Mobile IP Working Group
INTERNET DRAFT
22 June 2003

Charles E. Perkins
Nokia Research Center
Pat R. Calhoun
Airespace Systems

AAA Registration Keys for Mobile IP

draft-ietf-mobileip-aaa-key-13.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 an AAA Security Association with its home AAA server, however, it is possible to use that AAA Security Association to create derived Mobility Security Associations between the mobile node and its home agent, and again between the mobile node and the foreign agent currently offering connectivity to the mobile node. This document specifies extensions to Mobile IP registration messages that can be used to create Mobility Security Associations between the mobile node and its home agent, and/or between the mobile node and a foreign agent.

1. Introduction

AAA servers, such as RADIUS [14] and DIAMETER [5], are in use within the Internet today to provide authentication and authorization services for dial-up computers. Such services are likely to be valuable for mobile nodes using Mobile IP [13] when the nodes are attempting to connect to foreign domains with AAA servers. Requirements for interactions between AAA and Mobile IP are outlined in RFC 2977 [7]; that document describes an infrastructure which enables AAA servers to authenticate and authorize network access requests from mobile nodes. See also appendix C. The Mobile IP Registration Request is considered to be a request for network access. It is then possible to augment the functionality of the Mobile IP mobility agents so that they can translate between Mobile IP registration messages and the messages used within the AAA infrastructure, as described in RFC 2977. Mobility agents and AAA servers that conform to the requirements of RFC 2977 can be considered as appropriate network entities to support the message types specified in this document. Please consult RFC 2977 [7] for further details.

This specification makes use of a single AAA Security Association to create derivative Mobility Security Associations. A Mobility Security Association in this specification is a simplex connection that serves to authenticate MIPv4 control traffic between a MN and HA and/or a MN and FA. A Mobility Security Association is identified by the two end points, such as a MN IP address and a HA IP address, and a SPI. Two nodes may have one or more Mobility Security Associations established between each other; however, typically there is no reason to have more than one Mobility Security Association between two nodes.

This document specifies extensions to Mobile IP registration messages that can be used to create Mobiity Security Associations between the MN and FA and/or MN and HA based on the AAA Security Association between the MN and HAAA. These additional Mobility Security Associations may then be used in Mobile IP extensions to calculate the Authentication Data need by authentication extensions used in Mobile IP control messages. It is assumed that the AAA Security Association between the MN and its HAAA has been appropriately configured so that the AAA server has the authorization to provide key material to be used as the basis for the necessary Mobility Security Assocation between the MN and its prospective mobility agents.

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 having any home address. However, for Mobile IP to work, the mobile node is required to have a home address and a Mobility Security Association [13] with its home agent. When the Mobile IP Registration Reply packet is authenticated by the MN-AAA Authentication Extension [4], the mobile node can verify that the key material contained in the extensions were produced by the AAA server, and thus may be reliably used to create Mobility Security Associations with the home agent, or alternatively with the foreign agent.

It is also assumed that the AAA entities involved (i.e., the AAAH, AAAL, and the AAA interface features of the foreign agents and home agents) all have means outside of the scope of this document for exchanging keys. The extensions within this document are intended to work with any AAA protocol suite that allows for such key exchange, as long as it satisfies the requirements specified in RFC 2977 [7].

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 [2].

AAA
: Authentication, Authorization, and Accounting (see [9]).

AAA entity
: A network node processing AAA messages according to the requirements for AAA protocols (see [9]).

AAA security association
: A security association between a AAA entity and another node needing the services of that AAA entity. In this document all AAA security associations are between a mobile node and its home AAA server (AAAH). A mobile node's AAA security association with its home AAA server (AAAH) may be based either on the mobile node's IP address or on its NAI [1].

Key
: a number, kept secret. Only nodes in possession of the key have any hope of using the security transform to obtain correct results.

Key Material
: Data used for the purpose of creating a key.

Mobility security association
: A Mobility Security Association is a simplex

connection that serves to authenticate MIPv4 control traffic such as between a MN and HA and/or a MN and FA. A Mobility Security Association is identified by the two end points, such as a MN IP address and a HA IP address, and a SPI. Two nodes may have one or more Mobility Security Associations established between each other; however, typically there is no reason to have more than one Mobility Security Association between two nodes.

Registration Key
: A key used as the basis of a Mobility Security Association between a mobile node and a foreign agent. A registration key is typically only used once or a very few times, and only for the purposes of verifying a small volume of Authentication data.

Security Algorithm
: A set of rules for using input data and a secret key for producing data for use in security protocols.

SPI
: Security Parameters Index. The SPI is an arbitrary 32-bit value that assists in the identification of an AAA, IP, or Mobility Security Association.

Other terminology is used as defined in the base Mobile IP specification [13]. Furthermore, in order to simplify the discussion, we have used the word "Extension" instead of "Subtype of the Generalized Extension" in many cases. So, for instance, instead of using the phrase "The MN-FA Key Material From AAA Subtype of the Generalized MN-FA Key Reply Extension", we would instead use the phrase "The MN-FA Key Material From AAA Extension".

3. Overview of Operations with Key Extensions

When a mobile node depends on an AAA infrastructure to obtain authorization for network connectivity and Mobile IP registration, it may lack any pre-existing Mobility Security Associations with either its home agent, or the foreign agent controlling the access to the foreign network. The extensions defined in this document allow a AAA entity to supply key material to mobile nodes to be used as the basis of its Mobility Security Association with mobile agents. The AAA entity that will act on these extensions is part of the AAA infrastructure, and is typically identified within the foreign domain by methods outside the scope of this specification (see appendix C).

The key material may be requested by the mobile node in new extensions to Mobile IP Registration Request messages, and supplied to the mobile node in extensions to the Mobile IP Registration Reply messages. Alternatively, the AAA server MAY provide unsolicited key material to mobile nodes; the mobile node MUST then calculate new keys and update or create its relevant Mobility Security Association. The method by which key material is supplied to the mobility agents themselves is out of scope for this document, and would depend on the particular details of the security architecture for the AAA servers in the foreign and home domains (see RFC 2977 and appendix C). For the purposes of this document, we assume that there is a suitable AAA infrastructure available to the foreign agents, and that the mobile node does have an AAA Security Association with at least one AAA server in its home domain.

When a mobile node travels away from home, it may not have a Mobility Security Association with its home agent, perhaps because it does not yet have a home address [3]. The protocol and messages in this document are intended to facilitate the following operations which may occur between the mobile node, foreign agent, home agent, and AAA servers in the visited (local) domain (AAAL) and in the home domain (AAAH). In the following sequence of messages, the only message flows specified in this document are the Registration Request between the mobile node and the foreign agent, and Registration Reply between the foreign agent and the mobile node. The other messages described here result from the presumed action of the AAA entities as described in RFC 2977. See also appendix D.

1. If the mobile node does not have a Mobility Security Association with the foreign agent, it SHOULD include an MN-FA Key Request extension (see Section 7.1) as part of its Registration Request that it sends to the Foreign Agent.

2. If the mobile node does not have a Mobility Security Association with the home agent, it MUST add an MN-HA Key Request extension (see Section 7.3) as part of its Registration Request that it sends to the Foreign Agent.

3. If one or more AAA Key Request extensions were added, the mobile node MUST add the MN-AAA Authentication extension to its Registration Request after the AAA Key Request extension.

4. By action of the foreign agent, which is presumed to be also a AAA entity, the mobile node's key requests and authentication data are transferred to the local AAA server (AAAL), typically after reformatting to fit into the appropriate AAA messages, which are out of scope for this document.

5. After the information within the MN-AAA Authentication extension is verified by the AAA server in the home domain (AAAH), it then also generates the Key Material that has been requested by the mobile node, for the necessary Mobility Security Associations.

6. The respective keys for the Mobility Security Associations are distributed to the Home Agent and Foreign Agent via the AAA protocol.

7. The mobile node receives the Registration Reply message from the Foreign Agent.

8. If a MN-HA Key Material from AAA Key Material extension is present in the Registration Reply message, then the mobile node MUST create or update its Mobility Security Association with the Home Agent indicated in the Registration Reply, using the key computed from the Key Material in the AAA extension. In this case, if no Key Material extension is present, the mobile node MUST discard the Registration Reply. If the mobile node does not already have a Mobility Security Association with the Home Agent indicated in the Registration Reply message, and if no Key Material extension is present, the mobile node MUST discard the Registration Reply.

9. Using its (perhaps newly created) Mobility Security Association with the home agent, the mobile node authenticates the Registration Reply message, by checking the Authentication Data in the Mobile-Home Authentication extension.

10. If the Registration Reply passes authentication and contains a MN-FA Key Material From AAA extension (see section 7.2), the mobile node generates the registration key using the Key Material provided, according to its AAA security Association with the AAA. The resulting registration key is used to establish the mobile node's Mobility Security Association with its foreign agent, and is used to compute the authentication data used in the Mobile-Foreign authentication extension.

Any registration reply containing the MN-HA Key Material From AAA extension MUST also contain a subsequent Mobile Home Authentication extension, created using the generated MN-HA key. Similarly, a reply containing the MN-FA Key Material From AAA extension MUST also contain a subsequent Mobile Foreign Authentication extension, created using the registration key.

4. Mobility Security Associations

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 transform which uses the key to produce the authentication information which is present in the Mobile-Home Authentication extension or the Mobile-Foreign Authentication extension. In order for the mobile node to make use of key material created by the AAA server, the mobile node also has to be able to identify and select the appropriate cryptographic transform that uses the key to produce the authentication.

The transform identifiers are the same as those used in IPsec. They are tabulated in the list of Authentication Algorithms allowable as values for the "Attribute Type" (5) (i.e., "Authentication Algorithm"), one of the classifications in the tabulated Attribute Types for "IPSEC Security Association Attributes". See http://www.iana.org/assignments/isakmp-registry for the full listing of all Attribute Types and other Attributes for IPSEC Security Associations.

Mobility Security Associations shared between mobile nodes and home agents also require a replay protection method. The following table contains the supported replay methods.

Replay Method	Name	Reference
0,1	Reserved	
2	Timestamps	RFC 3344 [13]
3	Nonces	RFC 3344 [13]
4-65535	Unallocated	

5. Key Material Creation and Derivation

This section contains the procedures followed in the creation of the Key Material by AAA servers, and the key derivation procedures used by mobile nodes. Note that the AAA servers will also deliver the keys to the mobility agents (home agent, foreign agent) via the AAA protocol. AAA servers that follow these procedures will produce results that can be understood by mobile nodes. The mobility agents will faithfully transcribe the results into the appropriate Mobile IP extensions.

The example that follows makes use of HMAC-MD5 [8]. All mobile nodes and mobility agents implementing Mobile IP [13], and implementing the

extensions specified in this document, MUST implement HMAC-MD5 [13]. Other cryptographic functions MAY also be used.

The following steps are performed on the AAA server:

1. The AAA server identifies the mobile node. If the Home Address field of the Registration Request is either zero (0), or all ones (0xffffffff), then the Mobile Node's NAI is used instead of the mobile node's home address.

2. The AAA server generates a random [6] value of at least 128 bits to be used as the Key Material.

3. The AAA server inserts the random value into the Key Reply extension, in the ``Key Material'' field.

The following steps are performed by the mobile node:

1. Using the Key Material from the extension, the mobile node calculates

   key = HMAC-MD5 (AAA-key, {Key Material || home address})

2. The mobile node creates the Mobility Security Association, using the key and the other relevant information in the Key Extension.

The secret key used within the HMAC-MD5 computation is indicated by the AAA Security Association indexed by the AAA SPI, which has been previously configured as the basis for the AAA Security Association between the mobile node and the AAA server creating the key material.

6. Generalized Key Request/Reply Extensions

The extensions in this section are Generalized Extensions [13], and have subtypes as specified in section 7.

6.1. Generalized MN-FA Key Request Extension

Figure 1 illustrates the Generalized MN-FA Key Request Extension.

Type	TBD (not skippable) (see [13] and section 9)
Subtype	a number assigned to identify the way in which the Key Request Data is to be used when generating the registration key

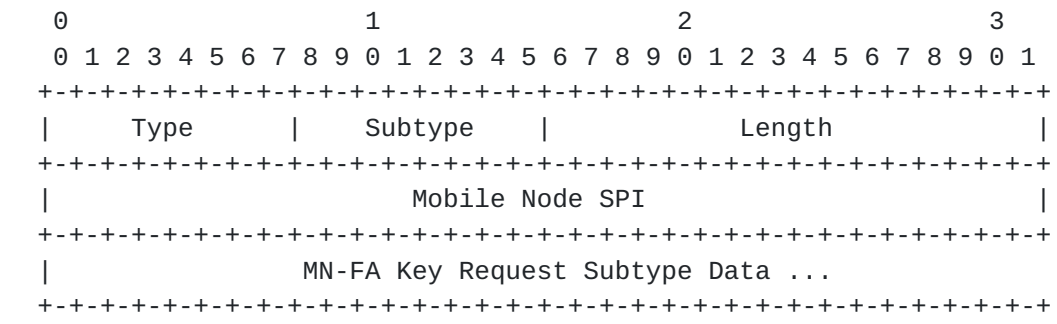

Figure 1: The Generalized Mobile IP MN-FA Key Request Extension

Length — The 16-bit Length field indicates the length of the extension. It is equal to the number of bytes in the MN-FA Key Request Subtype Data plus 4 (for the Mobile Node SPI field).

Mobile Node SPI — The Security Parameters Index that the mobile node will assign for the Mobility Security Association created for use with the registration key.

MN-FA Key Request Subtype Data — Data needed to carry out the creation of the registration key on behalf of the mobile node. This field is zero in length and carries no data.

The Generalized MN-FA Key Request Extension defines a set of extensions, identified by subtype, which may be used by a mobile node in a Mobile IP Registration Request message to request that some other entity create a Registration Key for use by the mobile node with the mobile node's new foreign agent.

6.2. Generalized MN-FA Key Reply Extension

The Generalized MN-FA Key Reply extension supplies a registration key requested by using one of the subtypes of the Generalized MN-FA Key Request extension. Figure 2 illustrates the format Generalized MN-FA Key Reply Extension.

Type — TBD (not skippable) (see [13] and section 9)

Subtype — a number assigned to identify the way in which the MN-FA Key Reply Subtype Data is to be decrypted to obtain the registration key

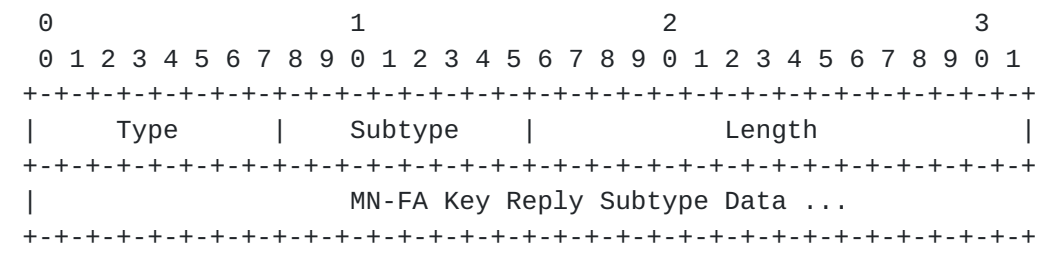

Figure 2: The Generalized Mobile IP MN-FA Key Reply Extension

Length The 16-bit Length field is equal to the number of bytes in the MN-FA Key Reply Subtype Data.

MN-FA Key Reply Subtype Data
An encoded copy of the registration key, along with any other information needed by the recipient to create the designated Mobility Security Association.

For each subtype, the format of the MN-FA Key Reply Subtype Data has to be separately defined according to the particular method required to set up the Mobility Security Association.

For the subtypes defined in this document, the MN-FA Key supplied in the data for a subtype of this extension may come by a request which was sent using a subtype of the Generalized MN-FA Key Request Extension. In such cases, the SPI to be used when employing the Mobility Security Association defined by the registration key is the same as given in the original request.

Once the mobile node creates the Mobility Security Association with the foreign agent, by using the transform indexed by the AAA SPI, it stores that Mobility Security Association indexed by the FA SPI in its list of Mobile Security Associations.

If the foreign agent receives a Registration Reply that has no MN-FA Key Reply extension, and if it has no existing Mobility Security Association with the mobile node, the foreign agent MAY change the Code value of the Registration Reply to MISSING_MN_FA (see section 8), effectively causing the registration to fail.

6.3. Generalized MN-HA Key Request Extension

Figure 3 illustrates the Generalized MN-HA Key Request Extension.

Type TBD (not skippable) (see [13] and section 9)

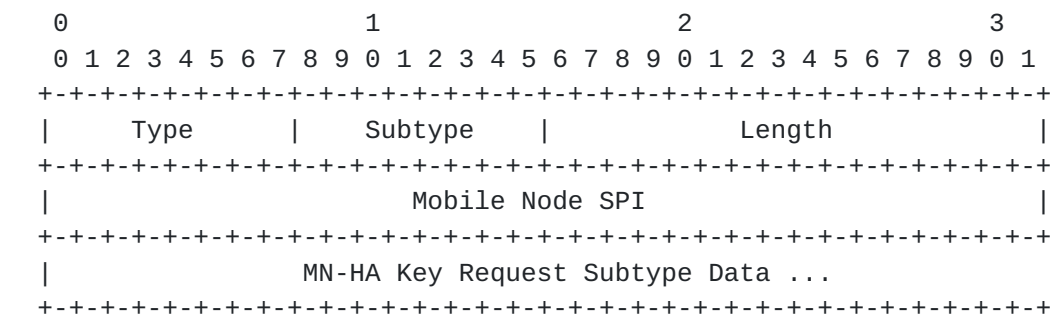

Figure 3: The Generalized Mobile IP MN-HA Key Request Extension

Subtype — a number assigned to identify the way in which the Key Request Data is to be used when generating the registration key

Length — The 16-bit Length field indicates the length of the extension. It is equal to the number of bytes in the MN-HA Key Request Subtype Data plus 4 (for the Mobile Node SPI field).

Mobile Node SPI — The Security Parameters Index that the mobile node will assign for the Mobility Security Association created for use with the registration key.

MN-HA Key Request Subtype Data — Data needed to carry out the creation of the registration key on behalf of the mobile node. This field is zero in length and carries no data.

The Generalized MN-HA Key Request Extension defines a set of extensions, identified by subtype, which may be used by a mobile node in a Mobile IP Registration Request message to request that some other entity create a MN-HA key for use by the mobile node with the mobile node's new home agent.

6.4. Generalized MN-HA Key Reply Extension

Type — TBD (not skippable) (see [13] and section 9)

Subtype — a number assigned to identify the way in which the MN-HA Key Reply Subtype Data is to be decrypted to obtain the MN-HA key

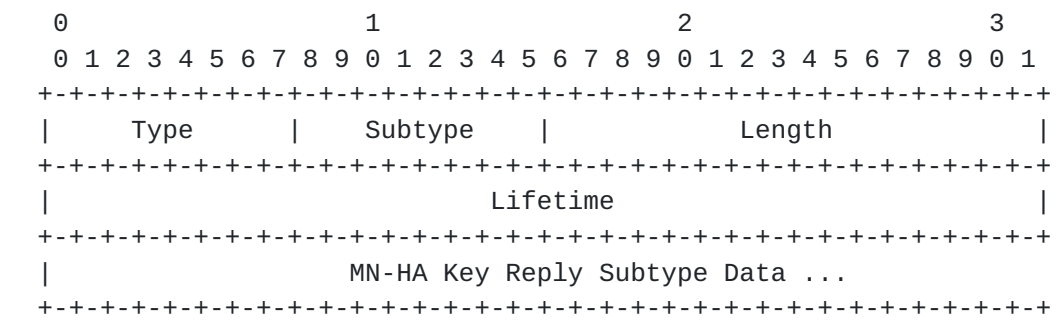

Figure 4: The Generalized Mobile IP MN-HA Key Reply Extension

Length The 16-bit Length field indicates the length of the extension. It is equal to the number of bytes in the MN-HA Key Reply Subtype Data plus 4 (for the Lifetime field).

Lifetime This field indicates the duration of time (in seconds) for which the MN-HA key is valid.

MN-HA Key Reply Subtype Data
An encrypted copy of the MN-HA key, along with any other information needed by the mobile node to create the designated Mobility Security Association with the home agent.

For each subtype, the format of the MN-HA Key Reply Subtype Data has to be separately defined according to the particular method required to set up the Mobility Security Association.

7. Key Request/Reply Subtypes

The extension subtypes in this section are subtypes of the Generalized Extensions specified in section 6.

7.1. MN-FA Key Request From AAA Subtype

The MN-FA Key Request From AAA subtype data uses subtype 7 of the Generalized MN-FA Key Request Extension (see section 6.1). The MN-FA Key Request From AAA extension MUST appear in the Registration Request before the MN-AAA Authentication extension. The subtype data field is zero in length.

7.2. MN-FA Key Material From AAA Subtype

The MN-FA Key Material From AAA extension, shown in figure 5, uses subtype 1 of the Generalized MN-FA Key Reply Extension (see section 6.2).

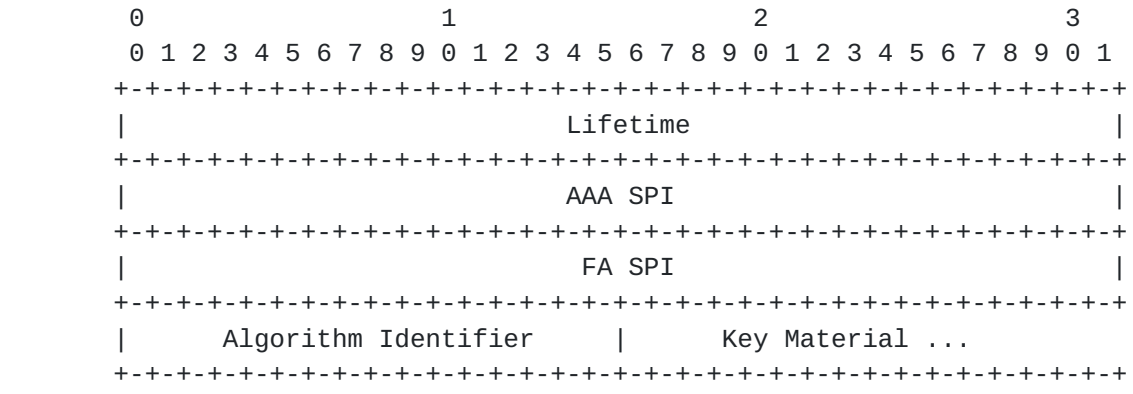

Figure 5: The MN-FA Key Material From AAA Subtype-Specific Data

lifetime This field indicates the duration of time (in seconds) for which the registration key is valid.

AAA SPI A 32-bit opaque value, indicating the SPI that the mobile node must use to determine the transform to use for establishing the Mobility Security Association between the mobile node and its prospective foreign agent.

FA SPI The SPI for the Mobility Security Association to the FA that the mobile node creates using the Key Material

Algorithm Identifier
This field indicates the transform to be used (stored as part of the Mobility Security Association with the foreign agent, and selected from among the values in the "Authentication Algorithm" table cited in section 4), for future computations of the Mobile-Foreign Authentication Extension.

Key Material
A random [6] value of at least 128 bits.

The MN-FA Key Material From AAA extension MUST appear in the Registration Reply before the Mobile-Foreign Authentication extension. The Key Material is provided by the AAA server for use by

the mobile node in creating the registration key, which is used to secure future Mobile IP registrations with the same foreign agent.

7.3. MN-HA Key Request From AAA Subtype

The MN-HA Key Request From AAA subtype data uses subtype 7 of the Generalized MN-HA Key Request Extension (see section 6.3). The MN-HA Key Request From AAA extension MUST appear in the Registration Request before the MN-AAA Authentication extension. The subtype data field is zero in length.

7.4. MN-HA Key Material From AAA Subtype

The MN-HA Key Material From AAA is subtype 7 of the Generalized MN-HA Key Reply Extension (see section 6.4).

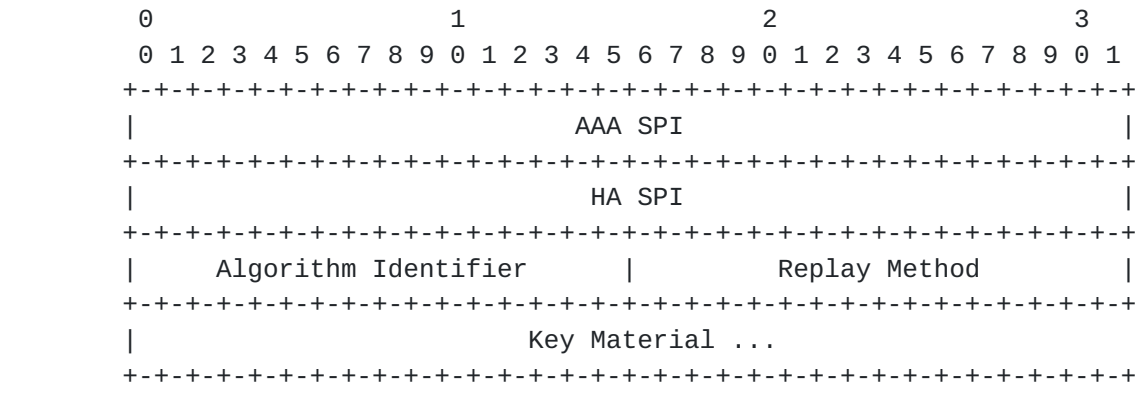

Figure 6: The MN-HA Key Material From AAA Subtype-Specific Data

AAA SPI A 32-bit opaque value, indicating the SPI that the mobile node must use to determine the transform to use for establishing the Mobility Security Association between the mobile node and its home agent.

HA SPI The SPI for the Mobility Security Association to the HA that the mobile node creates using the Key Material

Algorithm Identifier
This field indicates the transform to be used for future computations of the Mobile-Home Authentication Extension (see section 4)

Replay Method
This field contains the replay method to be used for future Registration messages (see section 4).

Key Material
A random [6] value of at least 128 bits.

The MN-HA Material Key From AAA subtype-specific data is shown in figure 6. The Mobile Node calculates the MN-HA key using the Key Material provided by the AAA server. The calculation proceeds by using the key shared between the mobile node and the AAA server that has previously been configured for securing all such communication requirements with the AAA server which will be contacted within the AAA infrastructure (see appendix C). The MN-HA key is intended for use by the mobile node to secure future Mobile IP registrations with its home agent. The MN-HA Key Material extension MUST appear in the Registration Reply before the MN-HA Authentication extension.

Once the mobile node creates the MN-HA Key, by using the transform specified in the AAA SPI, it stores the HA Security Information indexed by the HA SPI in its list of Mobile Security Associations. The mobile node uses the Identification field data from the Registration Request as its initial synchronization data with the home agent.

8. Error Values

Each entry in the following table contains the name of the Code [13] value to be returned in a Registration Reply, the value for that Code, and the section in which the error is first mentioned in this specification.

Error Name	Value	Section
MISSING_MN_FA	107	6.2

9. IANA Considerations

The numbers for the Generalized Extensions in section 6 are taken from the numbering space defined for Mobile IP registration extensions defined in RFC 3344 [13] as extended in RFC 2356 [11]. The numbers suggested in this section are already in use by implementations which have been tested for interoperability.

The number 7, assigned to the MN-FA Key Request From AAA Subtype extension (see section 7.1), is taken from the numbering space defined for the Generalized MN-FA Key Request Extension (see section 6.1).

The number 1, assigned to the MN-FA Key Material From AAA Subtype extension (see section 7.2), is taken from the numbering space defined for the Generalized MN-FA Key Reply Extension (see section 6.2).

The number 7, assigned to the MN-HA Key Request From AAA Subtype extension (see section 7.4), is taken from the numbering space defined for the Generalized MN-HA Key Request Extension (see section 6.3).

The number 7, assigned to the MN-HA Key Material From AAA Subtype extension (see section 7.4), is taken from the numbering space defined for the Generalized MN-HA Key Reply Extension (see section 6.4).

The Code value specified for error MISSING_MN_FA, listed in section 8, MUST NOT conflict with any other code values listed in RFC 3344, RFC 3024 [10], or RFC 2356 [11]. This value is to be taken from the space of error values conventionally associated with rejection by the foreign agent (i.e., 64-127).

Section 4 introduces the Replay Method Identifier namespace that requires IANA management. This specification makes use of 1-3; all other values other than zero (0) or one (1) are available for assignment, pending review and approval by a Designated Expert [12].

10. 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 calculate the Authentication Data needed by authentication extensions used with Mobile IP registration

messages. The Mobility Security Associations resulting from use of these extensions do not offer any higher level of security than what is already implicit in use of the AAA Security Association between the mobile node and the AAAH. In order to deny any adversary the luxury of unbounded time to analyze and break the secrecy of the AAA Security Association between the mobile node and the AAA server, that AAA Security Association MUST be refreshed periodically.

The provisioning and refreshing of the AAA key in the MN and AAA server is outside the scope of this document. Typical methods for provisioning and refresh at the MN include the use of https between the MN and a trusted provisioning server (e.g., over a wireless link layer). Wireless standards organizations specify the details of the wireless link operation, including authentication of the MN at the link layer.

Since the extensions defined in this specification only carries Key Material, which is used to derive keys, it does not expose any data that could be used in an attack aimed at recovering the key shared between the mobile node and the AAA. The authors do not believe this specification introduces any new security vulnerability.

11. Acknowledgements

Thanks to Fredrik Johansson, Tom Hiller, and the members of the IESG for their useful comments on this document.

References

[1] B. Aboba and M. Beadles. The Network Access Identifier. Request for Comments (Proposed Standard) 2486, Internet Engineering Task Force, January 1999.

[2] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. Request for Comments (Best Current Practice) 2119, Internet Engineering Task Force, March 1997.

[3] P. Calhoun and C. Perkins. Mobile IP Network Access Identifier Extension for IPv4. Request for Comments (Proposed Standard) 2794, Internet Engineering Task Force, January 2000.

[4] P. Calhoun and C. E. Perkins. Mobile IP Foreign Agent Challenge/Response Extension. Request for Comments (Proposed Standard) 3012, Internet Engineering Task Force, December 2000.

[5] Pat R. Calhoun, John Loughney, E. Guttman, Glen Zorn, and Jari Arkko. DIAMETER Base Protocol (work in progress). Internet Draft, Internet Engineering Task Force. draft-ietf-aaa-diameter-15.txt, October 2002.

[6] D. Eastlake, 3rd, S. Crocker, and J. Schiller. Randomness Recommendations for Security. Request for Comments (Informational) 1750, Internet Engineering Task Force, December 1994.

[7] S. Glass, T. Hiller, S. Jacobs, and C. Perkins. Mobile IP Authentication, Authorization, and Accounting Requirements. Request for Comments (Proposed Standard) 2977, Internet Engineering Task Force, October 2000.

[8] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. Request for Comments (Informational) 2104, Internet Engineering Task Force, February 1997.

[9] D. Mitton, M. St.Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens, and B. Wolff. Authentication, Authorization, and Accounting: Protocol Evaluation. Request for Comments (Informational) 3127, Internet Engineering Task Force, June 2001.

[10] Editor G. Montenegro. Reverse Tunneling for Mobile IP, revised. Request for Comments (Proposed Standard) 3024, Internet Engineering Task Force, January 2001.

[11] G. Montenegro and V. Gupta. Sun's SKIP Firewall Traversal for Mobile IP. Request for Comments (Informational) 2356, Internet Engineering Task Force, June 1998.

[12] T. Narten and H. Alvestrand. Guidelines for Writing an IANA Considerations Section in RFCs. Request for Comments (Best Current Practice) 2434, Internet Engineering Task Force, October 1998.

[13] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 3344, Internet Engineering Task Force, August 2002.

[14] C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote Authentication Dial In User Service (RADIUS). Request for Comments (Proposed Standard) 2865, Internet Engineering Task Force, June 2000.

A. Changes Since Previous Revision

- Cleaned up terminology:
  * Clarified the use of "security association" throughout the document as either "IPSec" or "Mobility" or "AAA".

B. Older Changes

In this revision of the document, there have been several major changes as a result of suggestions received during Last Call.

- Generalized Key Extensions previously specified in another document have been instead specified in this document in order that this document can be self-contained and not dependent on the standardization status of the other document.
- Additional explanation has been included for the purposes of clarifying the problem space and solution approach.
- An appendix has been added to describe the expected AAA infrastructure that will produce the keys that are to be distributed within the extensions specified in this document.
- Ladder diagrams have been included to illustrate the expected message flows containing the extensions defined in this document.

- HMAC-MD5 has been mandated for implementation by the mobile node, for compatibility with RFC 3344 [13]. The example text has been modified accordingly (see section 5).

- A table of Algorithm Identifiers has been identified as the numbering space for transform selection when establishing the Mobility Security Association using the keys distributed with the extensions in this document. See section 4.

- A terminology section has been added.

- This appendix has been added.

  * New terminology entries for "Registration Key", "AAA", "AAA entity", "Mobility Security Association", "AAA Security Association",

  * All instances of MN-FA key are now called "registration key"

  * All instances of the key between mobile node and home agent are called "MN-HA" key.

- Removed extraneous IANA considerations paragraph for HMAC_MD5

- Removed "Unsolicited" from subtype names

- Changed minimum Key Material length from 64 bits to 128 bits

C. AAA Infrastructure

In this appendix, we attempt to capture the main features of a basic model for operation of AAA servers that is assumed for understanding of the use of the Mobile IP registration extensions described in this document. This information has been adapted from the discussion in RFC 2977 [7].

Within the Internet, a mobile node belonging to one administrative domain (called the home domain) often needs to use resources provided by another administrative domain (called the foreign domain). A foreign agent that handles the mobile node's Registration Request is likely to require that the mobile node provide some credentials that can be authenticated before access to the resources is permitted. These credentials may be provided as part of the Mobile-AAA Authentication extension [4], relying on the existence of an AAA infrastructure such as is described in this section, and also described in RFC 2977 and RFC 3012 [4]. Such credentials are typically managed by entities within the mobile node's home domain. They may be also used for setting up secure communications with the

mobile node and the foreign agent, or between the mobile node and its home agent if necessary.

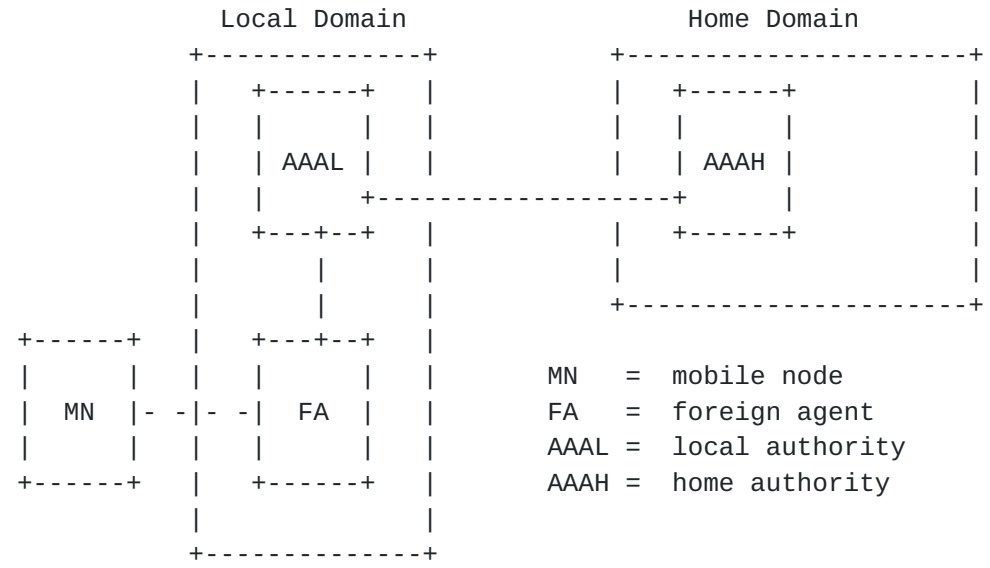

Figure 7: AAA Servers in Home and Local Domains

The foreign agent often does not have direct access to the data needed to verify the credentials. Instead, the foreign agent is expected to consult an authority (typically in the same foreign domain) in order to request proof that the mobile node has acceptable credentials. Since the foreign agent and the local authority (AAAL) are part of the same administrative domain, they are expected to have established, or be able to establish for the necessary lifetime, a secure channel for the purposes of exchanging sensitive (access) information, and keeping it private from (at least) the visiting mobile node.

The local authority (AAAL) itself may not have enough information stored locally to carry out the verification for the credentials of the mobile node. In contrast to the foreign agent, however, the AAAL is expected to be configured with enough information to negotiate the verification of mobile node credentials with its home domain. The home and foreign domains should be configured with sufficient IP Security Associations and access controls so that they can negotiate the authorization, and also enable the mobile node to acquire Mobility Security Associations with the mobility agents within the foreign domain. For the purposes of the key exchanges specified within this document, the authorization is expected to depend only upon secure authentication of the mobile node's credentials.

Once the authorization has been obtained by the local authority, and the authority has notified the foreign agent about the successful negotiation, the foreign agent can deliver the Registration Reply to the mobile node along with the key material.

In figure 7, there might be many mobile nodes from many different Home Domains. Each Home Domain provides a AAAH that can check credentials originating from mobile nodes administered by that Home Domain. There is a security model implicit in figure 7, and it is crucial to identify the specific security associations assumed in the security model. These IP Security Associations are illustrated in figure 8, and are considered to be relatively long-lived security associations.

First, it is natural to assume that the mobile node has an AAA Security Association with the AAAH, since that is roughly what it means for the mobile node to belong to the home domain.

Second, from the model illustrated in figure 7 it is clear that AAAL and AAAH have to share an IP Security Association, because otherwise they could not rely on the authentication results, authorizations, nor even the accounting data which might be transacted between them. Requiring such bilateral IP Security Associations is, however, in the end not scalable; the AAA framework must provide for more scalable mechanisms, but the methods by which such a broker model is to be created are out of scope for this document. See RFC 2977 for more details.

Finally, from figure 7, it is clear that the foreign agent can naturally share an IP Security Association with the AAAL. This is necessary in order for the model to work because the foreign agent has to have a way to find out that it is permissible to allocate the local resources to the mobile node, and further to transmit any successful Registration Reply to the mobile node.

Figure 8 illustrates the IP Security Associations we understand from our proposed model. Note that there may be, by mutual agreement between AAAL and AAAH, a third party inserted between AAAL and AAAH to help them arbitrate secure transactions in a more scalable fashion. The broker model which has been designed to enable such third-party processing should not have any effect on the Mobile IP extensions specified in this document, and so no description is provided here; see RFC 2977 [7] for more details.

Nodes in two separate administrative domains (for instance, AAAH and AAAL) often must take additional steps to verify the identity of their communication partners, or alternatively to guarantee the privacy of the data making up the communication. While these

considerations lead to important security requirements, as mentioned

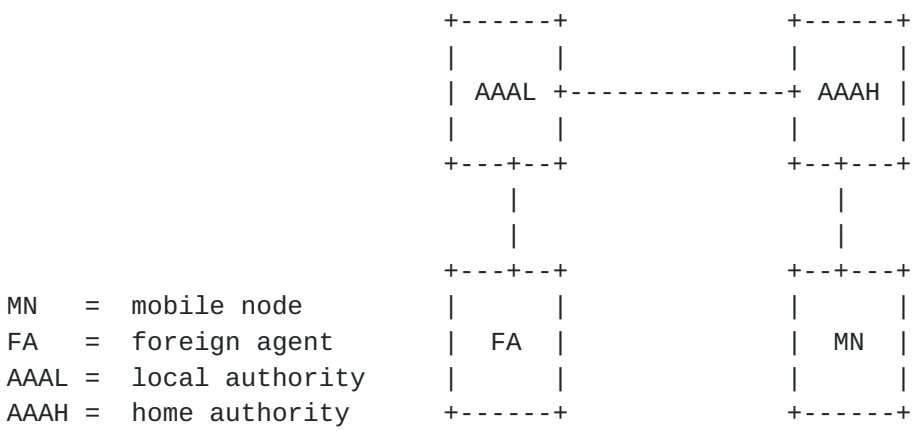

Figure 8: IP Security Associations

above in the context of security between servers, we consider the exact choice of IP Security Associations between the AAA servers to be beyond the scope of this document. The choices are unlikely to depend upon Mobile IP, or any specific features of the general model illustrated in figure 7. On the other hand, the Mobility Security Associations needed between Mobile IP entities are of central importance in the design of the key derivation extensions in this document.

One further detail deserves mention. The Mobility Security Association to be established between the mobile node and the foreign agent have to be communicated to the foreign agent as well as to the mobile node. The way that the key is distributed to the foreign agent is not relevant to any material in this document, and is expected to be handled as part of the AAA protocol processing between the AAAH and AAAL, and the further AAA protocol processing between the AAAL and the foreign agent. Any method by which the key can be securely transmitted to the AAAL and then relayed (possibly with re-encryption) to the foreign agent, is outside the jurisdiction of any Mobile IP specification, and thus compatible (by reason of non-interference) with the protocol extensions specified in this document.

D. Message Flow for Requesting and Receiving Registration Keys

In this section, we show message flows for requesting and receiving a registration key from the AAA infrastructure, described in section C. Challenge values, as specified in [4], might be added to the Advertisement and Registration messages for additional replay protection, but are not illustrated here.

Diagram 9 illustrates the message flow for the case when the mobile node explicitly requests a registration key.

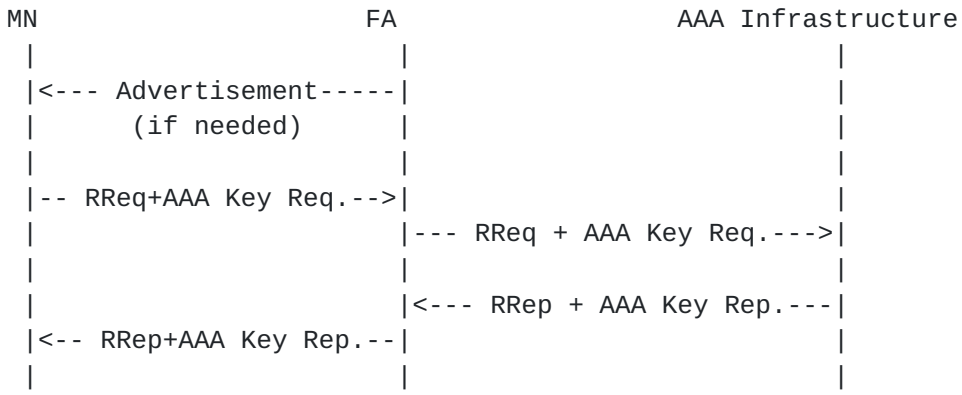

Figure 9: Message Flows for Requesting and Receiving Registration Keys

In diagram 9, the following message flow is illustrated:

1. The foreign agent disseminates an Agent Advertisement. This advertisement MAY have been produced after receiving an Agent Solicitation from the mobile node (not shown in the diagram).

2. The mobile node creates a Registration Request including the MN-HA Key Request and/or MN-FA Key Request, as needed, along with an authorization-enabling authentication extension as required by Mobile IP [13].

3. The foreign agent relays the Registration Request and/or Key Request(s) to its locally configured AAA Infrastructure (see appendix C), according to local policy.

4. The foreign agent receives a AAA Response with the appropriate indications for authorizing connectivity for the mobile node. Along with this AAA Response, the foreign agent may also receive key material by some secure method appropriate for communications between it and its local AAA infrastructure. At this point if the foreign agent has not relayed the Registration Request, it forwards it directly to the Home Agent and waits for a Registration Reply (not shown in the figure).

5. The foreign agent relays the Registration Reply to the mobile node, along with the new Key Material extensions to be used by the mobile node to establish Mobility Security Associations with the relevant mobility agents (foreign agent and/or home agent).

Diagram 10 illustrates the message flow for the case when the mobile node receives an unsolicited registration key from the AAA Infrastructure.

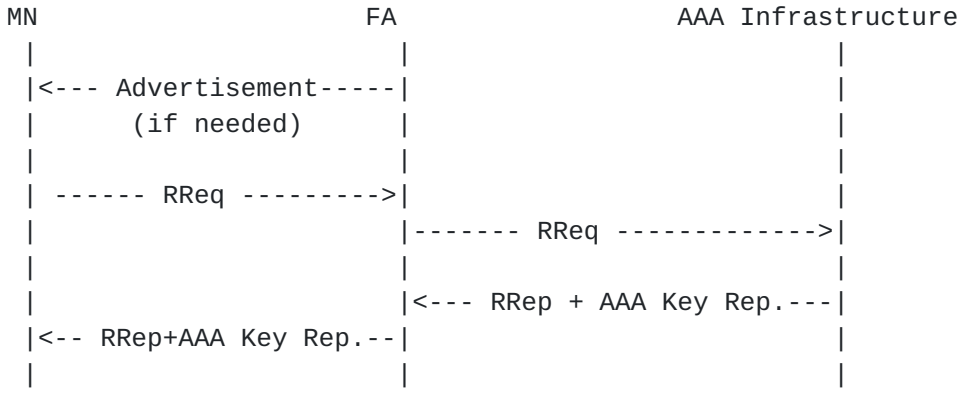

Figure 10: Message Flow for Receiving Unsolicited Registration Keys

In diagram 10, the following message flow is illustrated:

1. The foreign agent disseminates an Agent Advertisement. This advertisement MAY have been produced after receiving an Agent Solicitation from the mobile node (not shown in the diagram).

2. The mobile node creates a Registration Request including an authorization-enabling authentication extension as required by Mobile IP [13].

3. The foreign agent sends a AAA Request (possibly containing the Registration Request) to its locally configured AAA Infrastructure (see appendix C), according to local policy.

4. The foreign agent receives a AAA Response with the appropriate indications for authorizing connectivity for the mobile node. Along with this AAA Response, the foreign agent may also receive key material by some secure method appropriate for communications between it and its local AAA infrastructure. At this point, if the foreign agent has not relayed the Registration Request, it forwards it directly to the Home Agent and waits for a Registration Reply (not shown in the figure).

5. The foreign agent relays the Registration Reply to the mobile node, along with the new Key Material extensions to be used by the mobile node to establish Mobility Security Associations with the relevant mobility agents (foreign agent and/or home agent).

Addresses

Questions about this memo can also be directed to the authors:

Charles E. Perkins	Pat R. Calhoun
Communications Systems Lab	
Nokia Research Center	Airespace Networks
313 Fairchild Drive	110 Nortech Parkway
Mountain View, California 94043	San Jose, CA 95134
USA	USA
Phone: +1-650 625-2986	Phone: +1 408 635 2000
EMail: charliep@iprg.nokia.com	Email: pcalhoun@bstormnetworks.com
Fax: +1 650 625-2502	Fax: +1 408 635 2020