MIP6 Working Group
Internet Draft
Expires: April 2007

G. Giaretta
I. Guardini
E. Demaria
M. La Monaca
Telecom Italia
J. Bournelle
M. Laurent-Maknavicius
GET/INT

October 2006

Application Master Session Key (AMSK) for Mobile IPv6
<draft-giaretta-mip6-amsk-02.txt>

Status of this Memo

Copyright Notice

Abstract

The Extensible Authentication Protocol (EAP) defines an extensible framework for performing network access authentication. Most EAP authentication algorithms, also known as "methods", export keying material that can be used with lower layer ciphersuites. It can be useful to leverage this keying material to derive usage specific keys that can be used to authenticate users or protect information

exchange by other applications or services.For this purpose [10] proposes to derive root keys for each usage application and, then, child keys to actual be used.

This document defines how to generate a Usage Specific Root Key (USRK) and a series of Application Master Session Keys (AMSKs) specific to Mobile IPv6 service. These AMSKs can be used by Mobile Node and Home Agent to bootstrap Mobile IPv6 protocol operation.

Table of Contents

1. Introduction

Mobile IPv6 (MIPv6) requires that Mobile Nodes (MNs) and Home Agents (HAs) share a security association to protect binding management signaling. The MIPv6 protocol specification [1] mandates the use of IPsec for this purpose and therefore requires the MN to be provisioned with the data needed to bootstrap an IPsec Security Association (SA) with its Home Agent. This is one of the main issues of the so called Mobile IPv6 bootstrapping problem [11]. The IPsec SA between MN and HA can be established from a shared secret using IKE with Pre-Shared Key (PSK) authentication [6]. Alternatively, the Authentication Protocol for MIPv6 [5] presents a different security mechanism for Mobile IPv6 that requires a shared secret between MN and HA to authenticate the binding messages. In scenarios where network access control is based on EAP those shared secrets can be derived from the EAP key hierarchy [13]. In particular [10] specifies a mechanism for deriving cryptographically separate root keys from the EMSK, called Usage Specific Root Keys (USRK) in order to create a set of keys for usage specific needs.

This document defines how to generate EAP derived key (USRK) specific for Mobile IPv6 bootstrapping. In addition, it defines how to derive application specific keys (AMSKs) both for IPsec SAs and Authentication Protocol SAs. The solution presented in this document is agnostic of the AAA-HA interface model (e.g. push/pull model).

2. Terminology

Most of the terms used in this document are defined in this section; more detailed general mobility and EAP terminology can be found in [7] and [13].

MSA

Mobility Service Authorizer. A service provider that authorizes Mobile IPv6 service.

ASA

Access Service Authorizer. A network operator that authenticates a mobile host and establishes the mobile host's authorization to receive Internet service.

Split scenario

A scenario where the mobility service and the network access service are authorized by different entities (MSA!=ASA).

Integrated scenario

A scenario where the mobility service and the network access service are authorized by the same entity (MSA=ASA).

EAP server

The entity that terminates the EAP authentication method with the peer. In the case where no backend authentication server is used, the EAP server is part of the authenticator. In the case where the authenticator operates in pass-through mode, the EAP server is located on the backend authentication server.

MSK Master Session key

Keying material that is derived between the EAP peer and server and exported by the EAP method. The MSK is at least 64 octets in length.

EMSK Extended Master Session Key

Additional keying material derived between the peer and server that is exported by the EAP method. The EMSK is at least 64 octets in length, and is never shared with a third party.

USRK Usage Specific Root Key

Keys derived from the EMSK which are cryptographically separate from each other.

AMSK Application Master Session Key

Keys derived from the USRK which are cryptographically separate from each other.

MN Mobile Node

A node that can change its point of attachment from one link to another, while still being reachable via its home address.

HA   Home Agent

A router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link addressed to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address.

BU   Binding Update

A message indicating a mobile node's current mobility binding, and in particular its care-of address.

BA   Binding Acknowledgement

A message used to acknowledge receipt of a Binding Update.

3. Applicability Statement

The Mobile IPv6 bootstrapping problem statement [11] describes two main scenarios. In the first scenario (i.e. the split scenario), the mobility service is authorized by a different service authorizer (MSA, Mobility Service Authorizer) than the basic network access authorizer (ASA, Access Service Authorizer). In the second scenario (i.e. the integrated scenario), the mobile node's mobility service is authorized by the same service authorizer as the basic network access service authorizer. This implies that only in the integrated scenario it is possible to leverage the network access authentication to bootstrap mobility service. Therefore, the approach defined in this document applies only to the integrated scenario.

This specification assumes that AAA server and the EAP server are co-located, with the latter exporting the keys to the former. As already pointed out, the solution presented here addresses both the IPsec and rfc4285-based SAs bootstrapping.

3.1 Bootstrapping IPsec SAs with Pre-shared keys

The bootstrapping solution defined for integrated scenario [19] requires the mobile node to run an EAP exchange over IKEv2. In case the mobile node uses EAP for network access authentication, this implies that the MN executes two EAP exchanges, possibly with the same EAP server and using the same credentials.

Therefore, in this scenario a key derived from EAP key hierarchy and named IKEv2-AMSK can be used as the IKEv2 Pre-shared Key (PSK), with the advantage that only one EAP exchange is performed (during network access authentication).

The key is derived by the MN and the AAAH server and needs to be transferred to the HA (together with the MN/key identifier). Two different approaches are possible:

1. The AAAH server sends proactively the key to the HA (push approach). A requirement for this approach is that the AAAH server needs to know the HA assigned to the MN.

2. The HA requests to the AAAH the PSK during the IKEv2 exchange with the MN (pull approach). In this case the HA needs to know the AAAH server used by a specific MN for network access authentication.

Figure 1 and 2 (pag. 8) show the message flow of the two models. Note that in both approaches the MN/key identifier must be sent via the AAA-HA interface and needs to be the same identifier used in IKEv2.

3.2 Bootstrapping rfc4285-based SAs

Concerning rfc4285-based SAs, the keying material derived from EAP can be exploited in two different ways, since two possible authentication options are specified:

1. MN-HA Mobility Message Authentication Option. In this case a key derived from EAP key hierarchy and named MN-HA-AMSK, is used as the shared key for the security association between the MN and HA. Similarly to the IKEv2 Pre-shared key case, both the push and pull model can be envisioned for key delivery. The MN/key identifier must be sent via the AAA-HA

interface and needs to be the same identifier to be used as Mobile Node Identifier (in the form of NAI) in the BUs.

2. MN-AAA Mobility Message Authentication Option. In this case a key derived from EAP key hierarchy and named MN-AAA-AMSK, is used as the shared-key for the security association between the MN and the AAAH server. In this case, no key delivery is needed.

```
   EAP PEER    EAP-AUTH          EAP-AUTH Server
   Home
      MN         NAS                   Server
   Agent
      |                               |
   |
      |         EAP session           |
   |
      |<----------------------------->|
   |
      |                               |
   |
      |          o o o                |
   |
      |                               |
   |
      |           |   Access-Accept   |
   |
   U A|           |  EAP Success, MSK |
   |
   S M| EAP Succ. |<------------------+
   |
   R S|<----------|                   \ ------------
   |
   K K|                                |   USRK     |
   |
     s|                                |generation  |
   |
      |                                 ------------
   |
      |           Binging Update / IKEv2 IKE_AUTH
   |
      |---------------------------------------------------------------
   >|
      |
   |
      |                               |   "Key-Request, MN identity"
   |
      |                               |<------------------------------
   -|
      |                               |      "keying material"
   |
      |                               | ------------------------------
   >|
      |                                                 ----------- /
   |
      |                                                |  AMSKs    |
   |
      |                                                |generation |
   |
      |                                                 -----------
   |
```

Figure 1 - Pull model message flow

```
   EAP PEER    EAP-AUTH          EAP-AUTH Server
   Home
      MN          NAS                 Server
   Agent
      |                               |
   |
      |         EAP session           |
   |
      |<----------------------------->|
   |
      |                               |
   |
      |          o o o                |
   |
      |                               |
   |
      |           |   Access-Accept   |
   |
   U A|           |  EAP Success, MSK | "Keying material, MN
   identity"|
   S M| EAP Succ. |<------------------+-------------------------------
   >|
   R S|<----------|                   \ ------------
   |
   K K|                                |   USRK     |   ----------- /
   |
     s|                                |generation  |  |  AMSKs    |
   |
      |                                 ------------   |generation |
   |
      |                                                 -----------
   |
      |           Binging Update / IKEv2 IKE AUTH
   |
      |---------------------------------------------------------------
   >|
```

Figure 2 - Push model message flow

4. Key derivation

The key hierarchy proposed in this document is depicted in Figure 3. Just one key (MIP6-USRK) is directly derived from the EMSK. Three different keys are then generated from the MIP6-USRK: IKEv2-AMSK, MN-HA-AMSK and MN-AAA-AMSK. The basic assumption is that the MIP6-USRK is exported by the EAP server to the AAA server that sends this key to the HA; the other keys are then derived directly from the USRK by the HA of the MSP.

```
                                  EMSK
                                   |
                               MIP6-USRK
                                   |
                +-----------------------------------+
                |                  |               |
            MN-AAA-AMSK       MN-HA-AMSK       IKEv2-AMSK
```

Figure 3 - Proposed key hierarchy

4.1 Mobile IPv6 USRK derivation

Mobile IPv6 USRK (MIP6-USRK) is derived through the general key derivation function (KDF) specified in [10]. The KDF is based on a pseudo random function shown below:

```
KDF = PRF(key, data)

where:

PRF = HMAC-SHA-256
key = EMSK
data = label + "\0" + op-data + length
label = MIPv6-USRK-key
op-data = EAP Session-ID
length = 128 bit
"\0" = is a NUL byte (0x00 in hex)
+ denotes concatenation

Key name = PRF-64 (EAP Session-ID, key-label)
Where PRF-64 is the first 64 bits from the output.
```

4.2 Mobile IPv6 AMSKs derivation

Based on Mobile IPv6 USRK, the keys for Mobile IPv6 operations (IKEv2-AMSK, MN-HA-AMSK, and MN-AAA-AMSK) can be generated. These keys are derived as follows:

```
KDF (K,L,D,O) = T1 | T2 | T3 | T4 | ...
```

```
      where:
      T1 = prf (K, S | 0x01)
      T2 = prf (K, T1 | S | 0x02)
      T3 = prf (K, T2 | S | 0x03)
      T4 = prf (K, T3 | S | 0x04)

      prf = HMAC-SHA-256
      K = USRK-MIPv6
      L = key label
      D = application data
      O = output length
      S = L | " " | D | O
```

The application specific parameters are set as follows:

```
IKEv2 Pre-shared key AMSK (IKEv2-AMSK):
      key label = "MIPv6-IKEv2-key"
      application data = "HA Address"
      output length = variable (default 128)
(key name = PRF-64(IKEv2-AMSK | EAP Session-ID)

rfc4285 MN-HA key (MN-HA-AMSK):
      key label = "rfc4285-MN-HA-key"
      application data = "HA Address"
      output length = 128 bit
(key name  = PRF-64(MN-HA-AMSK | EAP Session-ID)

rfc4285 MN-AAA key (MN-AAA-AMSK):
      key label = "rfc4285-MN-AAA-key"
      application data = ""
      output length = 128 bit
(key name = PRF-64(MN-AAA-AMSK | EAP Session-ID)
```

The actual key(s) to be derived by MN and HA depend on the authentication method deployed by the operator (or imposed by specific technologies). It should be possible on the operator side to differentiate users' authentication method on profile basis.

The KDF does not include the home address in the application data because in this way the MN can derive the AMSK even if it does not know its home address yet. This is what might happen in some dynamic home address assignment scenarios.

4.3 Lifetimes

As specified in [10] the lifetime of USRK keys must be equal to the lifetime of the EMSK. Lifetime of child keys, instead, can be different then root key s lifetime and its specification is left to usage definition.

Since the IKEv2-AMSK serves only for identity verification and not for authentication or ciphering purposes, there might be no need to re-generate the key at regular intervals. For this reason its lifetime is set equal to the MIP6-USRK lifetime.

Since the MN-HA key is used to authenticate BUs and BAs messages, there is a clear need to keep these keys fresh and therefore to derive new keys periodically. This is discussed in section 5.3.

Obviously all keys must be refreshed whenever a new EMSK is generated (i.e. during re-authentication events).

5. Open issues

The usage of EAP-derived keying material is still a work in progress in IETF and a good amount of study is underway to standardize generation and usage for keys generated from the EMSK. For this reason, this document leaves open some issues as input for HOKEY WG and others related WGs.

5.1 Key length (and other key related parameters)

This specification doesn't address the problem of negotiating the key length; this is a general issue for AMSKs and should be solved in a generic way, not depending on the application that makes use of the keys (e.g. Mobile IPv6 bootstrapping).

One very basic approach, applicable to some scenarios, is that the operator pre-provisions the user equipment with the right parameters (e.g. the right key lenght for a specific application).

If an explicit negotiation is needed, a possible approach could be the one adopted in [18] that leverages the capability of some EAP methods (e.g. EAP-SIM, EAP-FAST, etc.) to carry arbitrary parameters during the authentication phase.

However, it is worthwhile noting that some applications require only fixed length keys (e.g. MN-HA-AMSK and MN-AAA-AMSK for the MIPv6 Authentication Protocol) and for those applications this is not an issue.

5.2 rfc4285 SAs

This document addresses only the negotiation of the shared secret among MN and HA (or AAA). Other parameters such as SPIs must be negotiated through other mechanisms. As for the key length issue this could be addressed by an explicit negotiation [18]. Another approach might be the derivation of the SPI from the EAP keying hierarchy itself.

5.3 Key Freshness

While not an issue for IKEv2 PSK authentication, for rfc2485-based authentications the keys used to authenticate binding management messages should be fresh and therefore periodically changed. This document addresses only bootstrapping mechanisms and so the renewal of keying material is out of scope. A suggested solution may be that a new MN-HA-AMSK is generated at each BU/BA completed exchange (e.g. exchanging nonces in BUs and BAs).

5.4 Multiple EAP sessions

In some scenarios (e.g. multi-homed terminals) a MN may have more than one active EAP session at the same time. Therefore, there is the need to define criteria for deciding which session(s) are in charge of generating AMSKs, and for which applications.

5.5 Identity management and key binding

A MN can be associated to several identities at the same time (e.g. pseudonyms for identity privacy or temporary identities for EAP fast reconnect techniques like [9]). The AAAH server must be aware of the identity used by the MN in IKEv2 or rfc-4285 signaling. In pull model this is needed to allow the AAAH server to select the correct key to be delivered, upon requests, to the HA. In push model this is needed to allow the AAAH server to proactively deliver to the HA the correct MN identity information so that the HA can bind the subsequent authentication requests to the right key.

6. AAA-HA interface requirements

In order to fulfil the bootstrapping of MIPv6-related SAs, this document adds/modifies some requirements for the HA-AAA interface [21]:

- G1.4 should use MUST (instead of SHOULD): "The AAA-HA interface MUST provide confidentiality since it may be used to transfer keying material (e.g. shared key generated during EAP authentication)"

- HAs must be able to fetch keys from AAA servers (pull approach)

- the AAAH server must be able to push a key into the HA (push approach)

- key identifiers and lifetimes must be transferred alongside the key

- in the request sent to the AAAH server in pull mode, HA must specify the HA address known be the MN, so that the AAAH server can derive the right key.

7. Security Considerations

Sending USRK for Mobile IPv6 from the AAA server to the HA requires that the protocol used for AAA-HA communication provides mutual authentication, integrity/reply protection and confidentiality.

Moreover, since this document is strongly based on EAP [8] and the EAP Keying Management Framework [13], additional security considerations are bound to those valid for the EAP Keying Framework.

8. IANA Considerations

This document does not require actions by the IANA.

9. Acknowledgments

The authors would like to thank Alpesh Patel, Hannes Tschofenig, Rafa Lopez and Antonio Skarmeta for reviewing the document and the European Commission support in the co-funding of the ENABLE project, where this work is partly being developed.

10. References

10.1 Normative References

[1] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[2] Arkko, J., Devarapalli, V., Dupont, F., "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[3] Manner, J., Kojo, M. "Mobility Related Terminology", RFC 3753, June 2004

[4] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and H. Lefkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[5] A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[6] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[7] Manner, J., Kojo, M. "Mobility Related Terminology", RFC 3753, June 2004

[8] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[9] Haverinen, H., Salowey, J. "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, January 2006.

[10] Salowey J., Dondeti L., Narayanan V., Nakhjiri M., "Specification for the Derivation of Usage Specific Root Keys (USRK) from an Extended Master Session Key (EMSK)", draft-salowey-eap-emsk-deriv-01 (work in progress), June 2006.

10.2 Informative References

[11] Patel, A. et al. "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-00 (work in progress), July 2004.

[12] K. Chowdhury, J. Bournelle, M. Nakhjiri, "Problem Statement for AMSK", February 2006.

[13] Aboba, B., Simon, D., Arkko, J., Levkowetz, H., "EAP Key Management Framework", draft-ietf-eap-keying-14(work in progress), June 2006.

[14] N.Cam-Winget, D. McGrew, J. Salowey, H.Zhou, "EAP Flexible Authentication via Secure Tunneling (EAP-FAST)", draft-cam-winget-eap-fast-00.txt (work in progress), February 2004

[15] Palekar, A. et al., "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-08 (work in progress), July 2004.

[16] Haverinen, H. and J. Salowey, "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)", draft-haverinen-pppext-eap-sim-13 (work in progress), April 2004.

[17] Arkko, J. and H. Haverinen, "EAP-AKA Authentication", draft-arkko-pppext-eap-aka-12 (work in progress), April 2004.

[18] Giaretta, G., Guardini, I., Demaria, E., Bournelle, J., Laurent-Maknavicius, M., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), October 2004.

[19] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping via DHCPv6 for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-00 (work in progress), October 2005.

[20] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft- ietf-mip6-bootstrapping-split-01 (work in progress), October 2005.

[21] Giaretta G., Guardini I., Demaria E., Bournelle J., Lopez, R., "Goals for AAA-HA interface ", draft-ietf-mip6-aaa-ha-goals-01 (work in progress), January 2006.

Authors' Addresses

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2286904
Email: gerardo.giaretta@telecomitalia.it

Ivano Guardini
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2285424
Email: ivano.guardini@telecomitalia.it

Elena Demaria
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2285403
Email: elena.demaria@telecomitalia.it

Michele La Monaca
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2285729
Email: michele.lamonaca@telecomitalia.it

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France
Email: julien.bournelle@int-evry.fr

Maryline Laurent-Maknavicius
GET/INT
9 rue Charles Fourier
Evry 91011
France
Email: maryline.maknavicius@int-evry.fr

Intellectual Property Statement

Full Copyright Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.