AAA Goals for Mobile IPv6
draft-ietf-mip6-aaa-ha-goals-03

Status of this Memo

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

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

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

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

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

This Internet-Draft will expire on March 16, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

In commercial deployments Mobile IPv6 can be a service offered by a Mobility Services Provider (MSP). In this case all protocol operations may need to be explicitly authorized and traced, requiring
the interaction between Mobile IPv6 and the AAA infrastructure. Integrating the AAA infrastructure offers also a solution component for Mobile IPv6 bootstrapping in integrated and split scenarios.

This document describes various scenarios where a AAA interface for Mobile IPv6 is actually required. Additionally, it lists design goals and requirements for such an interface.

Table of Contents

1. Introduction .................................................. 3
2. Terminology .................................................. 3
3. Motivation ..................................................... 3
4. Bootstrapping Scenarios ....................................... 4
  4.1. Split Scenario .............................................. 4
  4.2. Integrated Scenario ....................................... 5
5. Goals for the Split Scenario .................................. 6
  5.1. General goals .............................................. 6
  5.2. Service Authorization ..................................... 7
  5.3. Accounting ................................................ 7
  5.4. Mobile Node Authentication ............................... 8
  5.5. Provisioning of Configuration Parameters ............... 8
6. Goals for the Integrated Scenario ............................. 8
7. IANA Considerations ........................................... 8
8. Security Considerations ....................................... 9
9. Acknowledgements ............................................. 9
10. References ................................................... 9
  10.1. Normative References .................................... 9
  10.2. Informative References ................................... 9
Authors’ Addresses ................................................ 10
Intellectual Property and Copyright Statements .................. 12
1. Introduction

Mobile IPv6 [1] was originally designed as a protocol without any integration with the AAA infrastructure. Nonetheless, in some environments it might be desirable to authenticate the user based on existing credentials stored at the AAA server to authorize protocol operations, to enable accounting and credit control. Due to this requirement, Mobile IPv6 might require the interaction with the AAA infrastructure. Integrating the AAA infrastructure offers also a solution component for Mobile IPv6 bootstrapping [2] in split [3] and integrated [4] scenarios.

This document describes various scenarios where a AAA interface is required. Additionally, it lists design goals and requirements for such an interface.

This document only describes requirements, goals and scenarios. It does not provide solutions.

Notice that this document builds on the security model of the AAA infrastructure. As such, the end host/user shares credentials with the home AAA server and the communication between the AAA server and the AAA client may be protected. If the AAA server and the AAA client are not part of the same administrative domain, then some sort of contractual relationship between the involved administrative domains is typically in place in form of roaming agreements.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [5].

Some of the terms are also extracted from [2].

3. Motivation

Mobile IPv6 specification [1] requires that Mobile Nodes (MNs) are provisioned with a set of configuration parameters, namely the Home Address and the Home Agent Address, in order to accomplish a home registration. Moreover, MNs and Home Agents (HAs) must share the cryptographic material needed in order to setup IPsec security associations to protect Mobile IPv6 signaling (e.g. shared keys or certificates).

One approach is to statically provision the necessary configuration
parameters at MNs and HAs. This solution is sub-optimal from a deployment perspective, especially in large networks with a lot of users (e.g., a mobile operator network). For this reason the Mobile IPv6 bootstrapping problem was investigated and is described in [2]. Based on the analysed scenarios, two solutions were developed. The solution for the split scenario is described in [3] and the one for the integrated scenario can be found at [4]. A key point behind these scenarios is that, whenever static provisioning is not feasible, the AAA infrastructure of the MSP can be used as the central element to enable dynamic Mobile IPv6 bootstrapping. In this case the AAA infrastructure can be exploited to offload the end host’s authentication to the AAA server as well as to deliver the necessary configuration parameters to the HA.

Moreover, in case Mobile IPv6 is a service offered by a Mobility Service Provider (MSP), all protocol operations (e.g., home registrations) may need to be explicitly authorized and monitored (e.g., for accounting purposes). This can be accomplished relying on the AAA infrastructure of the MSP that stores user profiles and credentials.

In the split scenario, the deployment of this service model requires the availability of an interface between the Home Agent and the AAA infrastructure. The core capabilities that should be supported by this interface include Mobile IPv6 service authorization and maintenance (e.g. asynchronous service termination) as well as the exchange of accounting data. This basic set of features is needed in any Mobile IPv6 bootstrapping scenario. In the integrated scenario, the AAA server also delivers some Mobile IPv6 parameters to the NAS.

4. Bootstrapping Scenarios

This section describes some bootstrapping scenarios in which a communication between the AAA infrastructure of the Mobility Service Provider and the Home Agent is needed.

4.1. Split Scenario

In the split scenario [3], there is the assumption that the mobility service and network access service are not provided by the same administrative entity. This implies that the mobility service can be authorized by a different entity deploying its own AAA infrastructure. The entity offering the mobility service is called Mobility Service Provider (MSP) while the entity authorizing the service is the Mobility Service Authorizer (MSA).

In this scenario, the Mobile Node discovers the Home Agent Address
using the Domain Name Service (DNS). It queries the address based on
the Home Agent name or by service name. In the former case, the
Mobile Node is configured with the Fully Qualified Domain Name (FDQN)
of the Home Agent. In the latter case, [3] defines a new service
resource record (SRV RR).

Then the Mobile Node performs an IKEv2 [6] exchange with the HA to
setup IPsec SAs (to protect Mobile IPv6 signaling) and to configure
its Home Address (HoA). The IKEv2 Mobile Node to Home Agent
authentication can be done using either public key signatures or the
Extensible Authentication Protocol (EAP).

If EAP is used for authentication, the operator can choose any
available EAP methods. Note that even if EAP is used, the MN
authenticates the HA using public key based authentication. Based on
IKEv2, the HA may rely on a remote EAP server. In this case, a AAA
protocol such as RADIUS EAP [7]/Diameter EAP [8] must be used between
the HA and the home EAP server. This allows a pool of HAs to rely on
the same EAP server to authenticate Mobile Nodes. It also allows the
roaming mobility case in which the Mobile Node obtains the mobility
service in a different administrative domain (MSP != MSA).

The Mobile Node may also want to update its FQDN in the DNS with the
newly allocated Home Address. [3] recommends that the HA performs the
DNS entry update on behalf of the Mobile Node. For that purpose, the
Mobile Node indicates its FDQN in the IKEv2 exchange (IDii field in
IKE_AUTH) and adds a DNS Update Option in the Binding Update message
sent to the HA.

When the Mobile Node uses a Home Agent belonging to a different
administrative domain (MSP != MSA), the local HA may not share a
security association with the home DNS server. In this case, [3]
suggests that the home AAA server is responsible for the update.
Thus, the HA should send to the home AAA server the (FDQN, HoA) pair.
Note that the AAA exchange between the HA and the AAA server is
normally terminated before the HA receives the Binding Update
message. The reason is that the authentication has succeeded if the
Mobile Node is able to send the BU.

4.2. Integrated Scenario

In the integrated scenario [4], the assumption is that the user is
authenticated and authorized by the same authorizer than network
access service. The Mobility Service Authorizer (MSA) and the Access
Service Authorizer (ASA) are the same entity.

Two scenarios are possible. In the first case, the Home Agent is
allocated by the user’s home domain. In the second case it is
allocated by an entity in the visited domain. In both cases, it is assumed that the AAA server in the home domain (AAAH) authorizes both network access service and mobility service.

In this scenario, Mobile Node discovers the Home Agent Address using DHCPv6. During network access service authentication and authorization, AAAH also verifies if authenticating user is authorized to use mobility service. In affirmative case, the AAAH sends the information about the assigned home agent to the Network Access Server (NAS) where the Mobile Node is currently attached. Then, the NAS stores the received information. To request home agent data, the Mobile Node sends a DHCPv6 Information Request to the All_DHCP_Relay_Agents_and_Servers multicast address. With this request, the Mobile Node can specify if it wants a home agent provided by the visited domain (ASP/MSP) or by the home domain (ASA/MSA). In both cases, the NAS acts a DHCPv6 relay. When the NAS receives the DHCPv6 Information Request then it sends home agent information received from AAAH in a new DHC Relay Agent Option as defined in [9].

In case the Mobile Node cannot acquire home agent information via DHCPv6, it can try the default mechanism based on DNS described in [3]. After the Mobile Node has acquired the home agent information, the mechanism used to bootstrap the HoA, IPsec Security Association, and Authentication and Authorization with the MSA is the same described in the bootstrapping solution for split scenario [3].

5. Goals for the Split Scenario

Section 4 raises the need to define extensions for the AAA protocol used between the AAAH server and the HA. The following sections list a set of goals.

5.1. General goals

G1.1 The AAAH server and the HA MUST be able to authenticate each other (mutual authentication) in order to prevent the installation of unauthorized state on the HA. In some deployment scenarios, it may not be feasible for HA and AAAH to mutually authenticate each other. For example, let us consider the case where MSP is not the MSA. In such a case, several AAA intermediate proxies could forward MIP6 bootstrapping information back and forth between HA and AAA. Thus, to prevent the installation of unauthorized state on the HA, the path between HA and AAAH should be trustworthy.>
G1.2 The AAA-HA interface MUST provide integrity protection in order to prevent any alteration of exchanged data (e.g., Mobile IPv6 configuration parameters).

G1.3 The AAA-HA interface MUST provide replay protection.

G1.4 The AAA-HA interface SHOULD provide confidentiality since it may be used to transfer keying material (e.g., shared key generated during EAP method authentication).

G1.5 The AAA-HA interface SHOULD support inactive peer detection. This functionality can be used by the AAAH server to maintain a list of active HAs.

5.2. Service Authorization

G2.1 The AAA-HA interface SHOULD allow the use of Network Access Identifier (NAI) to identify the user.

G2.2 The HA SHOULD be able to query the AAAH server to verify Mobile IPv6 service authorization for the mobile node.

G2.3 The AAAH server MAY assign explicit operational limitations and authorization restrictions on the HA (e.g., packet filters, QoS parameters).

G2.4 The AAAH server MUST be able to send an authorization lifetime to the HA to limit Mobile IPv6 session duration for the MN.

G2.5 The HA MUST be able to request to the AAAH server an extension of the authorization lifetime granted to the MN.

G2.6 The AAAH server MUST be able to force the HA to terminate an active Mobile IPv6 session for authorization policy reasons (e.g., credit exhaustion).

5.3. Accounting

G3.1 The AAA-HA interface MUST support the transfer of accounting records needed for service control and charging. These include (but may not be limited to): time of binding cache entry creation and deletion, octets sent and received by the mobile node in bi-directional tunneling, etc.
5.4. Mobile Node Authentication

G4.1 The AAA-HA interface MUST support pass-through EAP authentication with the HA working as EAP authenticator operating in pass-through mode and the AAAH server working as back-end authentication server.

5.5. Provisioning of Configuration Parameters

G5.1 The HA SHOULD be able to communicate to the AAAH server the Home Address allocated to the MN (e.g., for allowing the AAAH server to perform a DNS update on behalf of the MN).

G5.2 The AAAH SHOULD be able to indicate to the HA if the MN is authorized to autoconfigure its Home Address.

6. Goals for the Integrated Scenario

In the integrated scenario, the AAA server provides the HA information to the NAS as part of the whole AAA operations for network access. Next goals are considered in addition to those described in section Section 5.

G6.1 The AAAH server MUST be able to communicate the Home Agent Information (IP Address or FQDN) to the NAS.

G6.2 The NAS SHOULD be able to notify that it supports the functionalities described in [4].

G6.3 The ASP/MSP SHOULD be able to indicate to the MSA if it can allocate a Home Agent to the MN.

G6.4 The AAA server of the MSA MUST be able to indicate to the NAS whether the MN is authorized to use a local Home Agent (i.e. a Home Agent in the ASP/MSP)

7. IANA Considerations

This document does not require actions by IANA.
8. Security Considerations

As stated in Section 5.1 the AAA-HA interface must provide mutual authentication, integrity and replay protection. Furthermore, if security parameters (e.g., IKE pre-shared key) are transferred through this interface, confidentiality is strongly recommended to be supported. However note that AAA protocols does not support this unless it exists a direct connection between corresponding entities.

9. Acknowledgements

The authors would like to thank James Kempf, Alper Yegin, Vijay Devarapalli, Basavaraj Patil, Gopal Dommety and Madjid Nakhjiri for their comments and feedback. Moreover the authors would like to thank Hannes Tschofenig for his deep technical and editorial review of the draft.

10. References

10.1. Normative References


10.2. Informative References


Authors’ Addresses

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Email: gerardo.giarettat@telecomitalia.it

Ivano Guardini
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Email: ivano.guardini@telecomitalia.it

Elena Demaria
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Email: elena.demaria@telecomitalia.it
Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: julien.bournelle@int-evry.fr

Rafa Marin Lopez
University of Murcia
30071 Murcia
Spain

Email: rafa@dif.um.es