MIP6 Working Group
Internet Draft
Expires: January 14, 2005

G. Giaretta
I. Guardini
E. Demaria
TILab
J. Bournelle
M. Laurent-Maknavicius
GET/INT

July 16, 2004

MIPv6 Authorization and Configuration based on EAP
<draft-giaretta-mip6-authorization-eap-01.txt>

Status of this Memo

Copyright Notice

Abstract

This draft defines an architecture, and related protocols, for performing dynamic Mobile IPv6 authorization and configuration relying on a AAA infrastructure. The necessary interaction between the AAA server of the home provider and the mobile node is realized using EAP, exploiting the capability of some EAP methods to convey

generic information items together with authentication data. This approach has the advantage that the access equipment acts as a simple pass-through for EAP messages and therefore does not play any active role in the Mobile IPv6 negotiation procedure, which makes the solution easier to deploy and maintain.

Table of Contents

1. Introduction

Mobile IPv6 [1] requires that Mobile Nodes (MNs) and Home Agents (HAs) share a set of configuration parameters: the MN must know its Home Address, the Home Agent Address and the cryptographic material needed to protect MIPv6 signaling (e.g. shared keys or certificates to setup an IPsec security association). MIPv6 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.

Manual configuration of Home Agents and Mobile Nodes also works as an implicit method for Mobile IPv6 authorization, because only the users that have been administratively enabled on a specific Home Agent are allowed to exploit Mobile IPv6 and its features.

However, in a large network (e.g. the network of a mobile operator), which may include millions of users and many Home Agents, the operational and administrative burden of this procedure may easily become overwhelming. In addition, the extensive use of manual and static configurations limits the flexibility and reliability of the system, in that it is not possible to dynamically assign the HA when

the user enters the network, which would help to optimize performance and resource utilization (e.g. assignment of the HA closest to the MN's point of attachment).

This is generally referred as the Mobile IPv6 bootstrapping problem. As discussed in [2], several bootstrapping scenarios can be identified depending on the relationship between the network operator providing IP services to the MN (Access Service Provider, ASP) and the service provider managing the HA (Mobility Service Provider, MSP). This document describes a solution to the bootstrapping problem that is applicable in a scenario where the ASP and the MSP are the same provider (Integrated ASP, IASP).

The proposed solution performs dynamic Mobile IPv6 authorization and configuration together with MN authentication for network access. MIPv6 negotiation and bootstrapping is controlled by the AAA server of the home provider (IASP), that interacts with the mobile node relying on AAA routing and EAP, exploiting the capability of some EAP methods (e.g. PEAPv2 [4], EAP-FAST [5]) to convey generic information items together with authentication data.

2. Terminology

General mobility terminology can be found in [3]. The following additional terms are used here:

ASP Access Service Provider

IASP Integrated Access Service Provider

MSP Mobility Service Provider

AAA Authentication Authorization Accounting

AAAH AAA server of the Home domain

3. Protocol Overview

The basic idea behind the solution proposed herewith is to perform Mobile IPv6 authorization and configuration during the authentication procedure undertaken by the Mobile Node to gain network access. In particular, this draft defines a method to:

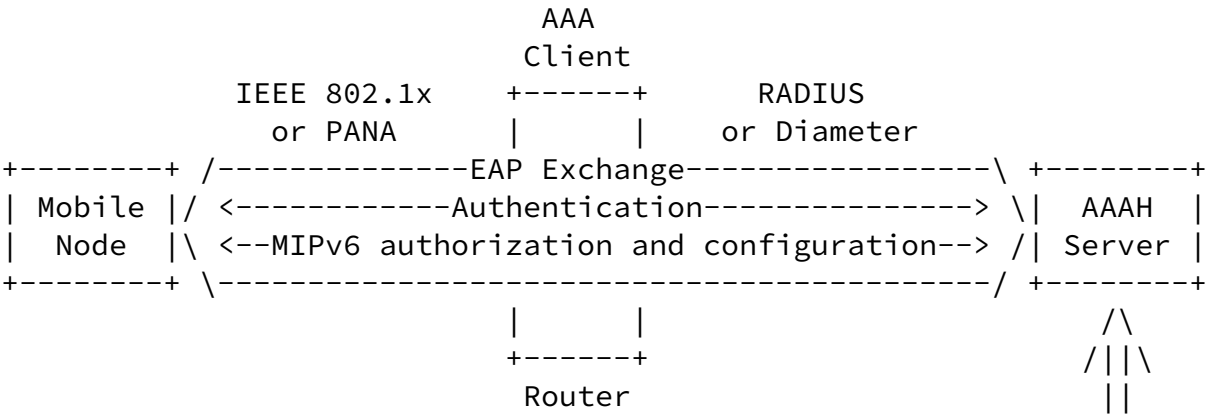
- explicitly authorize the use of Mobile IPv6 based on the service profile of the user, its position within the network, etc.

- dynamically allocate a Home Agent to the Mobile Node;

- dynamically configure Mobile IPv6 start-up parameters (i.e. MIPv6 bootstrapping) on both the Home Agent and the Mobile Node. These parameters include the Home Address and the cryptographic material needed to set-up the IPsec Security Association used to protect Mobile IPv6 signaling (i.e. Binding Updates and Binding Acknowledgements);

- allow the MN to negotiate additional Mobile IPv6 service options, such as the assignment of a HA within the visited domain.

Figure 1 shows the overall architecture of the solution proposed in this draft. The central element of the architecture is the AAA server of the Home Domain (i.e. AAAH), which interacts with both the MN and the selected HA to perform service authorization and configuration.



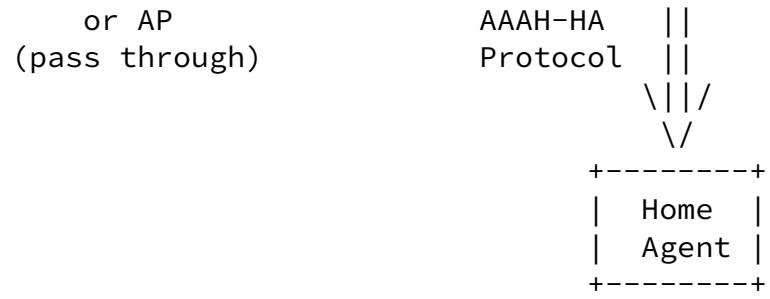


Figure 1 - Solution architecture

The solution is applicable to any access network relying on EAP [6] for user authentication and works with all EAP methods supporting the exchange of general purpose information elements, in the form of TLVs or AVPs, between EAP peers. Exploiting this capability, MN and AAAH can embed MIPv6 negotiation signaling within the same EAP conversation used to carry out user authentication.

This kind of operation is already supported by several tunneled (e.g. PEAPv2 [4]) and non tunneled (e.g. EAP-IKEv2 [8]) EAP methods, that also include native support for encryption, authentication and

integrity protection of exchanged configuration information (e.g. HA address).

Figure 2 shows an overview of the procedure defined to handle MIPv6 bootstrap on the Mobile Node. For the sake of simplicity it is assumed that the employed AAA protocol is Diameter, but obviously RADIUS is suitable as well.

The whole procedure can be divided in six steps:

1. EAP identity exchange (i.e. exchange of EAP Request Identity and EAP Response Identity messages);

2. set-up of a protected channel (e.g. TLS tunnel) for the delivery of subsequent EAP signaling. This is an optional step that is present only if the EAP method provides confidentiality support. It is mandatory only if the MIPv6 negotiation procedure involves the exchange of sensible information;

3. authentication phase. The actual authentication procedure and its security properties depend on the selected EAP method. In tunneled

EAP methods (e.g. PEAPv2) this step may involve one or more complete EAP conversations occurring within a previously negotiated TLS session. Each EAP conversation may accomplish user authentication relying on any available EAP method (e.g. EAP-MD5, EAP-SIM, EAP-AKA);

4. Mobile IPv6 service authorization and configuration. MN and AAAH exchange a sequence of signaling messages to authorize and configure Mobile IPv6. Those messages are encapsulated in TLVs (or AVPs) delivered as part of the on-going EAP session. If the EAP method provides confidentiality this protocol handshake is encrypted using the previously negotiated ciphersuite. During this phase, AAAH selects a suitable Home Agent for the MN and exchanges authorization and configuration data with it using a AAAH-HA protocol (e.g. SNMPv3 [16], COPS-PR [15], a new Diameter application), whose specification is out of the scope of the present document. At the end of this phase, the MN knows its own Home Address, the address of the correspondent Home Agent and the cryptographic material (i.e. pre-shared key) needed to set-up an IPsec security association with IKE [12]. The IKE pre-shared key can be either constructed by AAAH and then delivered to MN in a proper TLV or can be independently derived by MN and AAAH from the EAP key hierarchy;

5. EAP session termination. Assuming the mobile node has been successfully authenticated, the AAAH server sends a Diameter EAP Answer message with Result-Code equal to SUCCESS and, optionally, other authorization AVPs containing some filtering rules to be

enforced on the NAS (e.g. the AP if the access network is a WLAN, or the Enforcement Point in case of an IP network running the PANA [13] protocol). Then the NAS extracts the EAP Success message from the Diameter EAP Answer and forwards it to the MN terminating the EAP session;

6. set-up of IPsec Security Association and MIPv6 registration. At the end of the EAP communication, the MN gains network access and acquires a valid Care-of Address within the visited subnet (e.g. via stateless autoconfiguration); then, using the cryptographic material collected during the MIPv6 negotiation phase (step 4), it performs an IKE exchange to establish the IPsec Security Association with the HA. Finally, the MN performs MIPv6 registration, sending a Binding Update (protected with IPsec) to

the HA.

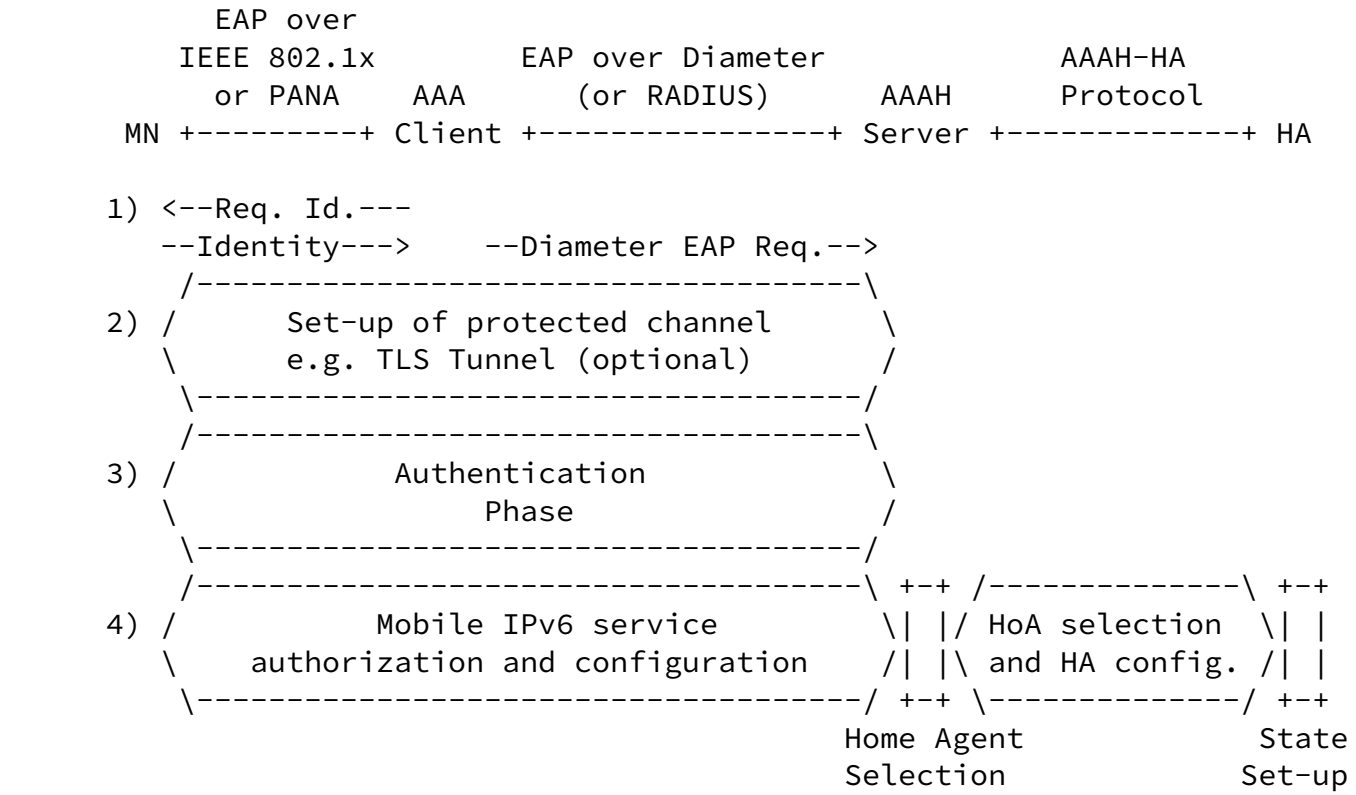


Figure 2 - Overview of Mobile IPv6 bootstrap procedure

This draft also defines the procedures to handle re-authentication events and to manage the termination of the Mobile IPv6 session.

In summary, the proposed architecture has the following advantages:

- allows the operator to maintain a centralized management (on the AAA server) of the user profiles and the authentication,

authorization and accounting procedures for any type of service, including Mobile IPv6;

- improves the reliability and performance of the Mobile IPv6 protocol, in that the HA to be dynamically assigned to the MN can be freely chosen among those that are closest to the user's point of attachment, thus optimizing network usage and reducing the transfer delay for data traffic in bi-directional tunneling;

- can be deployed, or extended with new features, without having to update the access equipment and the AAA protocols in use. Only minor changes in the AAA servers, the Home Agents and the mobile terminals are required, in that the AAA client does not play any active role in MIPv6 negotiation (i.e. it is a pass-through for EAP signaling). This reduces the deployment costs and makes the solution easy to use even when a Mobile Node is roaming with a provider different from its own;

- allows the usage of any AAA protocol supporting the transport of EAP messages for the communication between the AAA client and server (i.e. not just Diameter, but also RADIUS). This significantly simplifies the deployment of MIPv6 in existing communication networks, where support for Diameter protocol in access equipment is not so extensive.

As a whole, the solution adds a maximum of 2 RTTs (see the detailed protocol description in section 5) to the EAP conversation carried out by the mobile node to authenticate itself and gain network access. The number of extra RTTs can be reduced if the employed EAP method has the capability of transporting MIPv6 negotiation TLVs (or AVPs) together with authentication data. Nonetheless, it should be noted that the full negotiation procedure can be undertaken by the MN only during its initial bootstrap, and therefore the performance requirements are not so strict.

4. Requirements on EAP methods

In EAP methods, the EAP peer and EAP server exchange data in order to authenticate the EAP peer and eventually the EAP server (mutual authentication). This draft proposes the use of these exchanges to transport MIPv6 parameters, as part of an handshake that requires at maximum 2 RTTs. Thus, the main requirement for the applicability of our proposal is:

- the EAP method must provide a way to carry arbitrary parameters during or after the authentication phase. This implies that the EAP method must provide messages and mechanisms for this purpose.

Then, for security reasons, the EAP method must provide the following properties:

- mutual authentication: the EAP method must provide mutual authentication. The access network must authenticate users before granting them Mobile IPv6 service and the EAP peer should authenticate the access network before delivering sensitive data;

- integrity: the exchanged MIPv6 parameters must be protected against any alteration and thus the EAP method must provide integrity protection;

- replay protection: the EAP messages containing MIPv6 parameters must be protected against Replay Attack, so that an attacker is not able to get previous given data by replaying an old request;

- confidentiality: depending on which data the AAA server provides to the mobile node (e.g. an IKE pre-shared key), it may be necessary to protect the message exchange against eavesdropping.

The table below checks some existing EAP methods against the requirements listed above.

M-A: Mutual Authentication
R-P: Replay Protection

	M-A	Integrity	R-P	Confidentiality	Exchange of arbitrary Parameters
PEAPv2	x	x	x	x	x
EAP-FAST	x	x	x	x	x
EAP-TTLS	x	x	x	x	x
EAP-IKEv2	x	x	x	x	x
EAP-SIM	x	x	x	x	x
EAP-AKA	x	x	x	x	x
EAP-TLS	x	x	x	x	
EAP-MD5					

In summary, it is possible to note that the procedure described in this draft can be successfully undertaken with several tunneled (PEAPv2, EAP-FAST and EAP-TTLS) and non tunneled EAP methods (EAP-IKEv2, EAP-SIM, EAP-AKA, EAP-TLS), that all support the transport of arbitrary parameters in the form of TLVs or AVPs.

5. Detailed Description of the Protocol

This section details the procedures and message exchanges that can be adopted by the network operator to explicitly authorize the activation of Mobile IPv6 support for a specific user as well as enable dynamic bootstrapping of MIPv6 protocol parameters (e.g. Home Address, Home Agent Address).

5.1 Mobile Node bootstrap

If EAP is used for access control, when the MN enters the network it is immediately polled for its identity, by means of an EAP Request Identity message. This message is used to start the EAP communication. The MN replies sending its identity, in the form of a

NAI (Network Access Identifier), within an EAP Response Identity message, that is received by a local attendant (e.g. the Access Point

in the case of a Wireless LAN) and forwarded via AAA routing to the AAAH server using the Diameter EAP Application (or the RADIUS EAP extensions). Then the AAAH server selects an EAP method (e.g. based on the user service profile) and proposes it to the MN in subsequent EAP messages. In order to enable the Mobile IPv6 negotiation procedure defined in this document, the EAP method chosen by the AAAH server must be an EAP method supporting the transport of general purpose and variable length information elements, in the form of TLVs (or AVPs), together with authentication data (see section 4).

After this initial handshake, MN and AAAH undertake the actual authentication phase, that may require the exchange of a variable number of EAP Request/Response messages. In many EAP methods, like PEAPv2 or EAP-IKEv2, the authentication phase is preceded by the establishment of an encrypted channel between MN and AAAH that provides protection capabilities (i.e. privacy, integrity protection, etc.) for all the messages exchanged during the rest of the EAP conversation.

As soon as the authentication phase is completed, the procedure for MIPv6 bootstrapping may take place. In order to do that, the MN and the AAAH server exploit the on-going EAP communication to exchange a sequence of signaling messages encapsulated in a new TLV, called MIPv6-Authorization-TLV. This TLV is used as a generic container for other, more specific, TLVs.

The whole bootstrapping procedure is depicted in Figure 3.

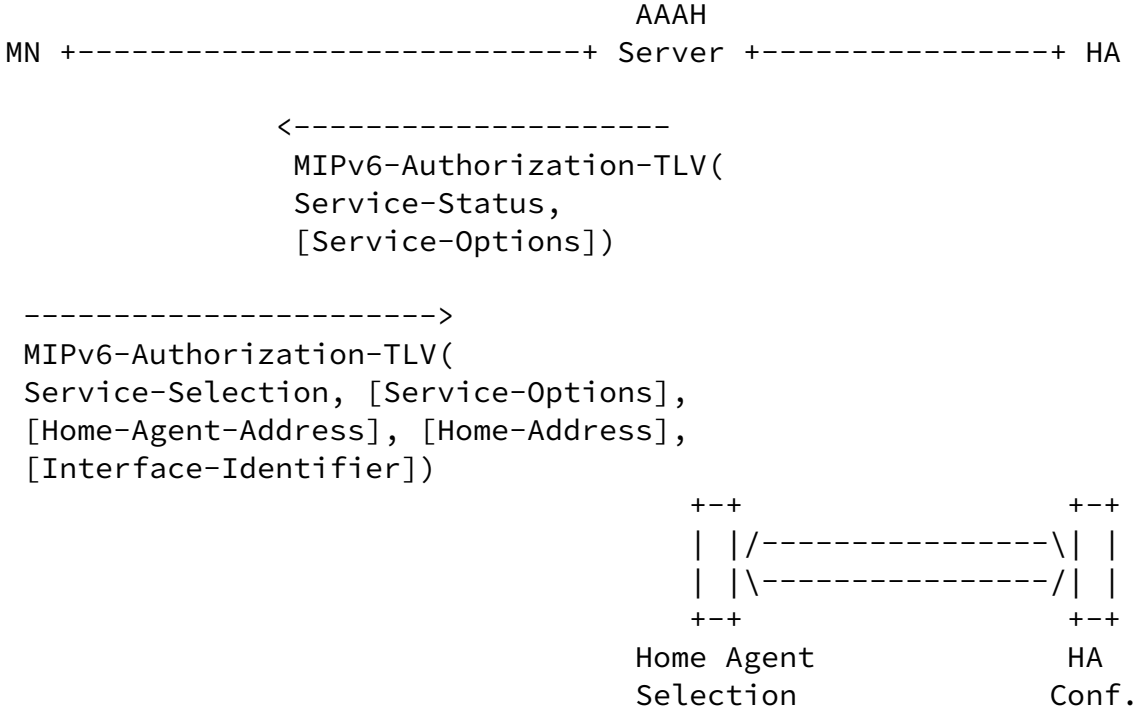


Figure 3 - MIPv6 bootstrapping procedure

AAAH starts the MIPv6 negotiation phase sending to the MN a MIPv6-Authorization-TLV including the following TLVs:

- Service-Status-TLV: used to communicate whether the home domain is willing to provide Mobile IPv6 service to the MN. This might depend on the user service profile or on other administrative rules (e.g. service accountability);

- Service-Options-TLV (optional): used to specify other service options the MN can ask for (e.g. allocation of a HA in the visited domain).

MN replies to this first message confirming its intention to start Mobile IPv6 and, optionally, providing a set of hints on the desired service capabilities; this is achieved delivering a MIPv6-Authorization-TLV including the following TLVs:

- Service-Selection-TLV: used by the MN to specify if it is willing to activate Mobile IPv6 protocol operation;

- Service-Options-TLV (optional): used by the MN to communicate which service options, among those previously advertised by AAAH, it would like make use of;

- Home-Agent-Address-TLV (optional): used by the MN to suggest a preferred Home Agent. This can be a HA with whom the MN has a pre-configured Security Association or a HA acquired through dynamic HA address discovery. The AAAH server treats this indication just as a hint, which means that, for administrative reasons, the MN may be assigned a Home Agent different from the one previously requested;

- Home-Address-TLV (optional): used by the MN to suggest a preferred Home Address (e.g. an address pre-configured on one of its network interfaces); like the previous TLV, this indication is considered only as a hint by the AAAH server;

- Interface-Identifier-TLV (optional): through this TLV, the MN can suggest a preferred Interface Identifier (selected according to [9] or following other criteria) to be used by the AAA infrastructure to build the Home Address starting from the selected home prefix. Also in this case, this information, if present, is treated as a pure hint by AAAH.

If in the Service-Selection-TLV the MN has chosen not to make use of

Mobile IPv6, AAAH terminates the EAP communication sending an EAP Success message, since the authentication procedure has been accomplished successfully.

Otherwise, if the MN has confirmed its willingness to start MIPv6 service, AAAH selects a suitable Home Agent through a Home Agent Selection Algorithm. Possible parameters to be taken into account by this algorithm include: current load of available HAs (e.g. number of active bindings), location of the MN and, eventually, the preferences provided by the MN itself in the previous message exchange (i.e. Service-Options-TLV, Home-Agent-Address-TLV, Home-Address-TLV). For example, based on the knowledge of the MN's current point of attachment (i.e. the current NAS), the AAAH server may select, among the HAs available in the home domain, the one that is closest to the MN in terms of IP routing hops. This approach is normally expected to improve performance. However, the detailed definition of a Home Agent Selection Algorithm is out of the scope of this document.

After a suitable HA has been identified, AAAH interacts with it to dynamically configure all the state needed to enable subsequent MIPv6 protocol operations, including the authorization lifetime of the

MIPv6 service granted to the MN. Possible protocols that can be used for this purpose include Diameter (through a new Diameter Application), SNMPv3 or COPS-PR. Further details about this communication are provided in section 6. Anyway, the detailed specification of the interface between AAAH and HA is out of the scope of this document.

As soon as the AAAH server has configured the state on the HA, it continues the EAP session communicating to the MN all the MIPv6 configuration data it is waiting for. This is achieved delivering to the MN an EAP Request containing a MIPv6-Authorization-TLV and the following sub-TLVs: Home-Address-TLV (i.e. the home address) and Home-Agent-Address-TLV (i.e. the address of the HA).

The pre-shared key needed to bootstrap the IKE session with the Home Agent, and set-up the correspondent IPsec Security Association, can be derived by the MN from the keying material exported by the employed EAP method. This approach provides excellent security guarantees but requires the definition of a specific Application Master Session Key (AMSK) [14] bound to MIPv6. Alternatively, if the on-going EAP session provides confidentiality support, the AAAH

server can override the default behaviour by explicitly delivering a valid PSK to the MN within an IKE-PSK-TLV.

After the MN has received all the configuration data from the AAAH server (i.e. HA address, Home Address and optionally the PSK), it sends back an EAP Response containing a Negotiation-Result-TLV, stating whether it accepts, or refuses, the proposed arrangement. If the MN refuses the configuration, the AAAH server should immediately release the resources previously allocated on the Home Agent.

After the completion of the EAP session, MN holds all data needed to perform Mobile IPv6 registration: the MN knows its Home Address, the address of the correspondent Home Agent and all cryptographic data needed to establish the IPsec security association with it; furthermore, since it has been successfully authenticated, the MN can acquire an IPv6 address to be used as Care-of Address.

The first operation carried out by the MN after the acquisition of the Care-of Address is the establishment of the IPsec Security Association with the HA, that is mandated by [1] to protect MIPv6 location update signaling. Set-up of the IPsec SA can be accomplished following the procedure detailed in [11]. In this regard, it is important to note that:

- since the mutual authentication in IKE Phase 1 is based on a Pre-Shared Key (PSK), Aggressive Mode must be used. This is because Aggressive Mode is the only way to use PSK authentication with a

NAI as peer identifier [12]. Indeed, the NAI of the MN is the only identity information stored in the HA (see section 6.2);

- in IKE phase 1 messages, the source address used by the MN has to be the Care-of Address, as described in [11]; the Home Address is used only in IKE phase 2;

- in IKE phase 2 (Quick Mode), while still using the CoA as source address of IKE messages, the MN has to use the Home Address as its peer identifier, so that the HA can correctly set the MN entries in its Security Policy Database (SPD) and in the Security Association Database (SAD).

As soon as the IPsec Security Association is established, MN can send a Binding Update to the HA, thus starting up Mobile IPv6 service.

5.2 Management of reauthentication events

At the expiration of AAA session time-outs or after a change in the point of attachment to the network (e.g. change of Access Point), a re-authentication procedure is performed leading to the user identity to be checked again along with its right to continue exploitation of network resources. To that purpose the AAAH server may repeat a full authentication or, alternatively, decide to use optimizations in order to make the procedure faster. Once this phase is completed the AAAH server also undertakes the re-negotiation of the MIPv6 service.

Since the MIPv6 bootstrapping procedure is assumed to be completely stateless, when a re-authentication event occurs the AAAH server may not know the state of the MIPv6 service on the MN. For this reason the AAAH server starts the MIPv6 negotiation as in the bootstrap case: it delivers a MIPv6-Authorization-TLV containing a Service-Status-TLV and optionally a Service-Options-TLV.

If the MIPv6 service is not active on the MN the procedure continues as described in section 5.1. Otherwise, the MN replies with a MIPv6-Authorization-TLV containing a Service-Selection-TLV indicating that the MIPv6 service is already in use. Furthermore, the MN inserts the Home-Agent-Address-TLV and the Home-Address-TLV to inform the AAAH server about its current state. The AAAH server can then get in touch with the HA to check the integrity of the state and eventually renew the MIPv6 authorization lifetime. If this procedure is accomplished successfully, the AAAH server terminates the EAP communication sending an EAP Success message. Otherwise, the AAAH server should continue the EAP communication renegotiating the MIPv6 service (i.e. allocation of a new HA and related Home Address).

This solution can be easily deployed even within a network including several AAA servers, each one managing a subset of the available

Network Access Servers (NASs). This is because the re-negotiation procedure does not assume to have any long term state related to Mobile IPv6 stored on the AAAH server. In this way, everything works correctly even if, due to MN's movements within the network, the AAAH server that handles the re-authentication is not the same server that authenticated the MN for the first time and performed the MIPv6 bootstrapping procedure.

6. Home Agent considerations

This section provides further thougths about the AAAH-HA communication and lists specific features that have to be supported by the Home Agent to allow dynamic negotiation of Mobile IPv6 protocol parameters.

6.1 Requirements on AAAH-HA communication

This draft details only the message exchange between the MN and the AAAH server. Obviously a complete Mobile IPv6 bootstrapping solution requires also the definition of a mechanism for the communication between the Home Agent and the AAAH server. Possible protocols that may be used for this purpose include SNMPv3, COPS-PR or Diameter.

The selected protocol should allow the AAAH server to:

- verify if the selected HA is available to serve the MN (e.g. based on current traffic load and on the number of active bindings);

- send to the HA the MN's NAI, the authorization lifetime of the Mobile IPv6 service granted to the MN, the IKE PSK to be used to bootstrap the IPsec Security Association and, optionally, a set of hints for the construction of the Home Address (i.e. a preferred Home Address or a preferred Interface Identifier);

- obtain from the selected Home Agent a valid Home Address to be assigned to the MN;

- force the termination of the Mobile IPv6 service for a specific MN removing the state stored on the correspondent HA;

- manage the extension of the authorization lifetime for a specific MN;

- retrieve the state associated to a specific MN from the correspondent HA.

Moreover, the protocol selected to implement the communication between the AAAH server and the HA should fulfill the following general requirements:

- inactive peer detection: the AAAH server should be able to

promptly detect an HA failure. This may be useful to aid the HA selection algorithm;

- mutual-authentication: the AAAH server and the HA must be able to authenticate each other in order to prevent the installation of unauthorized state on the HA;

- confidentiality: since the IKE pre-shared key is derived by the AAAH server and then delivered to the HA, the correspondent message exchange must be protected against eavesdropping. This implies that confidentiality is one of the main requirements;

- integrity: the exchanged configuration parameters must be protected against any alteration and thus the protocol must provide integrity protection.

6.2 Management of MIPv6 authorization state

The Home Agent is required to store some authorization data for each of the MNs it is serving. A new data structure may be used for this purpose and it should include at least the following fields:

- NAI of the user;

- Home Address assigned to the MN;

- Cryptographic Data: this field includes all the information to be used for bootstrapping IKE, that is the PSK value and its lifetime;

- Authorization Lifetime: it is the lifetime of the Mobile IPv6 service granted to the MN;

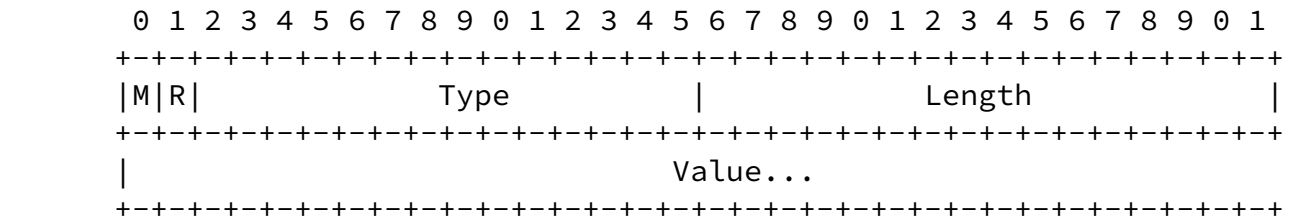
At the expiration of the Authorization Lifetime the HA should check if there is an active entry for the MN in its Binding Cache in order to verify if the MN is still using Mobile IPv6. If the entry is available the Home Agent should negotiate with the AAAH server an extension of the Authorization Lifetime granted to the MN. Otherwise, the HA should immediately release the authorization state associated to that MN and eventually notify the session termination to the AAAH server (e.g. by means of a Session Termination Request if the employed AAAH-HA protocol is Diameter).

Moreover, the release of the resources previously allocated on the Home Agent can be undertaken at any time by the AAAH server. Typically this happens at credit exhaustion or when the MN disconnects from the network.

The policies adopted by the AAAH server to release the resources allocated to the MN may vary depending on the user service profile. For instance, the AAAH server may decide to postpone the release of the resources on the HA in order to allow the MN to continue using the Mobile IPv6 service even if it has moved to an access network for which no roaming agreements are in place (e.g. a corporate network or a network providing cost-free access). In that case, the MN can continue to rely on the IPsec SA previously negotiated with the HA and the respective authorization is managed through the Mobile IPv6 Authorization Lifetime.

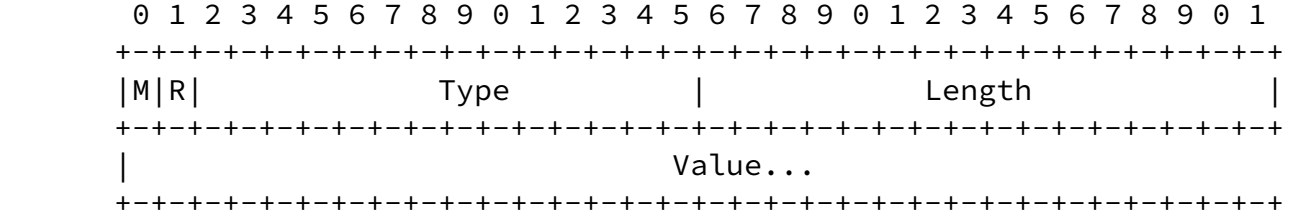
7. New EAP TLVs

The general format of an EAP-TLV is depicted below.



TLVs defined in this draft are:

- MIPv6-Authorization-TLV. This is a generic TLV which carries all TLVs related to MIPv6 authorization and configuration. It is defined as follows:



M

0 - Non-mandatory TLV

R

Reserved, set to zero (0)

Type

TBD - MIPv6-Authorization

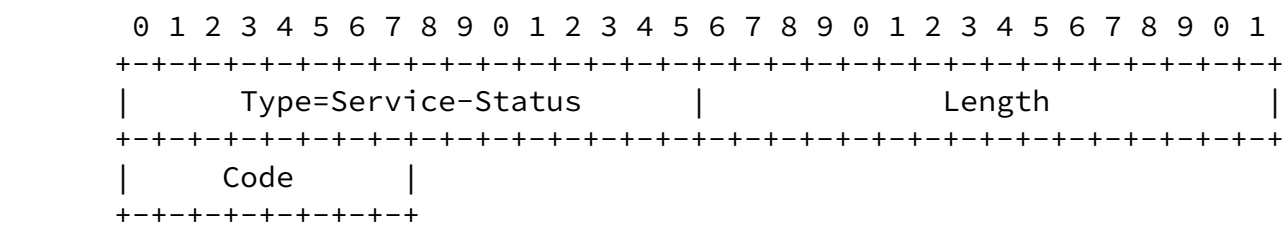
Length

The length of the Value field in octets

Value

This field carries the subsequent TLVs

- Service-Status-TLV. This TLV is sent by the AAAH to inform the MN about the status of Mobile IPv6 service. It is defined as follows:



Type

TBD - Service-Status

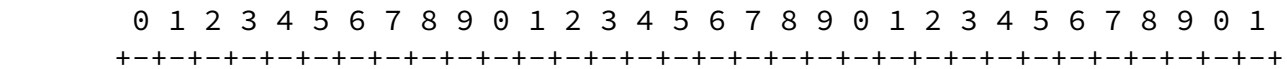
Length

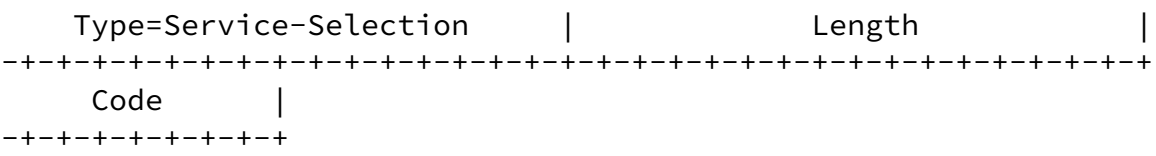
1

Code

0 = MIPv6 service is available
1 = MIPv6 service is not available

- Service-Selection-TLV. This TLV is sent by the MN to inform the AAAH whether it wants to activate MIPv6 service or whether the service is already active.





Type

TBD - Service-Selection

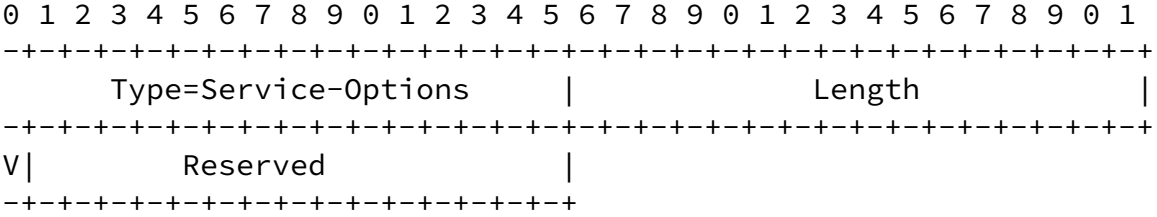
Length

1

Code

0 = activate MIPv6 service
1 = MIPv6 service already active
2 = do not activate MIPv6 service

- Service-Options-TLV. This TLV is used by the AAAH server to advertise the service options the MN can ask for. It is also used by the MN to communicate its selection to the AAAH. So far only the HA in visited domain option has been defined. The TLV has the following format:



Type

TBD - Service-Options

Length

2

V

from AAAH to MN:

0 = AAAH cannot provide a HA in the visited domain

1 = AAAH can provide a HA in the visited domain

from MN to AAAH:

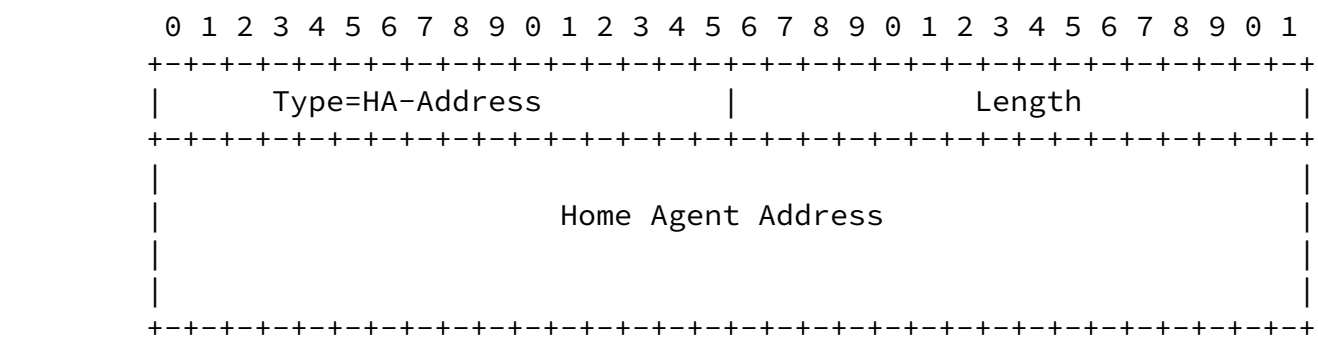
0 = MN does not specify any preference on HA location

1 = MN is requesting a HA in the visited domain

Reserved

15 bit reserved set to 0

- Home-Agent-Address-TLV. It is defined as follows:



Type

TBD - Home-Agent-Address

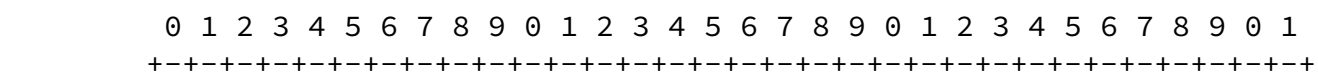
Length

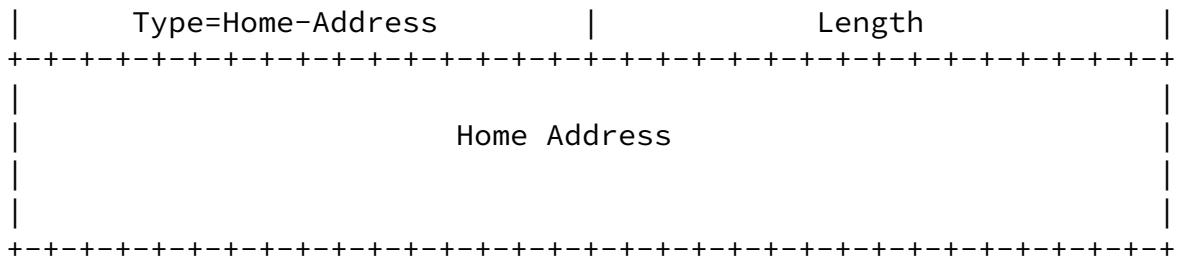
16

Value

Home Agent Address

- Home-Address-TLV. It is defined as follows:





Type

TBD - Home-Address

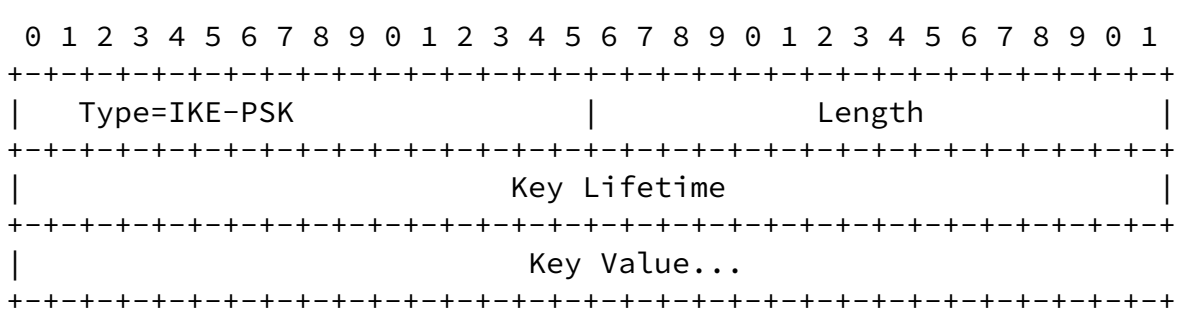
Length

16

Value

Home Address

- IKE-PSK-TLV. This TLV carries data related to IKE bootstrap; the value field contains the PSK lifetime and the PSK value.



Type

TBD - IKE-PSK

Length

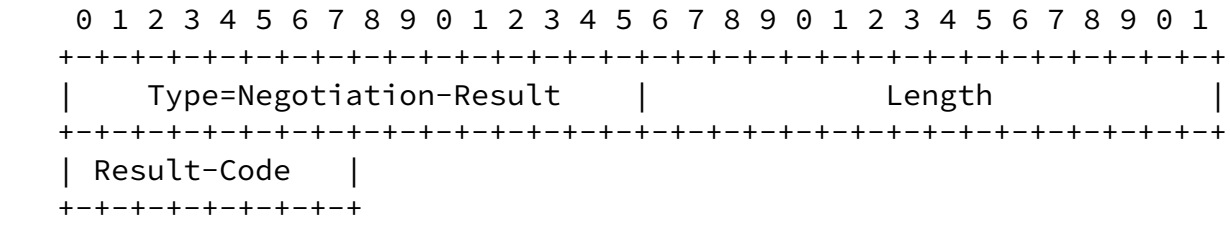
4 + Key length

Value

Key Lifetime - the lifetime of the PSK in seconds. A value of all ones means infinite

Key Value - the value of the PSK

- Negotiation-Result-TLV. It is defined as follows:



Type

TBD - Result

Length

1

Value

0 = Success
128 = Failure

8. Security Considerations

The Mobile IPv6 bootstrapping procedure described in this document assumes the MN and the AAA server of the home domain exchange the necessary parameters exploiting the EAP communication established for network access authentication. Therefore, to secure the bootstrapping procedure, the employed EAP method must support mutual authentication as well as integrity and replay protection. Moreover, if the pre-shared key needed to bootstrap the IPsec SA with the Home Agent is

not derived from the EAP key hierarchy but explicitly delivered to the MN by the AAAH server, the EAP method must also provide confidentiality. Several tunneled and non tunneled EAP methods, like PEAPv2 and EAP-IKEv2, fulfill all of these security requirements.

Acknowledgments

The authors would like to thank Simone Ruffino, Tom Hiller, Hannes Tschofening, Rafael Marin Lopez, Hiroyuki Ohnishi, Mayumi Yanagiya and Yoshihiro Ohba for their valuable comments.

References

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

[2] Patel, A. et al. "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-00 (work in progress), July 2004.

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

[4] Palekar, A. et al., "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-07 (work in progress), October 2003.

[5] N.Cam-Winget, D. McGrew, J. Salowey, H.Zhou, "EAP Flexible Authentication via Secure Tunneling (EAP-FAST)", draft-cam-winget-eap-fast-00.txt (work in progress), February 2004

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

[7] Funk, P., Blake-Wilson, S., "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", draft-ietf-pppext-eap-ttls-04 (work in progress), April 2004.

[8] Tschofenig, H., Kroeselberg, D., Ohba, Y., "EAP IKEv2 Method", draft-tschofenig-eap-ikev2-03, February 2004.

[9] Narten, T., Draves, R., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[10] Faccin, S., Perkins, C., Le, F., Patil, B., "Diameter Mobile IPv6 Application", draft-le-aaa-diameter- mobileipv6-03 (expired), April 2003.

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

[12] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[13] Forsberg, D. et al., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-04 (work in progress), May 2004.

[14] Aboba, B., Simon, D., Arkko, J., Levkowetz, H., "EAP Key Management Framework", draft-ietf-eap-keying-02 (work in progress), July 2004.

[15] K. Chan, D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith, R. Yavatkar, "COPS Usage for Policy Provisioning,", RFC 3084, March 2001.

[16] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

Authors' Addresses

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2286904
Email: gerardo.giaretta@tilab.com

Ivano Guardini

Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2285424
Email: ivano.guardini@tilab.com

Elena Demaria
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2285403
Email: elena.demaria@tilab.com

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France
Email: julien.bournelle@int-evry.fr

Maryline Maknavicius-Laurent
GET/INT
9 rue Charles Fourier
Evry 91011
France
Email: maryline.maknavicius@int-evry.fr

Intellectual Property Statement

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

Copyright Statement

Acknowledgement

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