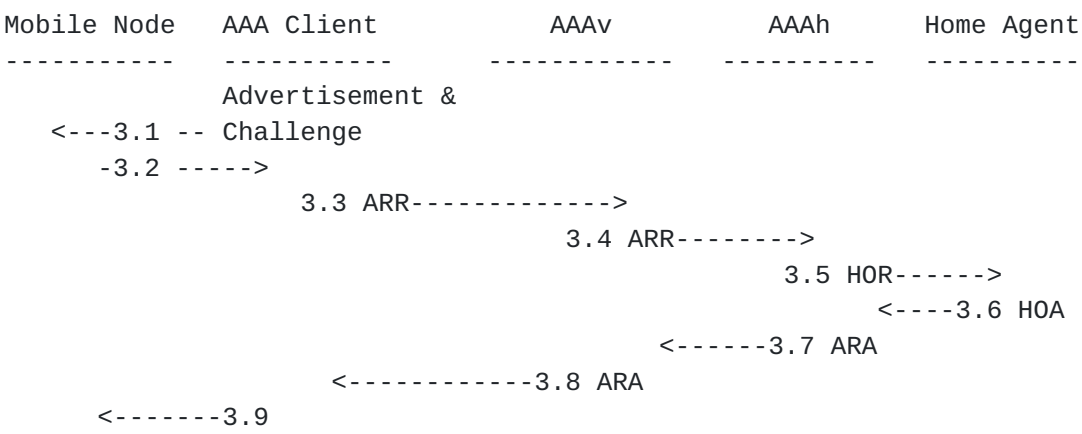
* The Home Agent sends back a HOA to the AAAv to inform it of the status: it includes the assigned Mobile Node Home Address if the Home Agent assigned one; it also includes the Binding ack created by the Home Agent to be sent encapsulated to the MN.

(2.8) The AAAh is informed of the assigned Home IP address (contained in the MIPv6-Mobile-Node-Address AVP) and the Home Agent address (contained in the MIPv6-Home-Agent-Address AVP) by the HOA message sent from the AAAv.

(2.9) The AAAh sends the AAAv an ARA carrying the Home IP address, the Home Agent IP address, the keying material with the previous information.

9.5.2. Home Agent Assignment in Home Network

If the AAAh decides to assign the HA in the Home network, the following exchange of messages takes place:



(3.5) AAAh allocates a Home agent on behalf of the MN: this can be done in a variety of ways, including using a load balancing algorithm in order to keep the load on all HAs equal.

* AAAh sends a HOR message to the HA including a newly created binding update and:

* The AAAh may allocate a home address for the mobile node and include it in a MIPv6-Mobile-Node-Address AVP within the HOR or else leave this allocation responsibility for the HA by leaving the Home address option of the binding update to zero and not sending any MIPv6-Mobile-Node-Address AVP.

* AAAh sends some security keying material to allow the Home Agent to compute the key(s) for the security association between the MN and the Home Agent to authenticate future Binding Updates.

(3.6) If the Home Agent does not receive any MIP-Mobile-node-address, and receives a BU with a Home address equals to 0, it assigns a Home IP address for that user; then creates the Binding Cache and computes the key(s) for the security association with the MN from the data received. It also generates a Binding Acknowledgement message to be sent encapsulated to the MN.

* The HA sends a HOA message to the AAAh including the Binding Ack and eventually the assigned Home IP address if one was requested.

(3.7) AAAh may also compute other keying material according to the keys requested by the MN and send it to the MN passing through the AAAv.

* AAAh then send an ARA message to the AAAv including the MIPv6-Mobile-Node-Address and MIPv6-Home-Agent-Address AVPs if the MN did not have any Home address or Home agent.

9.6. Home Agent Behavior

Upon receipt of the HOR, the Home Agent first processes the DIAMETER message: if the HOR is invalid, a HOA is returned with the Result-Code AVP set to DIAMETER_ERROR_BAD_HOR. Otherwise, the Home Agent processes the MIP-Binding-update AVP and creates the Binding Acknowledgement, encapsulating it within the MIP-binding-acknowledgement AVP.

If a home address is needed, the Home Agent assigns one and includes the address in both the Binding acknowledgement message (Home address option) and in the MIPv6-Mobile-Node-Address AVP.

HA then creates the Binding Cache and computes the key(s) for the security association with the MN from the data received.

10. Key distribution

As identified in the previous sections, many security keys need to be set up and shared between the IPv6 mobile nodes and other network entities, such as:

* the key between the mobile node and its Home Agent to authenticate the binding Update and Binding acknowledgement messages

* the key between the mobile node and the access router to protect (e.g. for confidentiality and integrity protection) the data over the access link.

The AAA entities can play a major role in the computation and distribution of these security keys. Two key distribution methods, relying on this AAA infrastructure and allowing authenticated key distribution, are proposed.

10.1. Key distribution based on Random numbers

The home AAA server generates one random number for each required security key. Then taking as inputs, to a key derivation algorithm shared with the mobile node, this random number, the long term key shared with the mobile node and optionally other data, the home AAA server derives the desired security key.

This one is securely transmitted to the network entity, the mobile node wants to share the key with.

And the random number is sent to the Mobile node which can derive the security session key thanks to the knowledge of the long term key and the key derivation algorithm shared with its home network.

This key distribution based on Random numbers is currently used in cellular networks and in the Diameter Mobile IPv4 Application [1]

10.2. Key distribution based on Diffie Hellman

As another possibility, the key distribution can be based on the Diffie Hellman mechanism.

Diffie Hellman allows two nodes to establish a shared secret key in a secure fashion. It, although, has a major vulnerability since it does not allow a node to figure out with whom it is establishing that secret key. To defeat this vulnerability, the two nodes public values must be authenticated.

The AAA infrastructure, and more particularly the security association between the Mobile node and its home network (AAAh) and the security association between the AAAv and AAAh, can provide that authentication.

If the mobile node wants to set up a securiy association with an entity in the visited domain (e.g. home agent assigned in the visited domain), the mobile node first sends its public Diffie Hellman value DH_MN authenticated with the long term security association shared with its AAAh. If the entity with whom the MN wants to set up a security association is in the visited domain, AAAv retrieves the entity's Diffie Hellman public value using intra domain security and sends this value, authenticated with the security association it shares with the AAAh, to the home network of the MN together with the message from the MN.

AAAh authenticates the Diffie Hellman Public values of the entity and the MN. It then sends the MN's Diffie Hellman Public Value to the AAAv using the security association it shares with AAAv, and sends the entity's Diffie Hellman Public Value to the MN, authenticated with the security association shared with the MN.

In this way, AAAh is used to authenticate the Diffie Hellman public values but as a difference with the previous method, since it does not have knowledge of the secret values, it can not derive the value of the session key. This method thus allow to securely distribute the security keys without having the AAA servers being aware of the value of those keys. AAA servers are here used as certificate authorities.

11. Conclusions

The Diameter Mobile IPv6 application defined in this document allows for support of authentication and authorization of IPv6 mobile nodes roaming between different domains. In addition, it support key distribution and mobility by optimizing these procedures. The application defines also new enhanced features that introduce flexibility in the definition of business models for service providers and allow for different types of terminals.

This first version focuses on the different functionalities involved in the support by the AAA infrastructure of inter domain roaming of Mobile IPv6 nodes.

12. Security Considerations

The Diameter Mobile IPv6 application defined in this document does not create new security breaches for the IPv6 MN and the foreign and visited domain. On the contrary, it allows for an effective and efficient MN authentication and authorization when roaming between different domains.

13. References

[1] Pat R. Calhoun, Charles E. Perkins, "Diameter Mobile IPv4 Application" Internet draft, Internet Engineer Task Force, November 2001

[2] Diffie, W. and Hellman, M., "New Directions ijn Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, Nov. 1976, pp. 664-654

[3] Franck Le, Stefano M. Faccin, "Key distribution mechanisms for Mobile IPv6" Internet draft, Internet Engineer Task Force, February 2001

[4] David B. Johnson, Charles Perkins, "Mobility Support in IPv6" Internet draft, Internet Engineer Task Force, November 2001

[5] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, Internet Engineer Task Force, November 1998

[6] Sarvar Patel, "Weaknesses of North American Wireless Authentication Protocol", IEEE Personal Communications, June 1997

[7] Pat R. Calhoun, Haseeb Akhtar, Jari Arkko, Erik Guttman, Allan C. Rubens,Glen Zorn, "Diameter Base Protocol" Internet draft, Internet Engineer Task Force, November 2001

14. Authors' Addresses

Franck Le
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 374-1256
E-mail: franck.le@nokia.com

Basavaraj Patil
Nokia Corporation
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972-894-6709
E-Mail: basavaraj.patil@nokia.com

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA

Phone: +1 650-625-2986
E-Mail: charles.perkins@nokia.com

Stefano M. Faccin
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 894-4994
E-mail: stefano.faccin@nokia.com