Mobile IP Working Group
INTERNET DRAFT
27 August 2001

Charles E. Perkins
Nokia Research Center
Pat R. Calhoun
Sun Microsystems Laboratories

Generalized Key Distribution Extensions for Mobile IP

draft-ietf-mobileip-gen-key-01.txt

Status of This Memo

Abstract

Recent proposals have suggested several kinds of key extensions for Mobile IP registration messages. These keys may be used between the mobile node and mobility agents, or between the mobility agents themselves. This document specifies generalized extension formats that can be useful for several kinds of key distributions. Each generalized extension format will have subtypes which indicate the specific format for the key distribution data.

1. Introduction

Recent proposals [5, 6] have suggested several kinds of key extensions for Mobile IP [4] registration messages. These keys may be used between the mobile node and mobility agents, or between the mobility agents themselves. This document specifies generalized extension formats that can be useful for several kinds of key distributions. Each generalized extension format will have subtypes which indicate the specific format for the key distribution data. Each generalized format conforms to the overall format suggested for generalized Mobile IP extensions recently described for MIER [2].

Different generalized extensions are defined depending upon the following factors:

- The intended use of the key

- Whether the extension requests a key or supplies a key

Extensions that request a key are allowable in Mobile IP Registration Request messages. Extensions that supply key material are allowable in Mobile IP Registration Reply messages.

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 [1].

2. Generalized MN-FA Key Request Extension

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

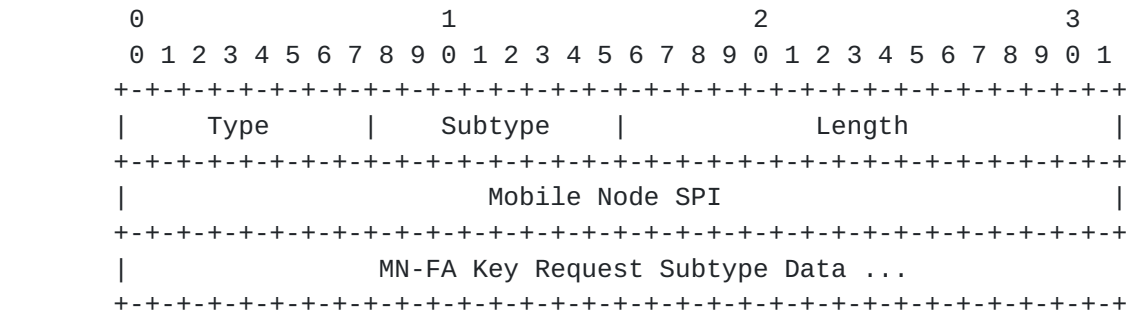

Figure 1: The Generalized Mobile IP MN-FA Key Request Extension

Type TBD (not skippable) (see [4] and section 8)

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-FA Key Request Subtype Data plus 4 (for the Mobile Node SPI field), and SHOULD be at least 20.
Mobile Node SPI	The Security Parameters Index that the mobile node will assign for the 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.

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 key for use by the mobile node with the mobile node's new foreign agent.

3. 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.

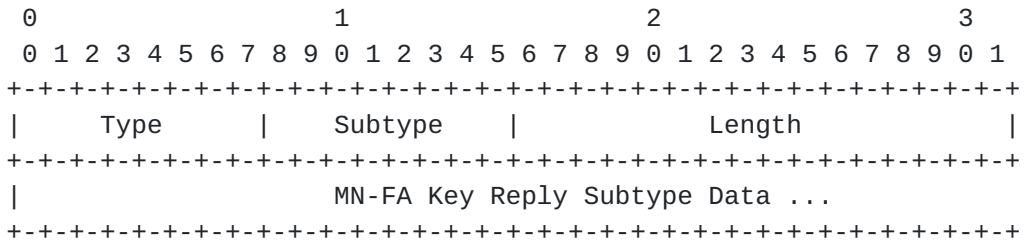

Figure 2: The Generalized Mobile IP MN-FA Key Reply Extension

Type TBD (not skippable) (see [4] and section 8)

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

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 key to be used between the mobile node and the foreign agent, 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 security association.

In some cases, the MN-FA Key supplied in the data for a subtype of this extension comes by a request which was sent using a subtype of the Generalized MN-FA Key Request Extension. In that case, the SPI to be used when employing the security association defined by the registration key is the same as given in the original request.

4. Generalized MN-HA Key Request Extension

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

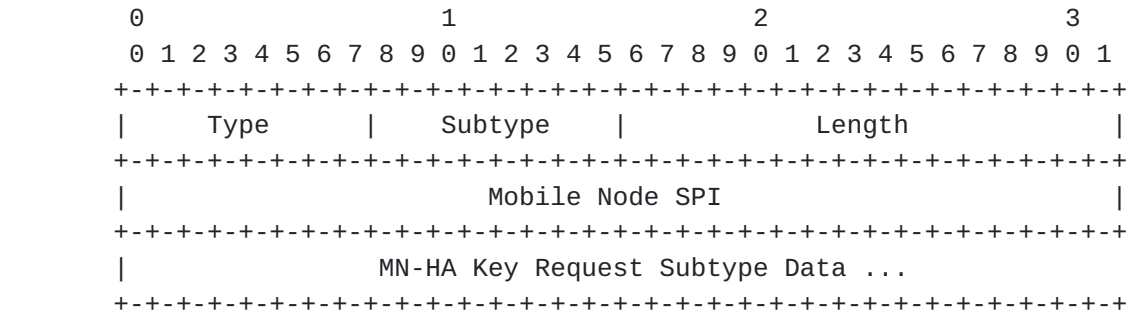

Figure 3: The Generalized Mobile IP MN-HA Key Request Extension

Type TBD (not skippable) (see [4] and section 8)

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), and SHOULD be at least 20.

Mobile Node SPI The Security Parameters Index that the mobile node will assign for the 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.

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 key for use by the mobile node with the mobile node's new home agent.

5. Generalized MN-HA Key Reply Extension

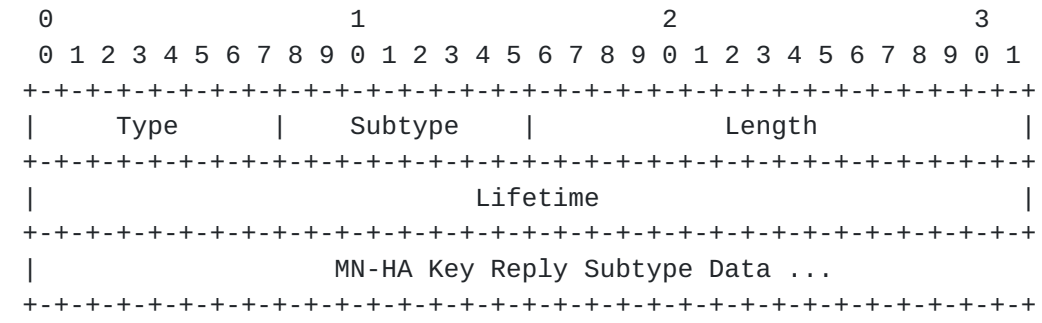

Figure 4: The Generalized Mobile IP MN-HA Key Reply Extension

Type TBD (not skippable) (see [4] and section 8)

Subtype a number assigned to identify the way in which the MN-HA Key Reply Subtype Data is to be decrypted to obtain 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 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 key to be used between the mobile node and its home agent, 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 security association.

6. Generalized FA-HA Key Reply Extension

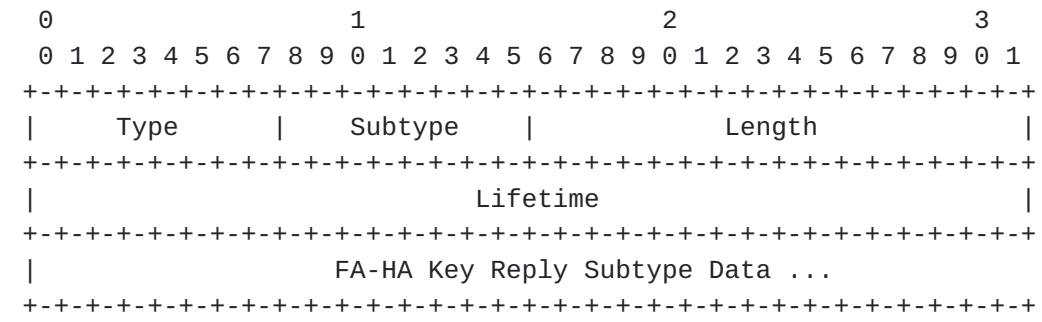

Figure 5: The Generalized Mobile IP FA-HA Key Reply Extension

Type TBD (not skippable) (see [4] and section 8)

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

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

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

FA-HA Key Reply Subtype Data
An encrypted copy of the key to be used between the foreign agent and the mobile node's home agent, along with any other information needed by the foreign agent

to create the designated Mobility Security Association with that home agent.

For each subtype, the format of the FA-HA Key Reply Subtype Data has to be separately defined according to the particular method required to set up the security association.

7. Generalized FA-FA Key Reply Extension

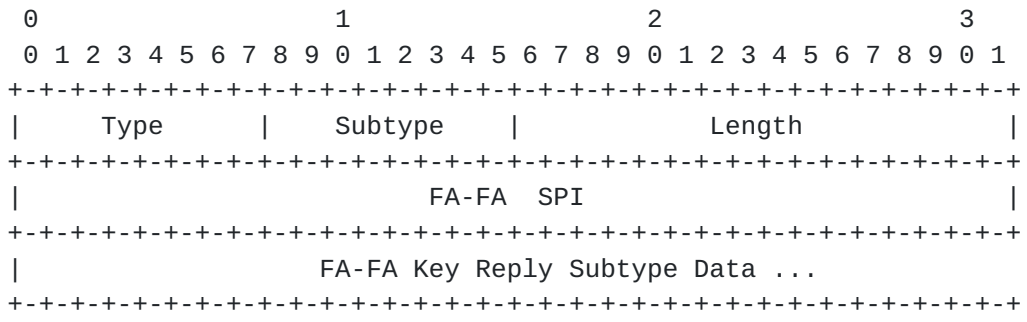

Figure 6: The Generalized Mobile IP FA-FA Key Reply Extension

Type — TBD (not skippable) (see [4] and section 8)

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

Length — The 16-bit Length field is equal to the number of bytes in the FA-FA Key Reply Subtype Data plus 4 (for the FA-FA SPI field).

FA-FA SPI — This field indicates the SPI that should be used to decipher the FA-FA key.

FA-FA Key Reply Subtype Data — An encrypted copy of the key to be used between two foreign agents, along with any other information needed by the foreign agents to create the desired security association.

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

8. IANA Considerations

The numbers for the Generalized Key Extensions specified in sections 2 through 7 are to be taken from the non-skippable range of the Mobile IP registration extension namespace defined in [4].

Section 2 introduces the Generalized MN-FA Key Request Extension namespace that requires IANA management. All values other than zero (0) are available for assignment via Standards Action [3].

Section 3 introduces the Generalized MN-FA Key Reply Extension namespace that requires IANA management. All values other than zero (0) are available for assignment via Standards Action [3].

Section 4 introduces the Generalized MN-HA Key Request Extension namespace that requires IANA management. All values other than zero (0) are available for assignment via Standards Action [3].

Section 5 introduces the Generalized MN-HA Key Reply Extension namespace that requires IANA management. All values other than zero (0) are available for assignment via Standards Action [3].

Section 6 introduces the Generalized FA-HA Key Reply Extension namespace that requires IANA management. All values other than zero (0) are available for assignment via Standards Action [3].

Section 7 introduces the Generalized FA-FA Key Reply Extension namespace that requires IANA management. All values other than zero (0) are available for assignment via Standards Action [3].

9. 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 implicit in use of the security association between the receiver and the entity distributing the key.

10. Acknowledgements

Thanks to Jouni Malinen and Madhavi Chandra for their careful review and suggestions for improving this specification.

References

[1] 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.

[2] M. Khalil, R. Narayanan, H. Akhtar, and E. Qaddoura. Mobile IP Extensions Rationalization (MIER) (work in progress). Internet Draft, Internet Engineering Task Force. draft-ietf-mobileip-mier-06.txt, April 2001.

[3] 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.

[4] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, October 1996.

[5] C. Perkins and P. Calhoun. AAA Keys for Mobile IP (work in progress). Internet Draft, Internet Engineering Task Force. draft-ietf-mobileip-aaa-key-00.txt, July 2001.

[6] C. E. Perkins, D. Johnson, and N. Asokan. Registration Keys for Route Optimization (work in progress). draft-ietf-mobileip-regkey-03.txt, July 2000.

Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nokia
6000 Connection Dr.
Irving, TX. 75039
USA
Phone: +1 972-894-6709
Email: Basavaraj.Patil@nokia.com

Phil Roberts
Megisto Corp.
Suite 120
20251 Century Blvd
Germantown MD 20874
USA
Phone: +1 847-202-9314
Email: PRoberts@MEGISTO.com

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

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1-650 625-2986
EMail: charliep@iprg.nokia.com

Pat R. Calhoun
Black Storm Networks
250 Cambridge Avenue, Suite 200
Palo Alto, California, 94306
USA
Phone: +1 650-617-2932
Email: pcalhoun@diameter.org

Fax: +1 650 625-2502 Fax: +1 650-786-6445