MIP6
INTERNET-DRAFT
Date: February 2004
Expires: August 2004

Stefano M. Faccin
Franck Le
Basavaraj Patil
Charles E. Perkins
Nokia Research Center

Francis Dupont
ENST Bretagne

Maryline Laurent-Maknavicius
Julien Bournelle
INT Evry

Mobile IPv6 Authentication, Authorization, and Accounting Requirements
<draft-le-aaa-mipv6-requirements-03.txt>

Status of This Memo

Abstract

This document describes the motivation why Diameter support for Mobile IPv6 is required and needs to be developped. It analyses the requirements expressed in RFC 2977 which was written both for MIPv4

and MIPv6; and it finally updates the IPv6 requirements for the AAA support for Mobile IPv6 to reflect the latest modifications and evolution of the Mobile IP, AAA and other relevant working groups.

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. But 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.

RFC 2977 [1] describes the requirements that have to be supported by a AAA service to aid in Mobile IP services; and Diameter extensions for Mobile IPv4 [2] 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 offer any mechanism by which the visited network can authenticate and authorize access to the network. In addition, extending the Diameter Mobile IPv4 Application 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.

Some Diameter Mobile IPv6 Application will have to be specified to allow Mobile IPv6 nodes to receive services from foreign domains. Such application will allow:

* local network access control: cf section 3
* remote network access control: cf section 3
* credentials/trusted third party: the AAA server act as trusted third party allowing user authentication and key distribution.
* MN-Attendant LSA establishment: cf section 3.1
* home address allocation

* home agent allocation (cf. 4.5): eventhough Mobile IPv6 specifies a dynamic home agent assignement procedure, the AAA servers allow a secure and efficient alternative method.

* transport of messages for MN-HA SA establishment by AAA

* key distribution for MN-HA SA establishment (need a higher level of trust than for the previous)

* transport of MN-HA mobility signaling messages (need the two previous items)

But before designing the solution, this document describes the Mobile IPv6 AAA requirements: RFC 2977 [1] describes the requirements for both Mobile IPv4 and Mobile IPv6 and this document will therefore be taken as the base. But since that time, many changes have happened in the IETF, different mechanisms have been defined and many modifications have ocurred in the Mobile IP and AAA working Groups; this draft will thus update the requirements to reflect those latest modifications for the Mobile IPv6/AAA requirements.

In RFC 2977 [1], after a description of the model, the requirements were presented in a progressive fashion:

- Requirements based on the general model

- Requirements based on providing IP service for mobile nodes

- Requirements derived from specific Mobile IP needs

This document will take the same structure, updating the requirements for the IPv6 specific case, and taking into account the latest amendments of the working groups.

2. Terminology

This document frequently uses the following terms in addition to those defined in RFC 2977:

Home Domain
: A Home Domain is the administrative domain with whom the user maintains an account relationship.

Foreign Domain
: An administrative domain, visited by a Mobile IP client, and containing the AAA infrastructure needed to carry out the necessary operations enabling network access and Mobile IP registrations.

Attendant
: The attendant is the entity that extracts identification and authorization data sent by the client and forwards them to AAAL for verification.

AAAL
: The AAA server in the foreign domain that mediates local access to the AAA infrastructure.

AAAH
: The AAA server in the home domain which is able to authorize each of its clients.

Credential
: Data provided by a client to the AAA server in a message authentication code constructed using a secret shared between the client and AAAH.

Local Security Association
: Security association shared between the client and the foreign domain. The sharing of such SA gives the foreign domain significant local control over the authentication of a roaming client: Local Security Association e.g. allows the foreign domain to authenticate the user and perform key distribution without involvement of any external authority such as the client's home domain. LSA can thus allow optimizations in terms of signaling load towards the external authorities and delay involved in the security procedures.

Key distribution
: Process or protocol whereby a shared secret becomes available to two or more parties for subsequent crytographic use.

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in RFC 2119 [11].

3. Basic model

The Basic Model described in RFC 2977 [1] still applies:

> When a client belonging to one administrative domain (called the home domain) roams to another administrative domain (called the foreign domain) and needs to use the local network resources, an attendant in the foreign domain is likely to require that the client provides some credentials that can be authenticated before access to the resources is permitted. These credentials may be something the foreign domain understands, but in most cases they are assigned by, and understood only by the home domain, and may be used for setting up secure channels with the mobile node.
>
> The attendant which often does not have direct access to the data needed to complete the transaction will forward the request to the local AAA server.
>
> The local AAAL itself may not have enough information stored locally to carry out the verification for the credentials of the client. In such cases, the AAAL has to contact other external authorities such as the AAAH to verify the client's credentials.
>
> In many typical cases, the authorization depends only upon secure authentication of the client's credentials. And once the authorization has been obtained by the local authority, and the authority has notified the attendant about the successful negotiation, the attendant can provide the requested resources to the client.

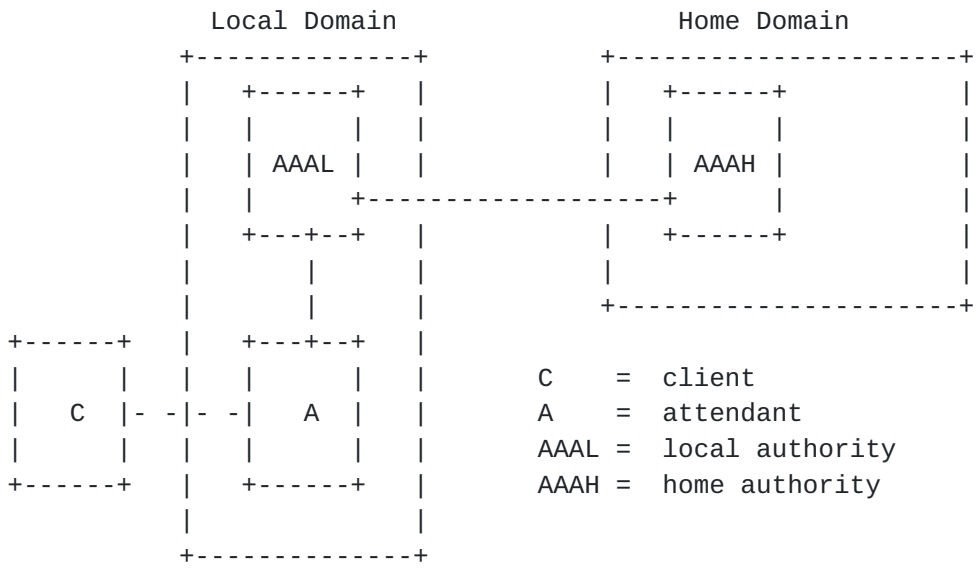

Figure 1: AAA Servers in Home and Local Domains

Therefore, the Security Association Model and the requirements deduced from this model (RFC 2977 [1] section 3) are still valid for IPv6.

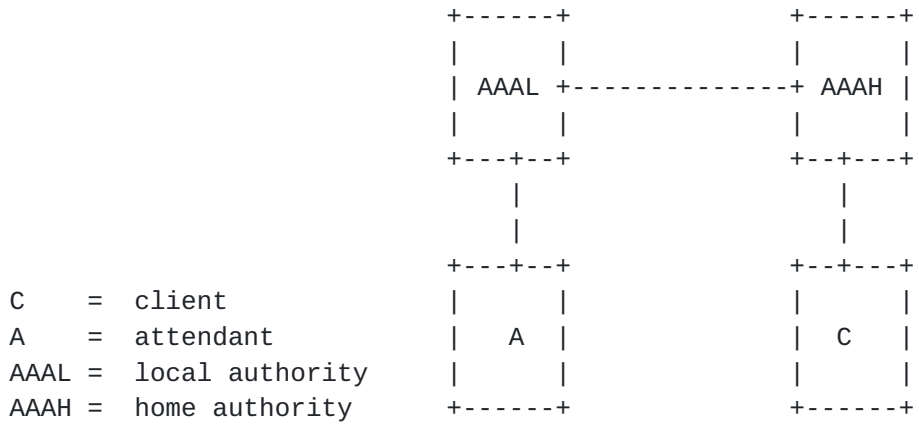

Figure 2: Security Associations

3.1. Modifications to basic model

A modification to the basic model that is required is the need to support and utilize Local Security Associations. LSAs have been recently introduced in IETF ([3], [5]). After an initial successful authentication of the user through the home domain, LSAs allow the local domain to authenticate the user and perform key distribution without involvement of any external authority such as the client's

home domain. LSA can thus allow optimizations in terms of signaling load between network domains and delay caused by security procedures between network domains: the requests can be processed locally and the latency due to the time taken to traverse the wide-area Internet that is likely to separate the AAAL and the AAAH can thus be avoided.

Thus, the following requirement is formulated:

- LSA ([3], [5]) SHOULD be supported and utilized by AAA in order to support, e.g., user re-registration, user re-authentication, key distribution/refreshment, etc.

3.2. AAA Protocol Roaming Requirements

The Diameter Mobile IPv6 Application is a new application extension to the Diameter Base Protocol [6]: the retransmission algorithms of the transport mechanism will therefore rely on the already defined ones.

Except this remark, all the other requirements described in section 3.1 of RFC 2977 [1] are still valid.

4. Requirements related to basic IP connectivity

Since the usages scenarios described in section 4 of RFC 2977 [1] are still valid, the two main requirements on AAA for IP connectivity are still applicable:

- Either AAA server MUST be able to obtain, or to coordinate the allocation of, a suitable IP address for the customer, upon request by the customer

- AAA servers MUST be able to identify the client by some means other than its IP address

And so are the derived ones such as:

- Policy in the home domain may dictate that the home agent instead of the AAAH manages the allocation of the home IP address for the mobile node. AAA servers MUST be able to coordinate the allocation of an IP address for the mobile node at least in this way.

In the Diameter Mobile IPv4 Application, clients use the Network Access Identifier (NAI) [7] to identify themselves. In the same way, in MIPv6, Mobiles nodes should use the NAI: AAA servers today identify clients using NAI, and in addition using NAI allows AAAL to

easily determine the home domain ("realm") for the client.

From these reasons, derives the following requirement:

- In the Diameter support for MIPv6, mobiles nodes SHOULD use the NAI

5. AAA for Mobile IP

Since RFC 2977 [1] was written for both MIPv4 and MIPv6 and the previous sections mainly describe the general, AAA and functional requirements, most of them are still valid for MIPv6.

This section analyzes the Mobile IPv6 specific requirements and, as MIPv6 and MIPv4 are quite different when looking at the architectural model(MIPv6 does not e.g. have the equivalent of a Foreign Agent), the main differences are described in this section.

5.1. Attendant functionnality

As defined in the basic model (section 2), the attendant is responsible for authorization and authentication of the user before giving him access to the local resources. The attendant receives the user's credentials and is in charge of performing the necessary functions to verify it (e.g. translating to the appropriate protocols) but the attendant is not responsible for the address allocation.

The attendant MAY interact with a DHCP Server, but instead of the attendant functionality being the address allocation entity as suggested in RFC 2977 [1], it is suggested that the attendant SHOULD be some other agent in the network. Since RFC 2977 [1] was written, several new mechanisms have evolved and new ones have been introduced in IETF, e.g. new working Groups have been created such as PANA.

This draft suggest the following requirement for support of Mobile IPv6 by AAA:

- AAA SHOULD support different network access protocols (e.g. PANA). The location of the attendant depends on the specific protocol. E.g. in the specific case of PANA, the attendant SHOULD be located in the PANA Agent defined in [3] if such agent is present in the network.

5.2. Security associations

RFC 2977 [1] requires the AAA servers to be able to perform key distributions, and in particular requires supports for key distribution for the security associations between the Home Agent and the Foreign Agent, and the SA between the Mobile Node and the Foreign Agent.

Since Mobile IPv6 does not have a Foreign Agent and mobility support in the protocol is different (i.e. MN directly sends Binding Updates directly to the home agent and correspondent nodes), these requirements do not apply for MIPv6 and SHOULD not be considered.

The remaining requirements about key distribution are still valid (support of mobile node-home agent security association, certificate validation, SA distribution, etc.) and SHOULD be supported for Mobile IPv6.

In the same way that in MIPv4, a security association is established between the mobile node and the attendant; for MIPv6, it is still relevant to set up a SA between the mobile node and the attendant, more particularly for Local Security Association.

5.3. Authentication and key distribution mechanisms.

When RFC 2977 [1] was written, the requirements did not specify any particular authentication and key distribution mechanisms. However,the Diameter Mobile IPv4 Application defines a very specific mechanism.

In order to make Mobile IPv6 support in AAA flexible and future proof, the following requirement is considered:

- for authentication and key distribution, support for Mobile IPv6 in AAA SHOULD allow different mechanisms to be supported.

EAP provides a more generic mechanism for authentication and the advantages of EAP are explained in RFC2284. Each authentication method (such as CHAP [9], AKA [10], etc.) has its own properties, and different users belonging to different home domains may have different requirements. The adoption of EAP as one of the mechanisms supported by AAA for Mobile IPv6 would provide a wider choice for the AAAH and MN of which authentication method to adopt based on their policies and requirements.

As for the key distribution, the Mobile IPv6 support in AAA should also allow different possible protocols and more flexible behavior.

For this reason, the following requirement is expressed:

- for authentication and key distribution, support for Mobile IPv6 in AAA SHOULD allow for AAA to act only as trusted third party.

This would allow the MN and the home agent to authenticate each other and perform key distribution with other mechanisms (e.g. IKE) without directly involving AAA.

If no SA is shared by MN and HA, an SA MAY be negotiated through AAA exchanges with AAA acting as trusted third party

5.4. Integration of Mobile IP and AAA procedures

The following requirement is already present in RFC 2977 [1] and still applies to Mobile IPv6:

- After the initial registration, the mobile node is authorized to continue using Mobile IP at the foreign domain without requiring further involvement by the AAA servers.

This implies that at the initial registration the mobile node needs to be authenticated and authorized, and mobility procedures need to be performed (e.g. between the foreign agent and the home agent) to guarantee the mobile node can use Mobile IP.

Initial registration may take a long time, e.g. if the foreign and the home domains are far away from each other. In order to reduce latency in the initial registration, it is important to reduce the time taken for communications between the AAA servers to traverse the wide-area Internet that is likely to separate the AAAL and the AAAH.

In the AAA support for Mobile IPv4, in order to reduce the number of messages between domains that traverse the network for initial registration of a Mobile Node and the resulting latency, the initial registration message between the foreign agent and the home agent is carried by AAA through the AAA functions in the visited network (AAAL) and the home network (AAAH). As a result, latency is reduced by handling the initial registration in conjunction with AAA and the mobile IP mobility agents.

A similar solution should be adopted also for the support of Mobile IPv6, and the following requirement is formulated:

- it SHOULD be possible to combine authorization and authentication of a mobile node through AAA with Mobile IPv6 mobility procedures (e.g. Binding Update).

Moreover, subsequent registrations, and authentication could be optimized thanks to LSA.

Thanks to this requirement, unless the authentication mechanism adopted requires several round trips, all needed AAA and Mobile IP functions can be processed during a single exchange of messages between the foreign domain and the home domain.

5.5. Home agent allocation

Another important requirement that needs to receive special attention when defining the IPv6 solution is the Home agent allocation. Scenarios for home agent allocation have already been described in RFC 2977 [1] and still apply.

The Diameter Mobile IPv4 Application defines the procedure to assign the Home agent in the visited domain. The ability to support this not only provides more flexibility, but also allows more business scenarios and reduces delays for the Mobile IP signaling procedures. Thanks to the application, the Home Agent allocated to the MN needs not be part of the MN home domain. E.g. this situation can occur if the home address of the mobile node is provided by one domain (e.g. an ISP that the mobile user uses while at home), and the authorization and accounting by another (specialized) domain, e.g., a credit card company. Another example is that the MN may want to get connectivity and the ability to be mobile in a foreign domain and by using the subscription with a home ISP (home domain), but the MN does not desire to be reachable for packets destined to the MN home address given by the home ISP.

Such functionality SHOULD also be considered when designing the AAA support for MIPv6 solution.

6. Security considerations

This document does not specify a solution but describes the requirements that need to be considered when developing a solution for Mobile IPv6 and AAA. The security requirements have been listed and explained in the previous sections. Different solutions MAY fulfill the functional requirements expressed in this document. For each of these, the security implications need to be analyzed

7. References

[1] Glass, et al.; Mobile IP Authentication, Authorization and Accounting Requirements, RFC 2977, Internet Engineering Task Force, October 2000.

[2] Pat R. Calhoun, Charles E. Perkins; Diameter Mobile IPv4 Application, Internet draft, Internet Engineering Task Force, February 2004.

[3] Protocol Carrying Authentication for Network Access WG (pana) http://www.ietf.org/html.charters/pana-charter.html.

[4] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin Protocol for Carrying Authentication for Network Access (PANA),Internet draft, Internet Engineering Task Force, February 9, 2004

[5] Stefano M. Faccin, Franck Le; AAA Local Security Association (LSA): The Temporary Shared Key (TSK), Internet draft, Internet Engineering Task Force, July 2001.

[6] Pat R. Calhoun, et al.; Diameter Base Protocol, RFC 3588, Internet Engineering Task Force, September 2003.

[7] B. Aboba et M. Beadles, The Network Access Identifier, RFC 2486, Internet Engineering Task Force, January 1999.

[8] Charles E. Perkins et al., AAA for IPv6 Network Access, Internet draft, Internet Engineering Task Force, July 2001

[9] W. Simpson, PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, Internet Engineering Task Force, August 1996

[10] J. Arkko et H. Haverinen, EAP AKA Authentication, Internet draft, Internet Engineering Task Force, 27 October, 2003

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

[12] Stefano M. Faccin, Franck Le; Diameter Mobile IPv6 Application, Internet draft, Internet Engineering Task Force, November 2001.

[13] Francis Dupont, Maryline Laurent-Maknavicius et Julien Bournelle; AAA for mobile IPv6; Internet draft, Internet Engineering Task Force, November 2001.

8. Authors' Addresses

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

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

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: Raj.Patil@nokia.com

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

Phone: +1 650-625-2986
E-Mail: charliep@iprg.nokia.com

Francis Dupont
ENST Bretagne
Campus de Rennes
2, rue de la Chataigneraie
BP 78
35512 Cesson-Sevigne Cedex
FRANCE
Fax: +33 2 99 12 70 30

EMail: Francis.Dupont@enst-bretagne.fr

Maryline Laurent-Maknavicius
INT Evry
9, rue Charles Fourier
91011 Evry Cedex
FRANCE
Fax: +33 1 60 76 47 11
EMail: Maryline.Maknavicius@int-evry.fr

Julien Bournelle
INT Evry
9, rue Charles Fourier
91011 Evry Cedex
FRANCE
Fax: +33 1 60 76 47 11
EMail: Julien.Bournelle@int-evry.fr