Mobile IP Working Group
INTERNET DRAFT
**15 June 1999**

Charles E. Perkins
Sun Microsystems Laboratories
Pat R. Calhoun
Sun Microsystems Laboratories

# AAA Registration Keys for Mobile IP

draft-ietf-mobileip-aaa-key-00.txt

## Status of This Memo



## Abstract

AAA servers, such as RADIUS and DIAMETER, are in use within the Internet today to provide authentication and authorization services for dial-up computers. Mobile IP requires strong authentication between the mobile node and its home agent. When the mobile node shares a security association with its home AAA server, however, it is possible to use that security association to create derivative security associations between the mobile node and its home agent, and again between the mobile node and the foreign agent currently offering a care-of address to the mobile node. This document specifies extensions to the Mobile IP Registration Reply packet that can be used to distribute such security information to the mobile node.

## 1. Introduction

AAA servers, such as RADIUS [8] and DIAMETER [2], are in use within the Internet today to provide authentication and authorization services for dial-up computers. Such services are likely to be equally valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. Mobile IP [7] requires strong authentication between the mobile node and its home agent. When the mobile node shares a security association with its home AAA server, however, it is possible to use that security association to create derivative security associations between the mobile node and its home agent, and again between the mobile node and the foreign agent currently offering a care-of address to the mobile node. This document specifies extensions to the Mobile IP Registration Reply packet that can be used to distribute such security information to the mobile node.

AAA servers typically use the Network Access Identifier (NAI) [1] to uniquely identify the mobile node; the mobile node's home address is not always necessary to provide that function. Thus, it is possible for a mobile node to authenticate itself, and be authorized for connection to the foreign domain, without even having a home address. However, for Mobile IP to work, the mobile node is required to have a security association with its home agent. When the Mobile IP Registration Reply packet is authenticated by the MN-AAA Authentication Extension [?], the mobile node can verify that the keys contained in the extensions were produced by the AAA server, and thus may be reliably used to create security associations with the home agent, or alternatively with the foreign agent.

The following operations are envisioned between the mobile node, AAA server, home agent, and foreign agent.

1. When a mobile node travels away from home, it may not have a security association with its home agent, perhaps because it does not yet have a home address.

2. When the mobile node first registers away from home, it includes a MN-AAA Authentication extension if it does not yet have a Mobility Security Association with a home agent.

3. At the time the information within the MN-AAA Authentication extension is verified by the AAA server, the AAA server also generates keys for the mobile node, encodes the keys according to its own security association with the mobile node, and causes insertion of the new key or keys along with the Registration Reply.

4. When the mobile node receives the Registration Reply message, it verifies the authenticity (and integrity) of the reply message by using information provided in the MN-AAA Authentication extension.

5. If the Reply passes authentication and contains the MN-HA Key extension (see section 4), the mobile node decodes the key according to its security association with the AAA. The resulting key is used to establish the mobile node's security association with its home agent.

6. Similarly, if the Reply passes authentication and contains the MN-FA Key extension (see section 5), the mobile node decodes the key according to its security association with the AAA. The resulting key is used to establish the mobile node's security association with its new foreign agent.

Any message containing the MN-HA Key extension or the MN-FA Key extension MUST also contain a subsequent MN-AAA Authentication Extension. If a Registration Reply message contains both a MN-HA Key extension and a Mobile-Home Authentication extension, the former extension MUST come first. Likewise, if a Registration Reply message contains both a MN-FA Key extension and a Mobile-Foreign Authentication extension, the former extension MUST come first.

## 2. Security Algorithms

Mobility Security Associations between Mobile IP entities (mobile nodes, home agents, foreign agents) contain both the necessary cryptographic key information, and a way to identify the cryptographic algorithm which uses the key to produce the authentication information typically included in the Mobile Home Authentication extension or the Mobile Foreign Authentication extension. In order for the mobile node to make use of key information sent to it by the AAA server, the mobile node also has to be able to select the appropriate cryptographic algorithm that uses the key to produce the authentication.

For use with the key extensions specified in this document, a table of security algorithm identifiers is also specified. This table is intended to conform to the table of reserved SPIs from RFC 2002, and to allocate some of the currently unused reserved numbers to identify certain common algorithm identifiers.

Algorithm identifier 0 is taken to mean that the mobile node and the AAA server share only one security association, and that unique security association is the one by which the mobile node is

instructed to decode the key information in the MN-HA or the MN-FA Key extension.

Other numbers are defined as follows:

| Algorithm Identifier | Name | Reference |
|---|---|---|
| 2 | MD5/prefix+suffix | RFC 2002 [7] |
| 3 | HMAC MD5 | RFC 2104 [3] |

New identifiers will be allocated as indicated by practical experience using the extensions defined in this document. See section 3 for specific information about using Algorithm Identifier 2. Algorithm Identifier 3 is used in exactly the same way, except that the specific computation used with MD5 follows RFC 2104 instead of RFC 2002.

## 3. Using Algorithm Identifier 2: MD5/prefix+suffix

The AAA indicates that the mobile node must use MD5 in prefix+suffix mode to recover the key information, by inserting the value 2 into the Algorithm Identifier field of the Key extension.

As with Mobile IP, all mobile nodes MUST be able to verify the authenticator within a MN-AAA Authentication extension by using MD5 in prefix+suffix mode, signified by selection at a SPI of any arbitrary 32-bit value. Therefore, it is economical to use the MD5 algorithm in prefix+suffix mode to encode the key within the particular key extension, as follows.

1. The AAA server identifies the mobile node's IP address, call it ``node-address''.

2. The AAA server calculates

   (key XOR (MD5(AAA-key | node-address | AAA-key)))

3. The AAA server inserts this result into the Key extension in the ``Security Information'' field.

4. The mobile node calculates

   temp = MD5(AAA-key | node-address | AAA-key)

5. The mobile node extracts the Security_Information of the key extension and calculates

   key = Security_Information XOR temp

## 4. MN-HA Key Extension

The MN-HA Key extension, shown in figure 1, contains the key for use by the mobile node to secure future Mobile IP registrations with its home agent. The MN-HA Key extension MUST appear in the Registration Request before the MN-AAA Authentication extension.

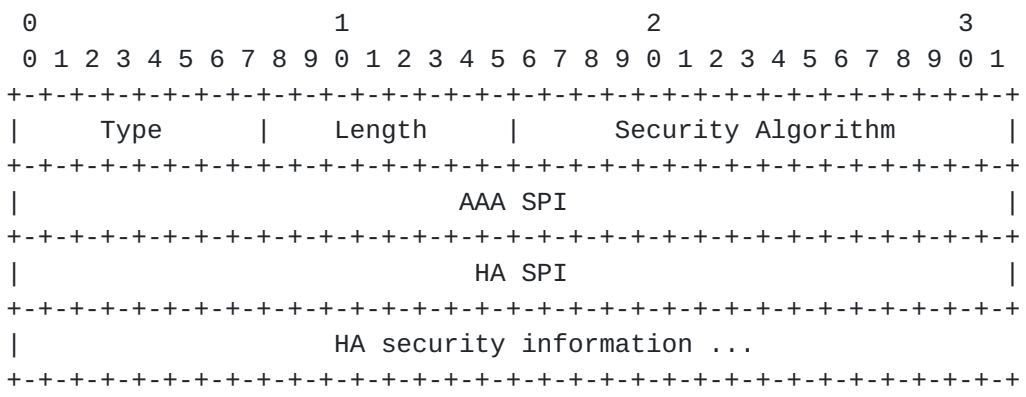


Figure 1: The MN-HA Key Extension

Type 126 (not skippable) [7]

Length 10 plus the length in bytes of the HA security information field

Security Algorithm A value in the table defined in section 2.

AAA SPI A 32-bit opaque value, indicating the SPI that the mobile node must use to determine the algorithm to use for recovering the HA security information.

HA SPI A 32-bit opaque value, which the mobile node MUST use to index all the necessary information recovered from the HA security information after it is decoded.

HA Security Information The necessary information (including the key) required by the mobile node to create a Mobility Security Assocation between itself and the home agent.

Once the mobile node decodes the HA Security Information, by using the algorithm indexed by the AAA SPI, it stores the Security Algorithm field, and the HA Security Information indexed by the HA SPI in its list of Mobile Security Associations.

## 5. MN-FA Key Extension

The MN-FA Key extension, shown in figure 1, contains the key for use by the mobile node to secure future Mobile IP registrations with the same foreign agent. The MN-FA Key extension MUST appear in the Registration Request before the MN-AAA Authentication extension.

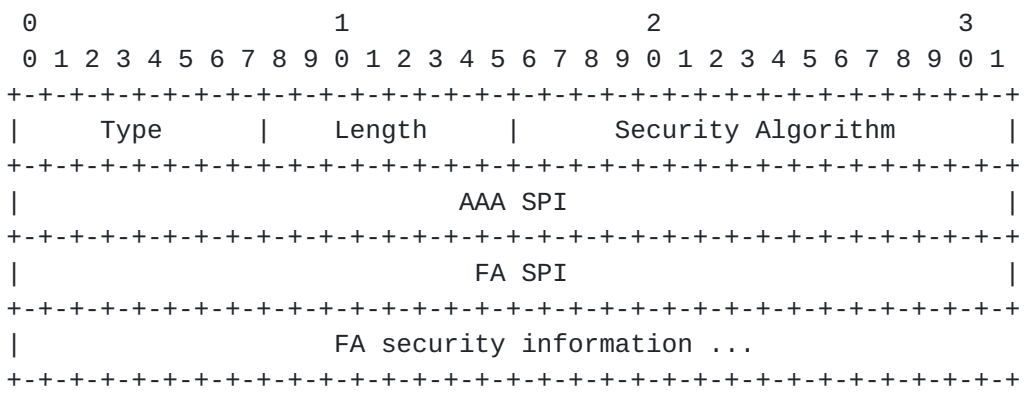


Figure 2: The MN-FA Key Extension

Type 133 (skippable) [7]

Length 10 plus the length in bytes of the FA security information field

Security Algorithm A value in the table defined in section 2.

AAA SPI A 32-bit opaque value, indicating the SPI that the mobile node must use to determine the algorithm to use for recovering the FA security information.

FA SPI A 32-bit opaque value, which the mobile node MUST use to index all the necessary information recovered from the FA security information after it is decoded.

HA Security Information The necessary information (including the key) required by the mobile node to create a Mobility Security Association between itself and the foreign agent.

Once the mobile node decodes the FA Security Information, by using the algorithm indexed by the AAA SPI, it stores the Security Algorithm field, and the FA Security Information indexed by the FA SPI in its list of Mobile Security Associations.

If the foreign agent receives a Registration Reply that does not have a MN-FA Key extension, and thus does not have a way to establish a Mobility Security Association with the mobile node, the foreign agent SHOULD change the Code value of the Registration Reply to MISSING_MN_FA (see section 6), effectively causing the registration to fail.

## 6. Error Values

Each entry in the following table contains the name of Code [7] to be returned in a Registration Reply, the value for the Code, and the section in which the error is first mentioned in this specification.

| Error Name | Value | Section |
|---|---|---|
| MISSING_MN_FA | 106 | 5 |

## 7. IANA Considerations

The number for the MN-HA Key and MN-FA Key extensions are taken from the numbering space defined for Mobile IP registration extensions defined in RFC 2002 [7] as extended in RFC 2356 [5]. The numbering for the extension also SHOULD NOT conflict with values specified in the Internet Draft for Route Optimization [6] Mobile Node NAI ??, or Foreign Agent Challenge extensions [?]. The Code values specified for errors, listed in section 6, MUST NOT conflict with any other code values listed in RFC 2002, RFC 2344 [4], or RFC 2356 [5]. They are to be taken from the space of error values conventionally associated with rejection by the foreign agent (i.e., 64-127).

## 8. Security Considerations

The extensions in this document are intended to provide the appropriate level of security for Mobile IP entities (mobile node, foreign agent, and home agent) to operate Mobile IP registration protocol. The security associations resulting from use of these extensions do not offer any higher level of security than what is already associated with the security association between the mobile node and the AAA. The security association with the AAA is the one from which both the Mobile IP described in this draft are derived.

References

[1] B. Aboba and M. Beadles. RFC 2486: The Network Access Identifier, January 1999. Status: PROPOSED STANDARD.

[2] P. Calhoun and A. Rubens. DIAMETER Base Protocol. draft-calhoun-diameter-07.txt, November 1998. (work in progress).

[3] H. Krawczyk, M. Bellare, and R. Cannetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, February 1997.

[4] G. Montenegro. Reverse Tunneling for Mobile IP. RFC 2344, May 1998.

[5] G. Montenegro and V. Gupta. Sun's SKIP Firewall Traversal for Mobile IP. RFC 2356, June 1998.

[6] Charles E. Perkins and David B. Johnson. Route Optimization in Mobile-IP. draft-ietf-mobileip-optim-08.txt, February 1999. (work in progress).

[7] C. Perkins, Editor. IP Mobility Support. RFC 2002, October 1996.

[8] C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote Authentication Dial In User Service (RADIUS). RFC 2138, April 1997.

Addresses

The working group can be contacted via the current chairs:

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Menlo Park, California 94025
USA

Phone: +1 650 786-5166
Fax: +1 650 786-5896
E-mail: nordmark@sun.com

Basavaraj Patil
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399
USA

+1 972-684-1489

bpatil@nortelnetworks.com

Questions about this memo can be directed to:

Charles E. Perkins
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1-650 786-6464
EMail: cperkins@eng.sun.com
Fax: +1 650 786-6445

Pat R. Calhoun
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1 650-786-7733
EMail: pcalhoun@eng.sun.com