Scalable Authentication Framework for Mobile-IP (SAFe-MIP)

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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.

For potential updates to the above required-text see: http://www.ietf.org/ietf/1id-guidelines.txt

Abstract

To date, a number of authentication protocols have been proposed for Mobile-IP. Among these incompatible protocols, it is not clear until now which one will be the preferred one for global deployment of Mobile-IP. Based on the policy of allowing various protocols to co-exist, this draft specifies an authentication framework that allows Mobile-IP entities to negotiate for a protocol to be employed. The framework also outlines the utilization of message extension for carrying all information required by the authentication protocol being used.

Based on the proposed framework, this draft then proposes a "Minimal Public Key Based Authentication" which addresses the need for scalable but lightweight authentication protocol. The proposed protocol secures the registration process, and requires a number of message rounds that is fully compatible with the base Mobile-IP.
1. Introduction

Mobile-IP [1, 2] is widely expected to be deployed in large scale in the near future. In order for Mobile-IP to be successfully deployed commercially, further enhancements to existing protocol are required. Among the key issues, security is an area that needs to be addressed satisfactorily. In addition, security measures must be scalable in that support for roaming over different domains in the global Internet is a basic requirement of Mobile-IP.

To date, a number of authentication protocols for Mobile-IP have been proposed [1, 3, 4, 5]. Among these incompatible protocols,
it is not clear until now which one will be the preferred one for global deployment of Mobile-IP. As we believe that "one size doesn’t fit all", we advocate the policy of allowing various protocols to co-exist. Based on the policy, this draft specifies an authentication framework that allows Mobile-IP entities to negotiate for a protocol to be employed. The framework also outlines the utilization of message extension for carrying all information required by the authentication protocol being used. This technique is intended to save the limited numbering space of Extension Type in Mobile-IP control message.

Based on the proposed framework, this draft then proposes a "Minimal Public Key Based Authentication" which addresses the need for scalable but lightweight authentication protocol. The proposed protocol secures the registration process, and requires a number of message rounds that is fully compatible with the base Mobile-IP. In achieving these goals, the protocol takes advantage of some properties of Mobile-IP, especially the trust relationships among Mobile-IP entities.

The protocol specification also takes into consideration the involvement of Authentication-Authorization-Accounting (AAA) servers, either in the foreign domain (called AAAP) or in the home domain (called AAAH). This consideration is in line with recent consensus within the Mobile-IP community to bring AAA entities into the picture. By doing so, we manage to clearly separate tasks for providing connectivity from those related to AAA, which brings more flexibility at deployment stage.

2. Conventions Used in This Document

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

3. New Authentication Framework for Mobile-IP

3.1 Support for Multiple Authentication Protocols

Allowing Mobile-IP entities to negotiate for an authentication protocol to be employed brings more flexibility in securing Mobile-IP. Such flexibility is favorable for various reasons such as:

- Different types of MNs ranging from powerful notebook to low-cost PDA can choose a protocol that best suits its computing power capability.
Different sites, with their different technical and organizational constraints, can have a set of available options to choose from for securing its Mobile-IP operation.

To allow a protocol negotiation to be conducted, some new message extensions are defined. In particular, one message extension is specified to carry the identifier of selected protocol. From this identifier, all participants can know for sure which protocol is currently being used. This is in contrast to some practice, in which authentication actions to be performed are just implicitly determined from the existence of certain message extensions.

Section 3.1.1 outlines the overview of this protocol negotiation, while new message extensions are defined in Section 3.1.2.

3.1.1 Negotiation Overview

Some new considerations on the registration process with regard to this negotiation are as follows:

(For conformance with specification of the base Mobile-IP [1], the specification below assumes only the existence of standard Mobile-IP entities, i.e.: MN, FA, and HA.)

- **FA Agent Advertisement:**
  Foreign Agent (FA), as the visited entity, includes "FA Authentication-Protocol-List" (FA-APL) Extension in its Agent Advertisement message. This extension (see Section 3.1.2.1) contains a list of authentication protocols supported by FA, in the order of FA’s preference (favorite choice first).

- **MN Registration Request:**
  MN, as the entity that’s typically most limited in terms of computing power, selects one protocol from the list. It SHOULD select one that is supported by its HA and favorable for itself. In its Request message, MN includes the identifier of selected protocol in an extension called "MN Authentication-Protocol-Identifier" (MN-API). See Section 3.1.2.2 for its message format.

- **FA Registration Request Processing:**
  In processing MN’s Request, FA MUST additionally ensure that the following conditions are satisfied:

  - **MN-API Extension MUST be present in the Request. Otherwise, FA MUST reject that Request with code: "Denied by Foreign Agent, MN-API Extension is required".**

  - The protocol identifier in MN-API Extension MUST be selected from the list in FA-APL. Otherwise, FA MUST reject that Request with code: "Denied by Foreign Agent, the selected protocol identifier is not from FA-APL Extension".
- HA Registration Request Processing:
  HA MUST check that the selected protocol is supported and authorized for use with MN and FA. If the selected protocol is not approved for use, HA MUST send a rejected Reply (code: "Denied by Home Agent, the selected protocol identifier is not approved for use"). In this case, HA then MUST include "HA Authentication-Protocol-List" Extension for MN to select in its next registration attempt. This extension (see Section 3.1.2.3) is included in Reply following the fixed message portion of the Registration Reply.

3.1.2 Message Format

3.1.2.1 FA Authentication-Protocol-List Extension

This extension, which is shown in Figure-1, is defined as a new extension of ICMP Router Advertisement. We suggest that its presence is made mandatory for Mobile-IP operation. Hence, it MUST appear in the ICMP Router Advertisement after Mobility Agent Advertisement Extension, but before Prefix-Lengths Extension and One-byte Padding Extension (if present).

```
+---------------------------------+-------------------+-------------------+
<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Auth. Protocol Identifier #1</th>
</tr>
</thead>
</table>
|         |          | additional Authentication Protocol Identifier(s)...
```

Figure-1. FA Authentication-Protocol-List (FA-APL) Extension

<table>
<thead>
<tr>
<th>Type</th>
<th>TBD (FA-APL Extension).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>(2*N), where N is the number of listed Authentication Protocol Identifiers(s).</td>
</tr>
<tr>
<td>Auth. Protocol-Identifier(s)</td>
<td>One or more identifiers of the protocols supported by FA. The number of identifiers present is determined from the Length field. Values for Authentication Protocol Identifier from 0-1000 are reserved, with the suggested initial list as follows: 1: Secret key based RFC-2002 style [1]. 2: Public Key based Authentication [3]. 3: Minimal Public Key based Authentication (See Section 4). 4: IKE based Authentication [4, 5].</td>
</tr>
</tbody>
</table>
3.1.2.2 MN Authentication-Protocol-Identifier Extension

This MN-API Extension is defined to be included in Registration Request. It MUST appear after the fixed message portion of Registration Request, but before the Mobile-Home Authentication Extension. If MN Network-Access-Identifier (MN-NAI) Extension [8] is present, this MN-API Extension SHOULD immediately follow MN-NAI. The format of MN-API is shown in Figure-2 below.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |Auth. Protocol Identifier (API) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure-2. MN Authentication-Protocol-Identifier (MN-API) Extension

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>API</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>2</td>
<td>16-bit identifier of selected authentication protocol. This value MUST be selected from the list in FA-APL Extension, or otherwise it will result in a rejected Reply from FA.</td>
</tr>
</tbody>
</table>

3.1.2.3 HA Authentication-Protocol-List Extension

This new extension, which is shown in Figure-3, is defined to be included in Registration Reply. HA MUST include this extension in its Reply, should it reject a Request with code: "Denied by Home Agent, selected protocol identifier is not approved for use". This extension MUST appear after the fixed message portion of Registration Reply, but before the Mobile-Home Authentication Extension.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  Auth. Protocol Identifier #1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       additional Authentication Protocol Identifier(s)... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure-3. HA Authentication-Protocol-List (HA-APL) Extension

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>(2*N), where N is the number of listed Authentication Protocol Identifiers(s).</td>
</tr>
</tbody>
</table>
3.2 General Extension for Authentication-Related Information

RFC-2002 [1] has outlined a general Extension mechanism that allows any new optional information to be defined in a format of "Type-Length-Value". However, the allocation of values for this Extension Type is not always easy due to its limited numbering space (8 bits). On the other hand, various new extensions are proposed in a number of recent drafts for many enhancements to Mobile-IP.

In order to save numbering space of this Extension Type and to simplify its allocation, this draft specifies the use of message extension for carrying all information related to the authentication protocol being used. A set of new extensions called "Authentication Information Message (AIM)" is defined, which are:
- Mobile-Home AIM Extension.
- Mobile-Foreign AIM Extension.
- Foreign-Home AIM Extension.

(In the presence of AAA servers, the "Home" and "Foreign" of the AIM Extensions above are taken to be AAAF and AAAH, respectively. This is because AAAH and AAAF are the entities responsible for all the AAA-related tasks in the home and foreign domain, respectively.)

The message format of an AIM Extension is shown in Figure-4.

```
   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +--------------------------------------------------+
   |     Type      |    Length     |  Authentication Object(s)... |
   +--------------------------------------------------+
```

Figure-4. Message format of an AIM Extension

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Authentication Objects(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>The number of bytes of all Authentication Object(s) included.</td>
<td></td>
</tr>
<tr>
<td>One or more authentication-related information item(s) intended to be delivered to the destined party. Each information item is encoded in T-L-V format. (See more explanation below).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Authentication Object in this framework is similar to one particular authentication-related extension in RFC-2002 specification. However, all the objects from one sender to the same destination are now encapsulated under one AIM Extension of that sender-destination. Moreover, an Authentication Object (AO) is defined and interpreted locally to each authentication protocol. In other words, it is the combination of field "Authentication-Protocol-Identifier" in MN-API Extension and field "AO-Type" that uniquely determines the format and semantic of an Authentication Object.

General format of an Authentication Object is shown in Figure-5.

```
0                   1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    AO-Type    |   AO-Length   |       AO-Data ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure-5. General format of an Authentication Object (AO)

| AO-Type        | Indicates the particular type of AO. |
| AO-Length      | Indicates the length (in bytes) of AO-Data. |
| AO-Data        | The particular data associated with this AO. |

One type of AO is particularly called "Authenticator-AO", since it carries the authenticator value of a message, which is either a secret-key based MAC value or a public-key based digital signature. The location of this Authenticator-AO in a message marks the end of the authenticated data. All Authentication Objects that appear before this Authenticator-AO MUST also be included in the calculation of authenticator value.

Another potential use of AO is that of type "Protocol Result Code", which is intended to carry specific result code related to the execution of authentication protocol being used. Using this technique, there’s no need to allocate and assign various values in Code field of Registration Reply for various authentication-related error reporting.

The "Minimal Public Key Based Authentication" proposed in Section 4 can serve as an example on the use of these AIM Extensions.
4. Minimal Public Key Based Authentication

4.1 A Lightweight Public Key Based Protocol

Currently, Mobile-IP protocol [1] still relies its authentication on the use of shared key cryptography with manual key distribution. However, it’s known that this approach leads to scalability problem in the key management.

On the other hand, a public key based authentication [3] has been proposed in order to provide a truly scalable authentication scheme. Although this scheme seems ideal in that no pre-established secret key association is required, however, high computation overheads involved may be of great concern to some MNs. Under this scheme, a MN is expected to satisfactorily perform computationally expensive public-key cryptography operations, including the need for obtaining recent Certificate Revocation List (CRL).

In between these two approaches, there exists another possible one which is based on the following assumptions:
- No security association between MN and AAAF is assumed to exist.
- However, it’s still assumed that MN and AAAH share a secret-key based security association.

Based on the authentication scenario above, a scalable yet lightweight public-key based authentication protocol is proposed in this draft. The proposed protocol ensures its scalability through the use of public key cryptography in its inter-domain authentication. However, the case of shared-key based association for MN and AAAH is considered here, due to its practicality and the fact that MN and AAAH are normally under the same organization.

A similar scenario is also considered in some recent drafts [4, 5]. While these drafts also suggest the use of public key based authentication between AAAH and AAAF, the operation is just to rely on mechanisms provided by other infrastructure, namely IPSEC [6] and IKE [7]. However, some concerns exist over this approach:
- Extra message exchange sessions that are employed in addition to those of Mobile-IP may result in poor MN’s handoffs.
- Due to the protocol dependency, organizations deploying Mobile-IP must first deploy IPSEC and IKE. This requirement can’t always be assumed to be easy, since various non-technical issues such as those related to cost and availability, may exist as constraints.

In contrast, being intended as a practical yet secure alternative solution, the proposed protocol aims to make use of the existing Mobile-IP control messages. As a result, message-round compatibility with the base Mobile-IP is fully preserved, which is vital in facilitating fast MN’s handoffs.
4.2 Goals and Design Principles

The protocol aims to provide the following security services to Mobile-IP registration:

- Mutual authentication among all the entities involved.
- Integrity of the registration messages.
- Assurance that the registration is fresh (anti-replay protection).

In achieving the goals above, some other design principles are set:

- No challenge-response is to be performed directly between FA and MN as in [9]. However, the freshness assurance of a registration must be ensured. In particular, a possible replay attack on AAAF which is also described in [10], must be prevented.
- Although the protocol takes AAA entities in its message flow, it must equally work should only Mobile-IP standard entities be involved.
- The protocol should assume the existence of only generic AAA entities. Hence, any AAA mechanisms such as RADIUS [11] or DIAMETER [12] can be employed. It is also assumed that the communication links between AAA servers and its FA or HA are already secured by the AAA protocol being use.

4.3 The Protocol

This section outlines the Minimal Public Key Based Authentication (Min-PKA) protocol. Only the case of MN’s registration performed via FA is considered in this draft. Throughout the protocol specification below, AAAF and AAAH are always assumed to be present. However, some additional considerations are also mentioned later, should no AAA servers be involved.

Some new considerations on the registration process with regard to Min-PKA protocol are as follows.

Agent Discovery:

In its ICMP Router Advertisement message, FA includes these following extensions after the Mobility Agent Advertisement Extension:

a) FA-APL Extension, which MUST contain an entry for Min-PKA protocol (Authentication-Protocol-Identifier = 3).

b) AAAF-Identity Extension (defined in Section 4.4.1.1), that’s used to inform the presence of AAAF in the foreign domain. This extension carries the following information of AAAF: AAA-Type, IP address, and NAI. The ”AAA-Type” field is particularly used to indicate the type of AAA protocol supported in AAAF. See Section 4.4.1 for further explanation.
MN Registration Request Generation:

- MN SHOULD include MN-NAI Extension following the fixed message portion of Registration Request.
- MN MUST include MN-API Extension with API field set to "3" for Min-PKA protocol.
- If AAAH is present in the home domain to process this Request, MN MUST include AAAH-Identity Extension (defined in Section 4.4.1.2).
- MN then appends Mobile-Home AIM Extension at the end of the Request message. This Extension contains the following AOs:
  a) Encapsulated Foreign Agent Advertisement (EFAA), which is an exact copy of previously received FA Advertisement. By including this Authentication Object, MN implicitly forwards AAAF’s information to AAAH. This information is necessary in order for AAAH to know whom it should perform the inter-domain authentication with. For the format of this authentication object, see Section 4.4.2.1.
  b) Mobile-Home Authentication (defined in Section 4.4.2.2), that carries MAC value generated using the shared key between MN and AAAH.

Registration Request Processing by FA:

From MN-API Extension, FA knows that MN selects Min-PKA protocol to be followed. It then proceeds as follows:

- No authentication steps are required to be done by FA. However, it needs to ensure that the Encapsulated FA-Advertisement (EFAA) is valid as recently advertised. Should FA find it invalid or outdated, FA MUST silently discard MN’s Request and cease further processing.
- Upon successful validation of EFAA, FA relays MN’s Request to AAAF according to the AAA protocol being use in the foreign domain. It’s assumed that this link is already secured by mechanisms in that AAA protocol.

Registration Request Processing by AAAF:

Knowing that the Min-PKA protocol is the authentication to be followed, AAAF processes the Request by appending Foreign-Home AIM Extension. The following Authentication Objects must be included in the extension:
a) Foreign-Nonce (defined in Section 4.4.3.1) that contains a nonce to be echoed later by AAAH in its Reply. The inclusion of this nonce is necessary, as explained in Section 4.5.

b) Certificate (see Section 4.4.3.2), in which AAAF puts a copy of its certificate and any other certificates that are necessary for trust hierarchy creation with AAAH.

c) Foreign PK-Authentication (see Section 4.4.3.3), in which AAAF places its digital signature spanning all the Request message fields.

AAAF then relays this Request message to the AAAH specified in AAAH-Identity Extension. In doing so, AAAF needs to take into consideration the value of AAA-Type in AAAH-Identity Extension. Based on this value, AAAF MUST correctly construct the registration message in the suitable format, and address this message to the right transport-layer’s port of AAAH.

Registration Request Verification by AAAH:

From MN-API Extension, AAAH knows that MN selects Min-PKA protocol to be followed. It then performs these following steps:

- Using its secret-key shared with MN, AAAH validates MAC value placed in the Mobile-Home Authentication AO.

- AAAH validates the value in Identifier field, which is either a nonce or a timestamp, to ensure the freshness of MN’s Request as specified in [1].

- From the presence of AAAF-Identity Extension inside the Encapsulated-Foreign-Agent-Advertisement, AAAH is aware of the involvement of AAAF in the foreign domain. First, AAAH must ensure that the relayed Request really comes from this AAAF.

- Next, AAAH extracts AAAF’s certificate from the Certificate AO and then verifies the validity of this certificate. AAAH MUST also ensure that the identity of AAAF in this certificate is the same as that in AAAF-Identity Extension.

- Following that, AAAH verifies AAAF’s digital signature which is placed in the Foreign PK-Authentication AO.

- AAAH then relays the necessary Request information to HA in order to update MN’s mobility binding.
AAA Generation of Registration Reply:

In generating Reply message, AAAH forms the following message extensions to be appended after the fixed message portion of Registration Reply:

- MN-NAI Extension, which is copied from the same extension included in the Request (if present).

- Mobile-Home AIM Extension, which contains Mobile-Home Authentication AO. This authentication object carries MAC value generated using the shared key between AAAH and MN.

- AAAF-Identity Extension, which is copied from the same extension included in Request (if present).

- Foreign-Home AIM Extension, which contains the following AOs:
  a) Foreign-Nonce, which is copied from AAAF’s Foreign-Nonce included in the relayed Request.
  b) Certificate, in which AAAH puts a copy of its certificate and any other certificates necessary for trust hierarchy creation with AAAF.
  c) Home PK-Authentication (defined in Section 4.4.3.4), in which AAAH places its digital signature spanning all the Reply message fields.

Registration Reply Authentication Processing by AAAF:

- AAAF extracts the AAAF-Identity Extension and ensures that AAAF itself is the intended recipient.

- AAAF then extracts the Foreign-Home AIM Extension and proceeds as follows:
  - It verifies that AAAH echoes a correct nonce value in the Foreign-Nonce AO.
  - It extracts AAAH’s certificate from Certificate AO and then verifies the validity of this certificate.
  - Upon successful validation of the Certificate, AAAF then extracts AAAH’s digital signature that’s placed in Home PK-Authentication AO. Using AAAH’s authenticated public key, AAAF verifies the validity of this signature.
  - After deleting AAAF-Identity Extension (if present) and Foreign-Home AIM Extension, AAAF relays the Reply message to FA through its secure link.
FA Receipt of Registration Reply:

After performing steps related to visitor list processing [1], FA then relays the Reply message to MN.

MN Receipt of Registration Reply:

Upon receipt of the Reply message, MN performs the following authentication actions:

- Using its secret-key shared with AAAH, MN validates MAC value inside the Mobile-Home Authentication AO.
- As specified in [1], MN MUST also ensure the validity of Identification field.

Although the presence of AAAH and AAAF is always assumed throughout the specification above, the protocol still can work in the absence of AAAH, AAAF, or both.

By having no AAAF-Identity Extension included in its Advertisement, FA indicates that no AAAF is to be involved in the foreign domain. In this case, some new considerations with regard to the specification above are:

- Registration Request Processing by FA:
  Inside the Foreign-Home AIM Extension, FA places:
  - its own certificate in the Certificate AO, and
  - its own digital signature in the Foreign PK-Authentication AO.

- Registration Request Processing by AAAH or HA:
  AAAH or HA learns of (authenticated) FA’s IP address from "Care-of Address" field in the fixed message portion of Registration Request.

Similarly, should no AAAH be involved, HA becomes the entity that is responsible for all the authentication steps in the home domain. In this case, FA or AAAF MUST form the Request message in the standard Mobile-IP format and relay it to UDP port number 434 (reserved for Mobile-IP control message). Finally, when preparing a Reply, HA places the following information in the Foreign-Home AIM Extension:

- its own certificate in the Certificate AO, and
- its own digital signature in the Home PK-Authentication AO.
4.4 Message Format

4.4.1 Extensions for AAA Identity

This family of extensions is used to inform the presence of AAA entities. Based on the general format shown in Figure-6, three extensions are defined in the next following sub-sections.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |           AAA Type            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AAA IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            AAA NAI...                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure-6. General message format of AAA Identity Extension

- **Type** (See Section 4.4.1.1 - 4.4.1.3).
- **Length** 6 plus the number of bytes in AAA NAI.
- **AAA Type** The 16-bit identifier indicating the type of AAA protocol supported. Valid values for use within this field are TBD.
- **AAA IP-Address** IP address of AAA entity.
- **AAA NAI** NAI of AAA entity. The actual length of this field is determined from the Length field.

4.4.1.1 AAAF-Identity Extension (on Router Advertisement)

This extension MAY be included in Agent Advertisement in order for FA to inform the presence of AAAF. Its message format follows the definition in Figure-6, with a new Extension Type assigned (TBD).

4.4.1.2 AAAH-Identity Extension (on Registration)

In the presence of AAAH in the home domain, MN is to include this extension in its Request message. The extension MUST appear before the Mobile-Home AIM Extension. Its format is exactly the same as that shown in Figure-6, with a new Extension Type assigned (TBD).
4.4.1.3 AAAF-Identity Extension (on Registration)

If AAAF is present in the foreign domain, this extension MUST be included by AAAH in its Reply message. Another new Extension Type is to be assigned for this extension (TBD).

4.4.2 Authentication Objects under Mobile-Home AIM Extension

4.4.2.1 Encapsulated Foreign Agent Advertisement (EFAA)

This Authentication Object is defined to carry an exact copy of previously received FA Advertisement message. Only message part starting from the Mobility Agent Advertisement Extension is taken into account. The message format is shown in Figure-7 below.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    AO-Type    |   AO-Length   |  Received FA-Advertisement...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure-7. Encapsulated FA Advertisement
```

- **AO-Type**: 10 (Encapsulated FA-Advertisement).
- **AO-Length**: The number of bytes in Received FA-Advertisement.
- **Received FA-Advertisement**: Copied from previously received FA Advertisement message, starting from its Mobility Agent Advertisement Extension until the end of the message.

4.4.2.2 Mobile-Home Authentication

This Authentication Object, which is shown in Figure-8, is intended to carry authenticator (MAC value) generated using the shared key between MN and AAAH.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    AO-Type    |   AO-Length   |             SPI...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... SPI (cont.)         |        Authenticator...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure-8. Mobile-Home Authentication
```
AO-Type           11 (MH-Authentication).
AO-Length         4 plus the number of bytes in the Authenticator.
SPI               Security Parameter Index (4 bytes).
Authenticator     Variable length that contains the MAC value of the message.

4.4.3 Authentication Objects under Foreign-Home AIM Extension

4.4.3.1 Foreign-Nonce

This Authentication Object contains a random number generated by AAAF which is sent to AAAH as a challenge. Its message format is shown in Figure-9. The inclusion of this challenge is necessary in order to prevent a possible replay attack as described in [10].

| AO-Type | AO-Length | Nonce...
|---------|-----------|----------
| 20      | 4         |          |

Figure-9. Foreign-Nonce

AO-Type           20 (Foreign-Nonce).
AO-Length         4.
Nonce             32-bit random number from AAAF as a challenge to be echoed by AAAH in Reply.

4.4.3.2 Certificate

This Certificate AO is used to convey the Certificate of AAAF or AAAH. As for its format, we can reuse the same definition outlined in Section 2.4.4 of [3], with AO-Type = 1 assigned in this draft.

4.4.3.3 Foreign Public Key Authentication

This Authentication Object is intended to carry AAAF’s digital signature in the relayed Request message. It MUST appear as the last
authentication object in the Foreign-Home AIM Extension. The message format for this AO can be based on the same definition given in [3], which is also shown in Figure-10 below.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   AO-Type     |   AO-Length   |          Auth. Type           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Foreign Digital Signature...                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure-10. Foreign Public Key Authentication

- **AO-Type**: 21 (Foreign PK-Authentication).
- **AO-Length**: 2 plus the number of bytes in the Foreign Digital Signature.
- **Authentication Type**: 2 bytes as identifier of the public key cryptographic method (algorithm) and key length used to generate digital signature.
- **Foreign Digital Signature**: The Digital Signature spanning all the previous message part that’s generated using the private key of AAAF.

### 4.4.3.4 Home Public Key Authentication

This Authentication Object is intended to carry digital signature of AAAH in the Reply message. Exactly one Home PK-Authentication AO MUST appear in the end of the Foreign-Home AIM Extension.

Its message format is similar to that defined in Section 4.4.3.3, however the following modifications are required:

- **AO-Type** = 22 (Home PK-Authentication).
- Field "Home Digital Signature" is named instead of "Foreign Digital Signature".

### 4.5 Security Analysis

This section gives an informal analysis on the security of the proposed protocol. Each security goal mentioned in Section 4.2 is discussed below.
- Authentication Service:

Based on the trust relationships in Mobile-IP, the protocol assumes that AAAH’s approval is sufficient to assure AAAF that the registration comes from the legitimate MN. Likewise, MN also relies on this AAAH’s approval for assurance that AAAF is indeed genuine and that the visited network would provide qualified services. These two assumptions are central in the proposed protocol, as they provide the basis for implicit authentication between MN and AAAF.

The assurance that AAAH itself is genuine is achieved through AAAH’s ability to produce a valid digital signature of the Reply. In turn, AAAH can be sure that the Request is issued by the legitimate MN from the presence of a valid MAC value in the Request message.

On the other hand, AAAH can authenticate AAAF by checking the validity of AAAF’s digital signature in the relayed Request. Lastly, MN can be convinced that the Reply really comes from AAAH because of the presence of a valid MAC value in the Reply.

- Integrity Service:

The inclusion of authenticator values in the registration messages also guarantees the integrity of those messages.

However, there exists a potential problem during the Agent Discovery phase. Despite the absence of any security associations between MN and entities in the foreign domain, MN needs to ensure the integrity and authenticity of the received FA Advertisement. In order to satisfy this requirement, the proposed protocol mandates the inclusion of Encapsulated FA-Advertisement (EFAA) Extension in MN’s Request. Accordingly, FA processes a Request only if EFAA Extension contains a valid recent FA Advertisement. This measure, together with the use of MAC value protecting the integrity of the Request, guarantees that an approval from AAAH would only be possible provided MN indeed receives an unaltered FA Advertisement.

- Anti-Replay Service:

In achieving the freshness assurance of a registration, the proposed protocol relies on the existing anti-replay protection as specified in [1].

Additionally, the protocol also mandates the use of AAAF’s nonce that must be echoed by AAAH in the Reply. AAAF only takes a Reply as a valid one, provided AAAH includes a correct nonce value in its authenticated Reply. The inclusion of this nonce is necessary in order to prevent a possible replay attack, in which a malicious attacker fools AAAF by replaying a Request followed by the
corresponding approved Reply. A more detailed discussion on this issue can also be found in [10].

Furthermore, the inclusion of this nonce is also a prudent practice as to prevent a possible chosen-plaintext attack on AAAF. In such attack, an adversary could freely choose bogus messages to get signed by AAAF, in its attempt to yield more information about AAAF’s private key. By including a nonce in the message part to be signed, the proposed protocol reduces this possible chosen-text attack into a less serious known-plaintext attack possibility.

5. Other Considerations

In addition to ensuring the authenticity, integrity, and freshness of a registration, the protocol may also be extended to perform key establishment. Shared keys for MN-AAAF and AAAF-AAAH can be generated for use in subsequent registrations. A shared key between MN and FA can also be generated to secure data traffic over the wireless link.

Finally, the use of public key authentication also opens a possibility of inter-domain service establishment with no prior direct agreement between the two domains. This may be possible through the involvement of a trusted entity within the Mobile-IP community. One domain can then trust an entity from different domain, as long as that domain is certified by this trusted entity through a valid certification chain. For this purpose, the following format of a Certificate is suggested:

Certificate ::= <certificate-chain within the local domain>,
              <certificate of the Trusted Financial Entity>,
              [certificate-chain to the Root-CA].

6. Summary

This draft presents a comprehensive authentication framework for Mobile-IP. Some new ideas are incorporated into the framework to provide an alternative solution to Mobile-IP authentication that is scalable, practical, and secure.

As it is predicted that the demand for Internet mobile access will increase dramatically in the near future, we hope that this proposed framework can help facilitate a faster secure Mobile-IP global deployment.

7. Security Considerations

This whole draft deals with security protections for Mobile-IP.
8. References


9. Acknowledgments

The authors are grateful to Dr. Winston Seah (Centre for Wireless Communications, National University of Singapore) for valuable discussions and his encouragement to investigate this topic.
10. Author’s Addresses

Sufatrio, Kwok-Yan Lam  
Centre for Systems Security Research  
School of Computing  
National University of Singapore  
Lower Kent Ridge Road  
Singapore 119260  
Email: {sufatrio, lamky}@comp.nus.edu.sg