Registration Keys for Route Optimization

Charles E. Perkins

cperkins@eng.sun.com

http://www.srvloc.org/~charliep

David B. Johnson

dbj@cs.cmu.edu

http://www.monarch.cs.cmu.edu/

Route Optimization Extensions

Route Optimization defines the following Mobile IP message extensions:

35 = Route Optimization Authentication Extension

96 = Previous Foreign Agent Notification extension

113 = Foreign Agent Key Request Extension

114 = Mobile Node Public Key Extension

115 = Foreign Agent Public Key Extension

116 = Registration Key Request Extension

120 = Home-Mobile Key Reply Extension

121 = Foreign Agent Key Reply Extension

122 = Mobile Node Public Key Reply Extension

123 = Foreign Agent Public Key Reply Extension

124 = Diffie-Hellman Key Reply Extension

125 = Registration Key SPI Extension

Foreign Agent Key Request Extension

Appended by the Foreign Agent to Mobile Node's Registration Request when the Foreign Agent has a security association with the Home Agent

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |           SPI .....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      .... SPI (continued)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type	113
Length	4
SPI	An opaque identifier picked by the Foreign Agent to identify the security association between itself and the Mobile Node which will use the Registration Key selected by the Home Agent

Mobile Node Public Key Extension

Appended by the Mobile Node to its Registration Request when it has a public key

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             | MN Public Key
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     ... Mobile Node Public Key, continued ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 114

Length (variable length) The number of bytes in the mobile node's public key

Mobile Node Public Key

The public key of the Mobile Node to be used when encoding the registration key

Foreign Agent Public Key Extension

Appended by the Foreign Agent to the Mobile Node's Registration Request when the Foreign Agent has a public key

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |             Length                |  SPI ...  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      ... SPI, continued                           |FA Public Key|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          ... Foreign Agent Public Key, continued ...          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type
: 115

Length
: (variable length) The number of bytes in the foreign agent's public key

SPI
: An 32-bit opaque identifier used to identify the security association created with the registration key

Foreign Agent Public Key
: The public key of the Foreign Agent to be used by the Home Agent when encoding the registration key

Registration Key Request Extension

Appended by the Mobile Node to its Registration Request when the Foreign Agent has advertised the 'S' bit

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |             Length            |   Prime ...   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
               ... Prime, continued ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    Generator ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                  Computed Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type	116
Length	(variable length) The number of bytes in the Prime, Generator, and Computed Value
Prime	a large prime number n serving as the modulus
Generator	a large prime number g serving as the base for exponentiation
Computed Value	g^x, for some large secret number x

Note that all three of *prime*, *generator*, and *computed value* have the same number of bits, so that *Length* should be a multiple of 3.

Home-Mobile Key Reply Extension

Appended by the Home Agent to the Mobile Node's Registration Reply when it is serving as a *KDC* for the key distribution.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             |    SPI ...    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             ... SPI, continued                |Encrypted Key...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Mobile Node's Encrypted Key, continued (variable length) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type	120
Length	(variable length) The number of bytes in the SPI plus the mobile node's encrypted key
SPI	a 32-bit opaque identifier, larger than 255

Mobile Node's Encrypted Key

The key chosen by the Home Agent, encrypted under the security association indicated by SPI

Foreign Agent Key Reply Extension

Appended by the Home Agent to the Mobile Node's Registration Reply when it is serving as a *KDC* for the key distribution.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             |    SPI ...    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           ... SPI, continued                  |Encrypted Key...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Foreign Agent's Encrypted Key, continued (variable length) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 121

Length (variable length) The number of bytes in the SPI plus the foreign agent's encrypted key

SPI a 32-bit opaque identifier, larger than 255

Foreign Agent's Encrypted Key

The key chosen by the Home Agent, encrypted under the security association with the Foreign Agent indicated by SPI

Mobile Node Public Key Reply

Appended by the Foreign Agent to the Registration Request when using the Mobile Node's Public Key to encode the registration key

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             |    SPI ...    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         ... SPI, continued                    |Encrypted Key...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Mobile Node's Encrypted Key, continued (variable) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 122

Length (variable length) 4 plus the length of the mobile node's encrypted key

SPI a 32-bit opaque identifier, larger than 255,

Mobile Node's Encrypted Key

The key chosen by the Foreign Agent

Note that the Home Agent also relays extension 122 to the Mobile Node by appending it to the Registration Reply

Foreign Agent Public Key Reply

Appended by the Home Agent to the Registration Reply when using the Foreign Agent's Public Key to encode the registration key

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             |    SPI ...    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              ... SPI, continued               |Encrypted Key...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Foreign Agent's Encrypted Key, continued (variable) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 123

Length (variable length) 4 plus the length of the foreign agent's encrypted key

SPI a 32-bit opaque identifier, larger than 255 identifying the security association which should operate using the key selected by the Home Agent

Foreign Agent's Encrypted Key
The key chosen by the Home Agent, encrypted by using the foreign agent's public key

Diffie-Hellman Key Reply Extension

Appended by the Home Agent to the Mobile Node's Registration Reply when it is serving as a *KDC* for the key distribution.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |              Length               |  SPI ...  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           ... SPI, continued                |  Computed Value |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            ... Computed Value, continued ...                   
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type	124
Length	(variable length) 4 plus the length of the *computed value*
SPI	a 32-bit opaque identifier, larger than 255, identifying the security association which should operate using the result of the Diffie-Hellman key exchange
Computed Value	$g^y \mod n$, where g and n are the *prime* and the *generator* transmitted by the mobile node

Registration Key SPI Extension

Appended by a mobility agent to specify what SPI should be associated with a registration key, when the information is not already available from context

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |           SPI .....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      .... SPI (continued)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 125

Length 4

Scenarios for getting Registration Keys

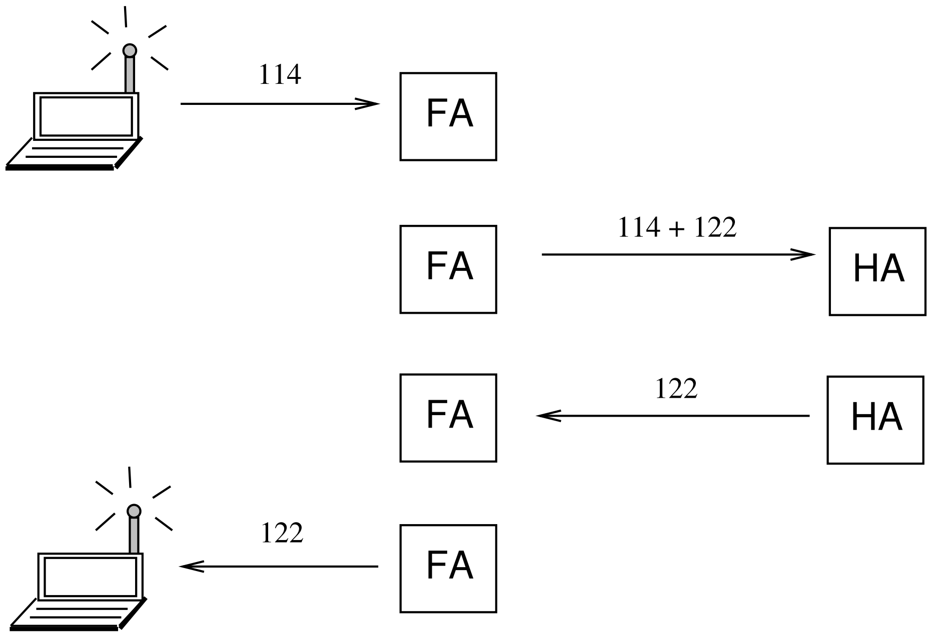
Using the above extensions, a mobile node can get a key if:

1. It has a security association with the foreign agent
2. It has a public key
3. The foreign agent has a public key
4. The foreign agent has a security association with the home agent
5. The mobile node is willing to carry out a Diffie-Hellman key exchange.

If the mobile node has a security association with the foreign agent, no additional Registration Key needs to be created as part of the Mobile IP Registration Request transaction. Otherwise, the following scenarios are provided for, using the Home Agent either as a KDC or to authenticate the key reply by the Foreign Agent.

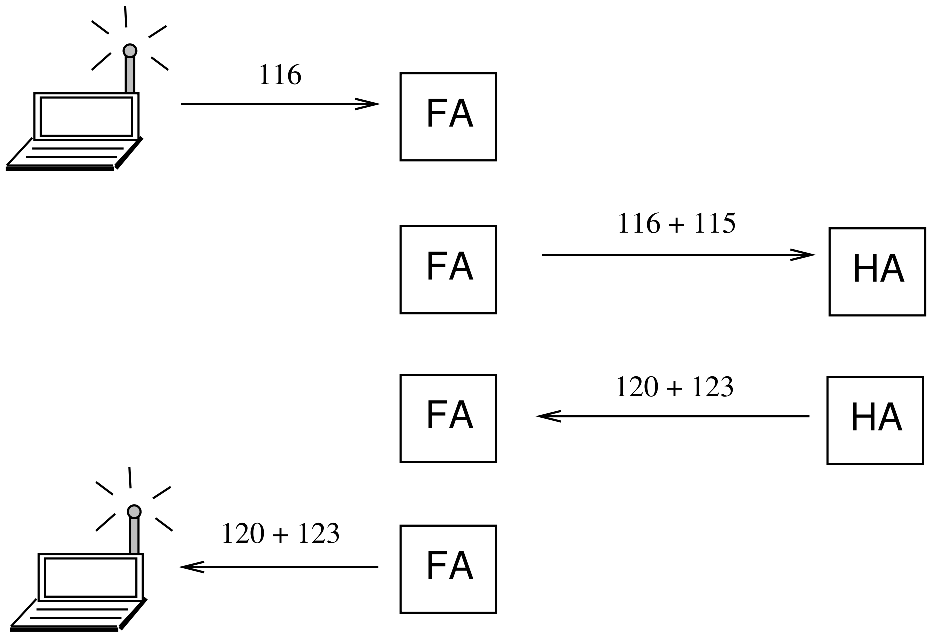
Each possible scenario results in setting up a *SPI* between the mobile node and the foreign agent.

Scenario 2: Mobile Node has a Public Key



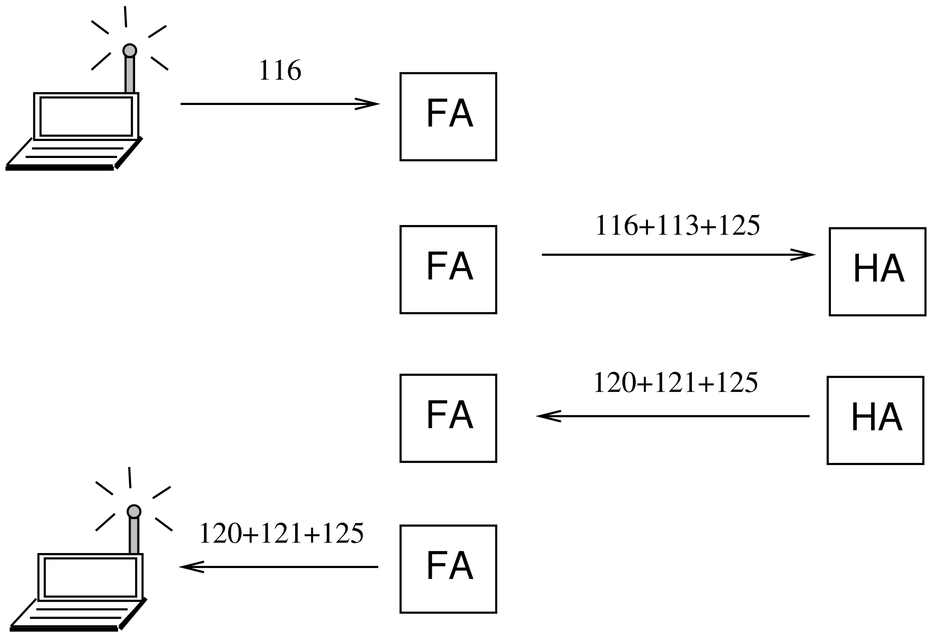
1. MN appends its Public Key (extension 114) to Registration Request
2. FA picks key, encodes it and further appends extension 122 to Registration Request
3. HA appends extension 122 to Registration Reply, authenticates
4. FA relays extension 122 to MN

Scenario 3: Foreign Agent has a Public Key



1. MN appends Registration Key Request (extension 116)
2. FA includes its Public Key by further appending extension 115
3. HA picks registration key, encodes it using FA's public key (extension 123) to Registration Reply
4. HA again encodes the key using MN's security association and includes the result in extension 120 to Registration Reply
5. FA relays extensions 120 and 123 to MN

Scenario 4: Foreign Agent has a Security Association with HA



1. MN appends Registration Key Request (extension 116)

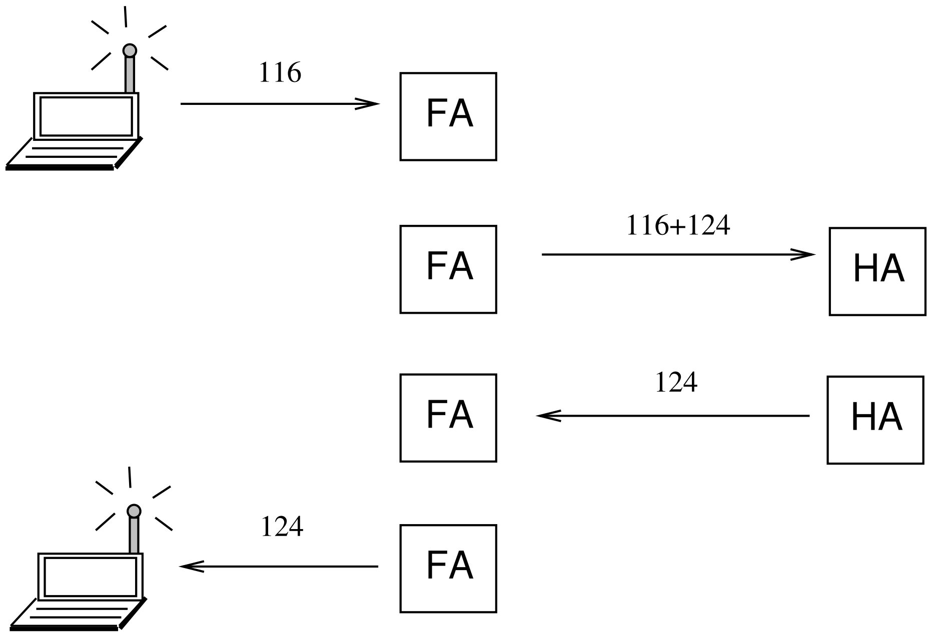
2. FA asks the home agent to pick a key by further appending extension 113 to Registration Request

3. HA picks registration key, encodes it using FA's security association and includes the result in extension 121 to Reply

4. HA again encodes the key using MN's security association and includes the result in extension 120 to Registration Reply

5. FA relays extensions 120 and 121 to MN

Scenario 5: Diffie-Hellman Key Exchange



1. MN appends Key Request (extension 116) to Registration Request
2. FA picks parameter, does Diffie-Hellman computation, includes the answer in extension 124 to Registration Request
3. HA appends extension 124 to Registration Reply, authenticates
4. FA relays extension 124 to MN

Diffie-Hellman Algorithm

Publicly known parameters: large numbers n and g, such that

$$1 < g < n.$$

- Mobile Node picks a large random number x and sends $g^x \ mod \ n$ to Foreign Agent
- Foreign Agent picks a large random number y and sends $g^y \ mod \ n$ to Mobile Node

Now, both Mobile Node and Foreign Agent can compute

$$key = g^{xy} \ mod \ n,$$

but no other node can easily do so. key is, of course, used as the registration key.

Programming Mobile Nodes to Request a Key

```
if (got 'S' bit) {
        if (have security association with previous FA) {
               /* append previous foreign agent notification */
        }

        /* Set up registration key */
        if (have security association with current FA) {
               use(it);/* Don't need to create a registration key */
        }
        else if (have a public key) {
               /* append MN Public Key request */
        }
        else if (want D-H exchange) {
               /* compute a value for prime p and generator g */
               /* use it and append MN Key request */
        }
        else
               /* append MN key request with null computed value, etc */
}
```