3GPP TR 33.822 V8.0.0 (2008-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security aspects for inter-access mobility between non 3GPP and 3GPP access network
(Release 8)

Keywords
3GPP, access network, Security

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x   the first digit:

1   presented to TSG for information;

2   presented to TSG for approval;

3   or greater indicates TSG approved document under change control.

y   the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z   the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This document studies the security architecture, i.e. the security features and the security mechanisms for inter-access mobility between 3GPP access system and non-3GPP access systems. For the general architecture for inter-access mobility cf. TR 23.882. This report is meant to provide more detail on the security aspects of inter-access mobility.

The scope should be extended to the mobility between two non-3GPP access systems, which interwork with 3GPP core entities. An example would be the mobility between two WLAN access systems providing 3GPP IP access.

Disclaimer: This TR reflects the discussions held in 3GPP SA3 while 3GPP SA3 was working towards TS 33.402 [14]. This TR may therefore be useful to better understand the basis on which decisions in TS 33.402 [14] were taken, and which alternatives were under discussion. However, none of the text in this TR shall be quoted as reflecting 3GPP's position in any way. Rather, 3GPP's position on security for non-3GPP access to EPS is reflected in the normative text in TS 33.402 [14]. Information in the TR may be inaccurate and outdated. One example of outdated text can be found in clauses 4.1 and 4.2 on alternatives for authentication protocols. The choices of authentication protocols finally made by 3GPP can be found in TS 33.401 [13] and TS 33.402 [14] respectively.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1]   3GPP TR 23.882: "3rd Generation Partnership Project; 3GPP System Architecture Evolution: Report on Technical Options and Conclusions".

[2]   3GPP TS 33.234: "3rd Generation Partnership Project; Wireless Local Area Network (WLAN) interworking security".

[3]   3GPP TS 29.061: "3rd Generation Partnership Project; Technical Specification Group Core Network; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[4]   3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[5]   "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", draft-ietf-mobike-protocol-03.txt, Sep 2005.

[6]   RFC 3957 "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4".

[7]   "NETLMM protocol", draft-giaretta-netlmm-dt-protocol-00.txt, June 2006.

[8]   RFC 4285 "Authentication Protocol for Mobile IPv6".

[9]   "Mobile IPv6 Bootstrapping for the Authentication Option Protocol", draft-devarapalli-mip6-authprotocol-bootstrap-03.txt, September 2007.

[10]   "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", draft-ietf-dime-mip6-split-05.txt, September 2007.

[11]   "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-06.txt, September 2007.

[12]   RFC4832 "Security threats of network based mobility management".

[13]   3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[14]   3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

3   Definitions, symbols and abbreviations

3.1   Definitions

For the purposes of the present document, the following apply:

Access network: one of following access network: GPRS IP access, WLAN 3GPP IP access, WLAN Direct IP access LTE, WiMax, etc.

Data origin authentication: The corroboration that the source of data received is as claimed.

WLAN 3GPP IP Access: Access to an IP network via the 3GPP system.

WLAN Direct IP Access: Access to an IP network is direct from the WLAN AN.

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards.

Trusted Access: A non-3GPP IP Access Network is defined as a "trusted non-3GPP IP Access Network" if the 3GPP EPC system chooses to trust such non-3GPP IP access network. The 3GPP EPC system may choose to trust the non-3GPP IP access network operated by the same or different operators, e.g. based on business agreements. Specific security mechanisms may be in place between the trusted non-3GPP IP Access Network and the 3GPP EPC to avoid security threats. The decision whether a specific non-3GPP IP Access Network is trusted or untrusted is up to the 3GPP EPC operator, and is not based on the specific link-layer technology adopted by the non-3GPP IP Access Network.

Source access system: in handover situations, this is the access system, from which the UE is handed over.

Target access system: in handover situations, this is the access system, to which the UE is handed over.

3.2   Symbols

For the purposes of the present document, the following symbols apply:

Gi	Reference point between GPRS and an external packet data network
Wi	Reference point is similar to the *Gi* reference point, applies to WLAN 3GPP IP Access
Wm	Reference point is located between 3GPP AAA Server and Packet Data Gateway respectively between 3GPP AAA Proxy and Packet Data Gateway
Wu	Reference point is located between the WLAN UE and the PDG. It represents the WLAN UE-initiated tunnel between the WLAN UE and the PDG
Gi+/Wi+	Mobile IP signalling and bearer plane between the Gateway (i.e. GGSN or PDG) and the MIP HA;

3.3   Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication Authorisation Accounting
AN	Access network
APN	Access Point Name
BSF	Bootstrapping Function
DS-MIPv6	Dual stack MIP
FA	Foreign Agent
GBA	Generic Bootstrapping Architecture

GGSN	Gateway GPRS Support Node
HA	Home agency
HN	Home network
IP	Internet Protocol
IPSec	IP Security protocol
I-WAN	Interworking Wireless Local Area Network
MIP	IP mobility
MOBIKE	IKEv2 Mobility and Multihoming Protocol
MS	Mobile Station
MN	Mobile Node
NAI	Network Access Identifier
NAT	Network Address Translation
NAF	Network Application Function
NETLMM	Network-based localized mobility management
PDG	Packet Data Gateway
PDP	Packet Data Protocol
RFC	Request For Comments
RRQ	MIPv4 Registration Request
RRP	MIPv4 Registration Response
SAE	System Architecture Evolution
SGSN	Serving GPRS Support Node
SPI	Security Parameter Index
URI	Uniform Resource Identifier
USIM	UMTS subscriber identity module
UE	User Equipment

4 Authentication protocols across access systems

Editor's note: it will be decided later if this section is needed in the final report.

It is assumed that an SAE user has a USIM which is used as user credential in authentication.

Authentication protocols are assumed to be run between the UE and an authentication server in the home network. It is likely there will always be a 3G AAA server to terminate authentication protocols in SAE, but this is still to be decided by SA2 (i.e. it is still to be decided whether always AAA protocols, e.g. DIAMETER, will be used to carry authentication data, or whether MAP may still be used). When AKA is used then the 3G AAA server will interface with a 3G Authentication Centre.

Even for one user, the type of authentication protocol depends on the type of access network. E.g. for I-WLAN EAP-AKA may be used, whereas for UTRAN UMTS AKA will be used.

4.1 UMTS AKA

UMTS AKA will be used across UTRAN. It is still to be decided by SA3 whether UMTS AKA or EAP-AKA will be used over LTE.

4.2 EAP-AKA

EAP-AKA may be used across I-WLAN and for WiMAX.

4.3　　Others

5　　Establishment of security contexts in the target access system

Each type of access system may require there own security contexts, which may need to be available to protect the access network. An example is an MSK key in a WLAN access system using an EAP method for authentication and key agreement. The MSK is then used to derive further keys.

An example of an access system more complex than WLAN and requiring more security contexts to be set up is WiMAX. WiMAX does not only need keys for the protection of the link layer, but e.g. also keys to protect Mobile IP signalling of the WiMAX-internal Mobile IP (CMIP or PMIP) layer providing WiMAX-internal mobility, which is different from the SAE Mobile IP layer providing mobility between access systems, of which at least one is non-3GPP.

There may also be access systems, which do not require any security context, e.g. a DSL-based access system relying on physical security.

The establishment of these security contexts in the access system may be done in two ways:

with the support of SAE;

without the support of SAE.

5.1　　Establishment of security contexts with the support of SAE

In this case, the credentials the UE shares with the 3G AAA server are used to establish security contexts in the access system. An example of this case is I-WLAN Direct IP access, where the SIM or USIM are used to establish MSK required to protect the WLAN link layer. Another example is likely WiMAX: the WiMAX Forum is currently working on solutions for 3G-WiMAX interworking, which would allow to bootstrap WiMAX-internal security contexts from a key derived from a run of EAP-AKA between the UE and the 3G AAA server.

5.2　　Establishment of security contexts without the support of SAE

In this case, credentials other than those available in 3G networks are used to establish security contexts in the non-3GPP access system. An example of this case is WiMAX when WiMAX-specific credentials are used to set up IP connectivity across WiMAX. SAE plays no role in this set up, so the establishment of these security contexts is out of scope of SAE.

It is assumed that the SAE user always uses a USIM on UICC to perform mutual authentication and establish security contexts with the Home Network.

It is to be decided by SA3 whether a UE-PDG tunnel is required.

6 Establishment of IPsec tunnel between UE and PDG across the target non-3GPP access system (if required)

One of the two variants of the S2 interface in the SAE architecture, cf. TR 23.882, allows to connect an access system to the evolved SAE packet core via an IPsec tunnel between the UE and a PDG. WLAN 3GPP IP access is an example of the use of such a tunnel, but WLAN is not the only access system which may be connected in this way. This section deals with the roaming of a UE between an access system (old) to another access system (new), for the case that at least the target access system requires such a UE-PDG tunnel.

The level of security achieved in certain deployments of non-3GPP IP access networks though internal security mechanisms (including confidentiality, integrity protection, protection of signalling, key management, etc) of some such non-3GPP IP access networks may be trusted by the 3GPP Evolved Packet Core (EPC) operator. In such case, no additional security mechanisms (e.g. IPSec tunnels from the UE to the EPC) are required. in the sense that the non-3GPP IP access network can interwork with the 3GPP EPC without relying on an IPsec tunnel to the UE. Such non-3GPP IP access networks are referred to here as "trusted non-3GPP IP access networks". The decision whether a specific non-3GPP IP access network is trusted or untrusted is up to the 3GPP EPC operator and is not based on the specific link-layer technology adopted by the non-3GPP IP access network.

If the non-3GPP IP access network is trusted (i.e. based on business, roaming and interconnection agreements), the need for a PDG functionality to connect the non-3GPP IP access to the EPC is FFS.

6.1 The source access system has a UE-PDG tunnel

An example of this case is mobility between two I-WLAN 3GPP IP access systems. The problem to be solved is to retain the IPsec tunnel even when the IP address of the UE changes due to mobility.

There are two cases here: the PDG remains the same or the PDG changes.

If PDG remains the same, the existing IPsec tunnel could be maintained. In order to achieve this, a mechanism proposed in TR 23.882, Annex E, is MOBIKE. For MOBIKE to work, it is required that the PDG remains the same while the UE moves.

If the PDG changes, then it is not a matter of maintaining the IPSec tunnel, but creating a new one with the target PDG. In such case, the focus becomes the mechanisms on the S2 interface, not what happens between the new PDG and the UE.

Another possible solution to retain the IPsec tunnel when the PDG remains fixed would be the use of an IP mobility mechanism (e.g. Mobile IP). The Mobile IP Home Agent would have to be e.g. located between the PDG and the UE, but close to the PDG, ensuring that the outer IP address of the IPsec tunnel remains constant, even while the UE moves and acquires a new local IP address. The adoption of MIP for mobility is FFS.

If the PDG changes, then it is not a matter of maintaining the IPSec tunnel, but creating a new one with the target PDG. In such case, in addition, to the establishment of the new IPsec tunnel, the mobility of the PDG has to be handled by the S2 interface.

6.2 The source access system does not have a UE-PDG tunnel

An example of this case is mobility between a 3GPP access system, such as LTE or UTRAN, and an I-WLAN 3GPP IP access system. The problem to be solved is to set up the IPsec tunnel in the target system in an efficient way.

Neither MOBIKE nor an additional layer of Mobile IP will help here.

7 Security for IP based mobility

There may be several layers of Mobile IP being used in a complete SAE system, including access networks. E.g. there is a WiMAX-internal Mobile IP layer. The considerations in this section are concerned with the outermost such layer, where the related Home Agent 3GPP HA resides in the 3G network. It is still to be decided if the HA is located in the SAE anchor, cf. architecture in section 4.

7.1 General requirement

Major security threats related to IP mobility, when the procedures are not properly secured, are:

- IP address ownership needs to be verified else redirection attacks will happen

- Traffic sent to a target redirected elsewhere

- Attacker can blackhole traffic to a victim

- Attacker can insert itself on-path as a Man-in-the-Middle

- Redirecting traffic for someone to a victim

- Leads to (D)DoS (distributed denial of service) 3rd party bombing

- Consequently charging can be confused

- (D)Dos attack on mobility anchor

Key handling principle for inter-3GPP HO:

Before handover from EUTRAN to non-3GPP IP access network and/or from non-3GPP IP access network to EUTRAN, UE and EPS core network use the present key and the same key derivation function to derive the new key, which is to be used after handover.

(From S3-070732)

Some of the main problems that need to be considered when defining secuity context transfer optimizations for non-3GPP/3GPP handovers are:

- Security (avoiding negative impact on LTE/UMTS security)

- User privacy related to identity management

- AAA architecure misaligmnent between 3GPP and non-3GPP accesses

- Difficulty of defining a unique reference point for (secure) inter-access security context transfer.

- Possible standardization impact outside 3GPP (IETF, IEEE).

These shall be taken into account when looking at optimizations for handovers between 3GPP and non-3GPP accesses.

There are different kinds of make-before-break solutions using pre-authentication. This pre-authentication could take place either at the time of hand-over preparation, or (for e.g. single-radio terminals) the authentication could (perhaps) be prepared at the initial attach. It is an agreed working assumption that solutions based on pre-authentication should be the focus of the SA3 study for authentication optimizations for handovers between 3GPP and non-3GPP accesses

7.2   Host based Mobility

7.2.1   Security associations used with Mobile IP

Figure 1 gives an overview of the MIP security associations which need to be present irrespective of the version of
Mobile IP used. More security associations may be required for certain versions of Mobile IP. E.g. for Mobile IP v4
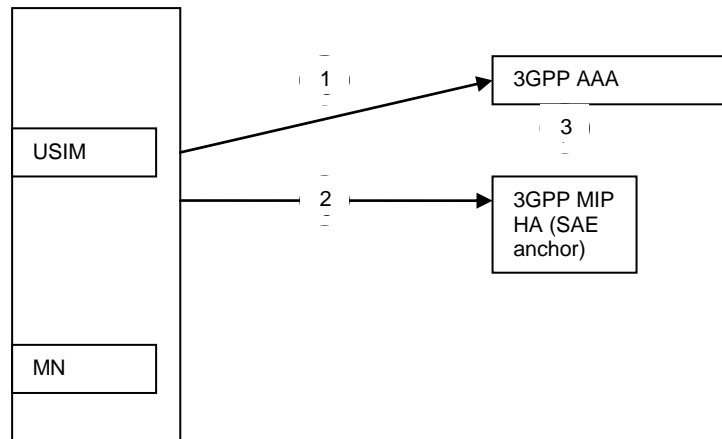with a Foreign Agent, security associations between MN and FA, and FA and HA are needed.

Figure 1: Overview of the security architecture for MIP

The needed security associations are:

-     A security association between the UE and 3GPP AAA. It is assumed that the 3GPP AAA in HPLMN is in
      charge of user authentication and authorization. This security association is based on a long-term secret.

-     A security association between the UE and 3GPP MIP HA. This security association is established dynamically.

-     A security association between 3GPP MIP HA and 3GPP AAA server in the same network. Typically, this
      security association is static. NDS/IP could be used when proxy AAA is used in roaming case. See TS 33.210 for
      more detail information [4].

7.2.2   Security protocols used with Mobile IP

1. The security association between the MN and 3GPP AAA is used for (mutual) authentication. In our context, the
    authentication protocol may be e.g. EAP-AKA. This protocol is independent of Mobile IP, but keys derived from
    a run of this protocol may be used for Mobile IP purposes.

2. The security association between the MN and 3GPP MIP HA is used for MIP signalling integrity protection. The
    protocols used depend on the version of Mobile IP. To give examples:

    MIPv4: Home agent and mobile nodes shall be able to perform message authentication according to RFC 3344.
    MN-HA key agreed between HA and MN during MIP authentication is used to compute the digest in the
    Mobile-Home Authentication Extension according to RFC3344. The Mobile-Home Authentication Extension is
    used to provide integrity of signalling between Mobile Node and Home Agent. HMAC-MD5 shall be used as
    authentication algorithm with a key size 128 bit. HA will compute the UDP payload (RRQ or RRP data), all
    prior extensions, the type, length and SPI of the extension with MN-HA key in MIP Req-resp. MN uses with
    HMAC-MD5 to verify the received message from HA.

    For MIPv4 with a foreign agent, more security associations are needed, as mentioned in the previous subsection.
    RFC3344 can also be used for these. The foreign agent shall be able to support message authentication using
    HMAC-MD5 and key size of 128 bits, with a key distribution mechanism (FFS).

MIPv6: IPsec is specified as the means of securing signalling messages between the Mobile Node and Home Agent for Mobile IPv6 (MIPv6) in RFC3776. RFC4285 proposes an alternate method for securing MIPv6 signalling messages between Mobile Nodes and Home Agents. The alternate method consists of a MIPv6-specific mobility message authentication option that can be added to MIPv6 signalling messages. The alternate method is entirely based on shared secrets and does not use IPsec.

3. The security association between 3GPP MIP HA and 3GPP AAA server in the same network is used to securely transport the MN-HA keys from AAA server to MIP HA. It may not be needed if the interface between AAA server and HA is secured by other means.

Home agent and mobile nodes may perform message authentication whenever it is needed.

7.3   Bootstrapping of Mobile IP parameters

7.3.1   General

It would be undesirable for SAE if the UE had to obtain security credentials to be used specifically for Mobile IP signalling security. Rather, the security associations required for Mobile IP should be able to be derived from security credentials already available. In the case of SAE, this means that it should be possible to derive the security associations required for Mobile IP from the USIM.

Authentication between the MN and the network shall be performed as. A subscriber, who wants to use MIP, will have its subscriber profile located in the 3GPP AAA in the Home Network. The subscriber profile will contain information on the subscriber that may not be revealed to an external partner, At MIP registration , during a change of location between different access networks by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not.

7.3.2   RFC3957 used in conjunction with GBA

NOTE: this subsection applies only to MIPv4.

MN-HA key generation & distribution based on RFC 3957. This method uses pre-shared secret between MS and AAA server to establish a shared secret between MS and HA and / or MS and FA.
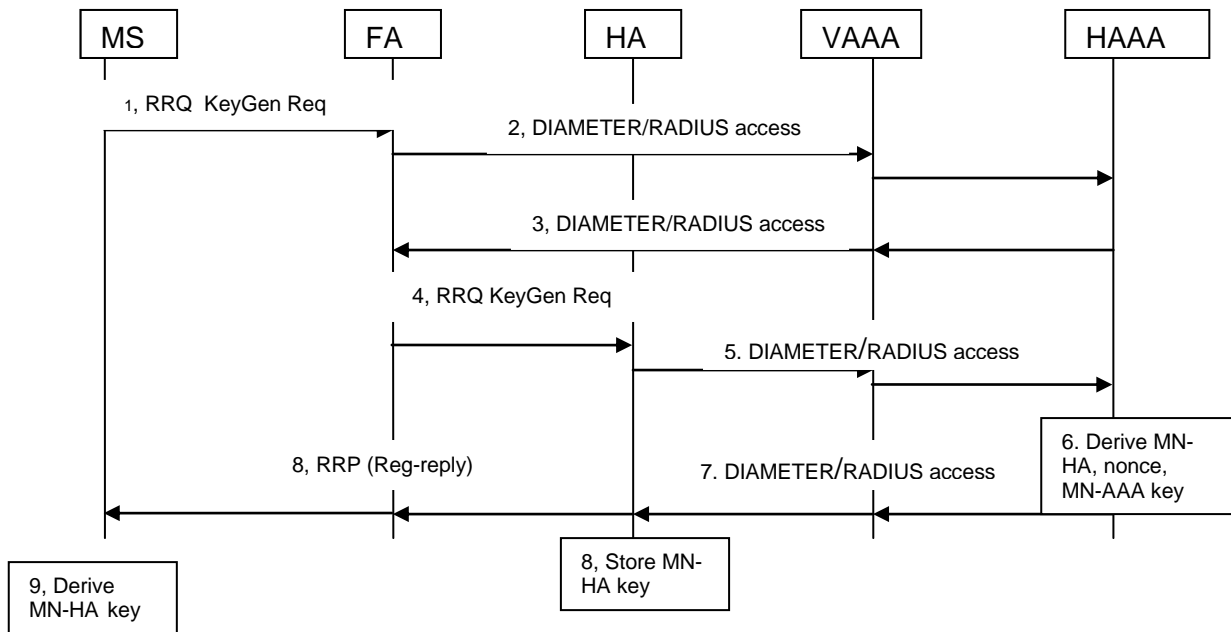
Figure 2: MN-HA key generation & distribution

1. During initial MIPv4 registration, MS includes a new extension (called the MN-HA Key Generation Nonce Request extension [RFC 3957]) in RRQ to request for a nonce from HAAA. The RRQ also contains the MS's credential in the MN-AAA authenticator extension.

2. FA sends DIAMETER/RADIUS Access-Request to HAAA to authenticate the MS credential.

3. If the MS is authenticated successfully, the HAAA returns DIAMETER/RADIUS Access-Accept.

4. FA forwards the RRQ to the HA.

NOTE: If co-located care-of address mode is used, then RRQ message will be sent from MS to HA directly without FA in above picture

5. HA sends DIAMETER/RADIUS Access-Request to HAAA. In case of Roaming, the message will send through VAAA to HAAA. The DIAMETER/RADIUS Access-Request contains the MN-HA SPI attribute to request for a MN-HA key to HAAA that the MN-HA key needs to be derived. The HA may include the MS credential in the DIAMETER/RADIUS Access-Request.

Editor's note: it's FFS if it's possible for a HA in the visited network.

6. HAAA selects a nonce and derives the MN-HA key from the MN-AAA shared secret, MS's NAI, and the nonce.

7. HAAA returns DIAMETER/RADIUS Access-Accept that contains the MN-HA key and the nonce.

8. The HA sends RRP with a new extension (called the Generalized MN-HA Key Generation Nonce Reply Extension [RFC 3957]) carrying the key generation nonce, and the MN-HA authenticator computed from the MN-HA key. The new extension must precede the MN-HA authenticator. (FA forwards the RRP to the MS)

9. The MS derives the MN-HA key and uses it to verify the MN-HA authenticator in the RRP.

One possible way is to use GBA in conjunction with RFC 3957. In this case HAAA is associated with NAF.
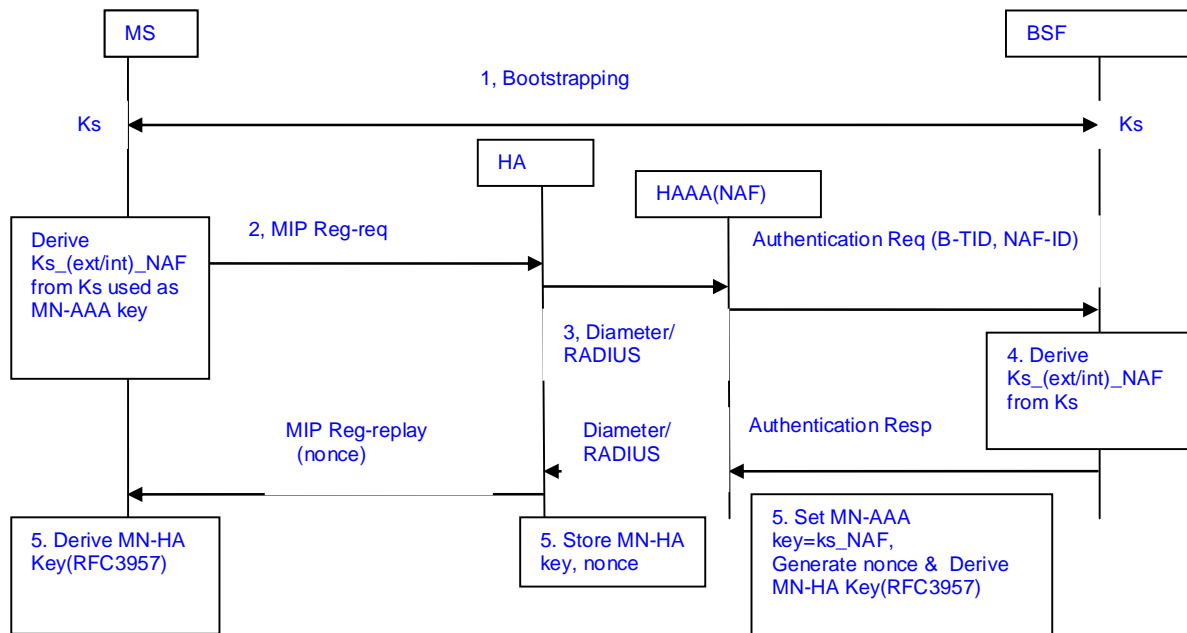
Figure 3: Using GBA to derive and distribute MN-HA Keys (HAAA as NAF)

Generic Bootstrapping Architecture (GBA) allows bootstrapping of shared secrets between a UE/MN and the home network (Bootstrapping Service Function, BSF), which can then be used to derive further shared secrets to be used between MS and a Network Application Function(NAF).

Two options for using GBA in the inter access mobility authentication are considered:

- using GBA to derive the MN-HA Keys, in which case the HA is used as NAF and.

- using GBA to provision MN-AAA Keys, in which case HAAA is used as a NAF.

Figure 5 shows how GBA could be used to derive and distribute MN-HA Keys when HAAA as NAF, i.e. HAAA is associated with a Network Application Function (NAF).

1. The MN performs a bootstrapping procedure with the BSF and generates a (master) shared secret, Ks. Bootstrapping procedure is performed between the UE/MS and the BSF (which is located in the home network). During bootstrapping, mutual authentication is performed between the MS and the home network, and a bootstrapping key, Ks, will be generated by both the UE/MS and the BSF. Associated with the Ks include a Bootstrapping Transaction Identifier (B-TID) and a lifetime of the Ks.

NOTE: This procedure is only needed during initial registration (and it can be done before the MIP registration). It is not repeated at every HO (Handover). The only time it needs to be repeated is when the key is about to expire. But even in this case, the GAA procedure is done "offline"—i.e. the next MIP registration does not need to wait for GAA procedure to complete.

2. MN can then start MIP related signalling with the HA, which in turn contacts the HAAA.

3. HA then contacts to HAAA using Diameter/RADIUS. **Note**: in the baseline document only RADIUS message is shown in the figure and the text. However, both Diameter and RADIUS can be used.

4. The HAAA, acting as a NAF, does not have the MN-AAA key, as the MN-AAA key is supposed to be generated by the BSF using Ks and other inputs to a KDF (key derivation function). Therefore, the HAAA will contact the BSF and fetch the MN-AAA key (Ks_(ext/int)_NAF of the HAAA) needed to authenticate the MN.

5. MN-HA keys are then derived from the MN-AAA Key using RFC 3957.

NOTE: If foreign agents (FA) are used, then foreign agent use Diameter/RADIUS to communication with HAAA.

Editor's note: it needs to check how to send the B-TID in MIP registration message.

7.3.3 Use GBA to generate MN-HA key

NOTE: This subsection applies to MIPv4and MIPv6.

In this alternative authentication method, HA is associated with NAF.

Home Agent (HA) is associated with a NAF, and Ks_(ext/int)_NAF would be used as MN-HA key: the MN performs a bootstrapping procedure with the BSF and generates a (master) shared secret, Ks. After that, the MN can start MIP related signalling with the HA, which in turn contacts the BSF to fetch MN-HA key.
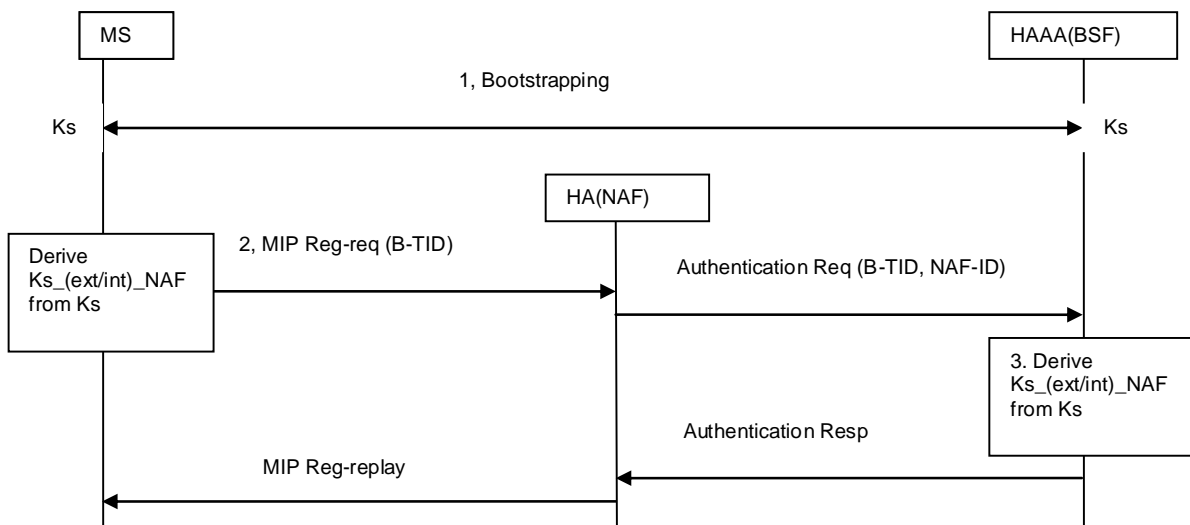

Figure 4: Overview of GBA operations

1. Bootstrapping procedure is performed between the UE/MS and the BSF (which is located in the home network). During bootstrapping, mutual authentication is performed between the MS and the home network, and a bootstrapping key, Ks, will be generated by both the UE/MS and the BSF. Associated with the Ks include a Bootstrapping Transaction Identifier (B-TID) and a lifetime of the Ks.

NOTE: This procedure is only needed during initial registration (and it can be done before the MIP registration). It is not repeated at every HO (Handover). The only time it needs to be repeated is when the key is about to expire. But even in this case, the GAA procedure is done "offline"—i.e. the next MIP registration does not need to wait for GAA procedure to complete.

2. Once bootstrapping is completed, UE/MS can make use of the bootstrapped security association with a network application server, called the Network Application Function (NAF). To do so, the UE/MS communicates with the NAF. The UE/MS conveys to the NAF the B-TID.

3. The UE/MS derives the application specific session keys Ks_(ext/int)_NAF using a pre-defined key derivation function (KDF), with Ks, identifier of the NAF (NAF_Id), as well as other information as input. Upon receiving the request from UE/MS in step 2, the NAF contacts the BSF over the Zn to request the Ks_(ext/int)_NAF. The NAF provides the B-TID received from the UE/MS, and provides its own identity (NAF_Id). The BSF derives the Ks_(ext/int)_NAF in the same way as the UE/MS, and returns the derived key to the NAF. The Ks_(ext/int)_NAF can then be used as the shared secret between the MS and the NAF for any further security operations.

NOTE: If foreign agents (FA) are used, then foreign agent implements GAA NAF to get the MN-FA key.

7.3.4   Use partial GBA to derive MN-HA Keys

NOTE: This subsection applies to MIPv4 and MIPv6.

GBA was designed for a situation where a UE wants to securely access potentially many application servers (NAFs), while having to be authenticated to the home network (and consume authentication vectors) in the Ub protocol run only once. Furthermore, the NAFs the UE wants to access may and need not be known at the time of the Ub protocol run. These requirements do not apply to MIP bootstrapping: the number of MIP servers with which the UE needs to share a key is limited to one, namely the Home AAA or Home Agent (when no Foreign Agent is used), and two, when an FA is used (or three, when two FAs are involved in a handover situation). In addition, the addresses of HA and FA cannot be chosen by the UE any time later, but are assigned by the home network (HA) and the visited network (FA), respectively. Therefore, the full functionality of GBA may not be needed.

A disadvantage of the use of GBA for MIP bootstrapping is that the HA, and, if applicable, the FA, need to support NAF functionality. An off-the-shelf HA or FA does not do that.

Editor's note: the intention of this GBA extension is a subset of GBA and should not be a problem.

We consider two cases below. For both cases, the following is assumed:

-    a UE has to run the Ub protocol with the BSF before starting MIP registration.

-    the BSF is integrated with the AAA server (as in the current baseline document).

-    the AAA server distributes keys to HA and FA using standard AAA procedures (for MIPv4: RFC4004: DIAMETER Mobile IPv4 application, and for MIPv6: draft-ietf-dime-mip6-split-03), and does not use the Zn interface.

-    the distributed keys are used with the Mobile IPv4 and Mobile IPv6 authentication mechanisms defined in RFC 3344 and RFC 4285 respectively

Editor's note: it's FFS whether RADIUS extension also needs to be supported.

With these assumptions, HA and FA can be off-the-shelf, and need not be GBA-aware. The Ua and the Zn interfaces are not needed.

Case 1:   HA and FA addresses and/or names are acquired by the UE independently of the Ub protocol run

In this case, the BSF and the UE derive keys Ks_(ext/int)_NAF to be shared between UE and HA, and UE and FA, respectively, as specified in TS 33.220.

Editor's note: no change to Ub in Case 1.

Case 2:   The HA address and/or name is acquired by the UE as part of the Ub protocol run

In this case, the BSF can send the FQDN, and possibly also the IP address, of the HA to the UE in a new element in the XML body of the "200OK" message, which is the last message in the Ub protocol run. This provides an alternative to SAE HA address assignment. Note that it may not be obvious for all access systems how to let the UE acquire the SAE HA address.

Editor's note: the Ub interface will be affected in Case 2.

The FA address needs to be acquired by the UE locally.

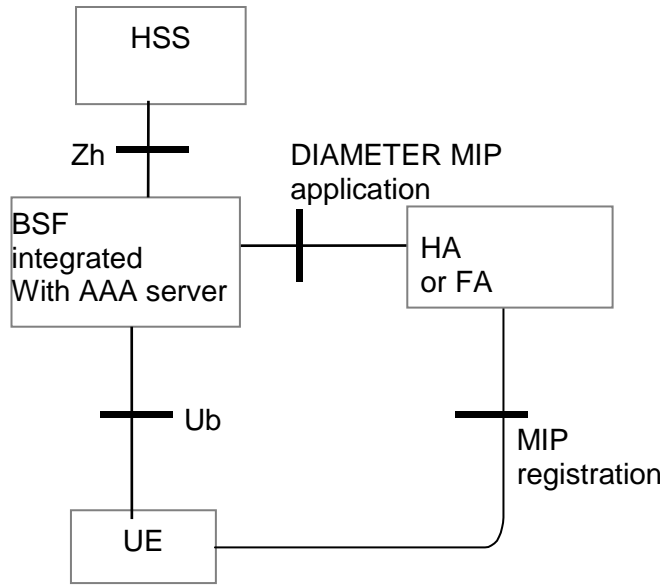The use of partial GBA for MIP bootstrapping is captured in Figure 5.

Figure 5: Partial GBA for MIP bootstrapping

7.3.5   Using IKEv2

Authentication between the MN and the network and IPsec SA setup between the MN and the HA for MIPv6 shall be performed using IKEv2 as defined in the IETF draft [draft-ietf-mip6-bootstrapping-split-02.txt]. In SAE, the home agent communicates with the AAA server to perform mutual authentication. The IKEv2 authentication is performed using EAP-AKA.
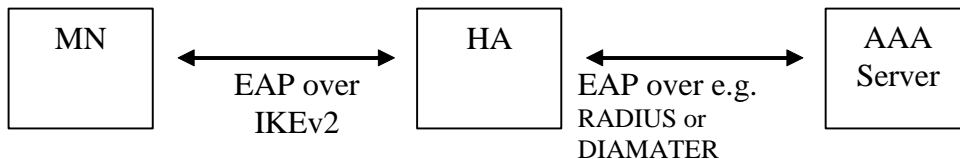

Figure 6: MN-Network authentication and MN-HA IPsec SA setup for MIPv6

Editor's note 1:   adding relatively heavy protocol of IKEv2 should be considered to be for further study if cost efficiency is in appropriate level.

Editor's note 2:   this is only one of multiple different options.

Editor's note 3:   both I-WLAN scenarios 2 and 3 should be studied

(From S3-070820)

The first procedure that must be performed by the MN is the discovery of the HA address, which in case of EPS is the IP address of the PDN GW.

As soon as the Mobile Node has discovered the PDN GW address, it establishes an IPsec Security Association with the Home Agent itself through IKEv2. The detailed description of this procedure is provided in RFC4877. The IKEv2 Mobile Node to Home Agent authentication is performed using Extensible Authentication Protocol (EAP).

When the Mobile Node runs IKEv2 with its Home Agent, it shall request an IPv6 Home Address through the Configuration Payload in the IKE_AUTH exchange by including an INTERNAL_IP6_ADDRESS attribute. When the Home Agent processes the message, it allocates a HoA and sends it a CFG_REPLY message. The IPv6 Home Address allocation through IKEv2 allows to bind the Home Address with the IPsec security association so that the MN can only send Binding Updates for its own Home Address and not for other MN's Home Addresses.

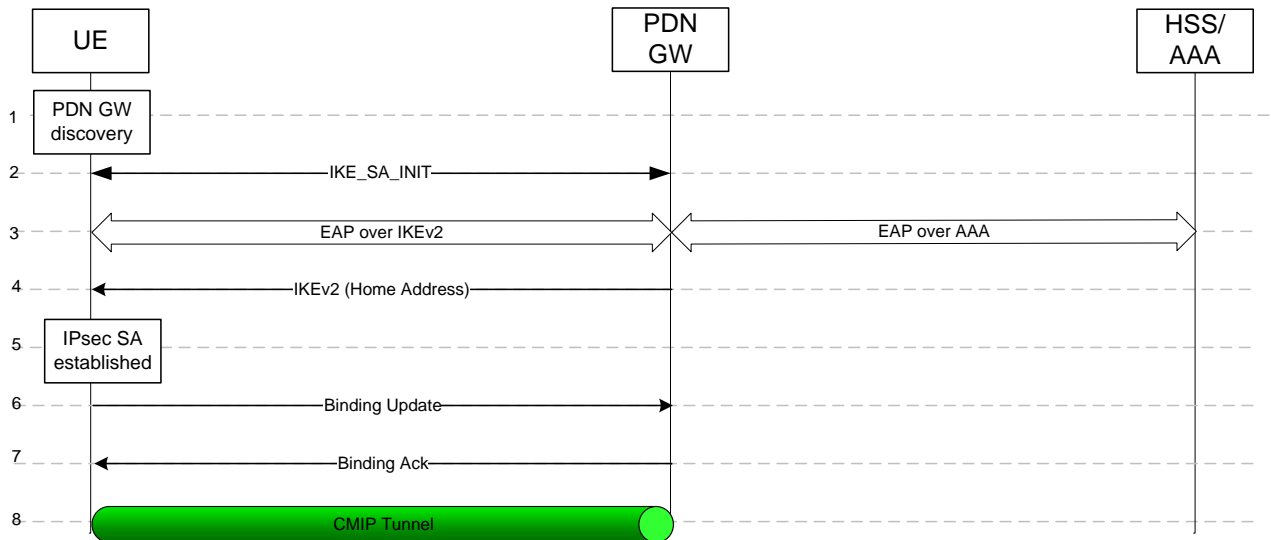Figure 7 provides the flow for the initial DS-MIPv6 bootstrapping.

Figure 7: DS-MIPv6 bootstrapping based on IKEv2

1) The UE discovers the PDN GW address based on the procedure specified in 23.401.

2) The UE starts an IKEv2 exchange with the PDN GW. The first part of this exchange is an IKE_SA_INIT exchange.

3) The UE indicates that EAP is used for IKEv2 authentication and an EAP exchange is performed. EAP is carried over IKEv2 between the UE and the PDN GW and over the AAA protocol between the PDN GW and the AAA server.

4) During the IKEv2 exchange, the PDN GW allocates an IPv6 Home Address and send it to the UE in a IKEv2 Configuration Payload.

5) As a result of the previous steps, an IPsec SA is established to protect DS-MIPv6 signalling.

6) The UE sends the MIP Binding Update message to the PDN GW.

7) The PDN GW processes the binding update. The PDN GW sends the MIP Binding Ack to the UE.

8) As a result of the above steps a MIPv6 tunnel is established and the UE can start using its home address at the application level.

7.3.6   Security bootstrapping for DS MIPv6 using MIP options

(From S3-070748)

This procedure uses the MIP authentication options defined in RFC4285 [8] to provide authentication of Binding Update and Binding Acknowledgement messages, namely the

- MN-HA Mobility Message Authentication Option and the

- MN-AAA Mobility Message Authentication Option.

The AAA Mobility Message Authentication Option is used when the MN and the HA do not yet have a shared key, i.e. in the situation requiring bootstrapping of the MN-HA key.

It is assumed that the MN and the AAA server share a long-lived security association.

   NOTE: It is ffs whether there is a need to dynamically generate the MN-AAA key and, if so, how to do it.
          Alternatives would include derivation during network access authentication and GBA.

The MN-HA key is derived from the MN-AAA key and a nonce. The nonce is requested by the MN in a Key Generation Nonce Request option and provided by the AAA server to the MN in a Key Generation Nonce Reply option. These options are described in draft-devarapalli-mip6-authprotocol-bootstrap [9].

NOTE: Instead of using a nonce for generating the MN-HA key from the MN-AAA key, also the timestamp from the Mobility Message Replay Protection Option, cf. below, could be used. This is ffs.

The HA may provide a Home Address to the MN using the Home Address Options defined in draft-devarapalli-mip6-authprotocol-bootstrap [9].

The communication between the Home Agent and the AAA server is based on DIAMETER extensions described in draft-ietf-dime-mip6-split [10]. This communication is assumed to be authenticated (integrity-protected).
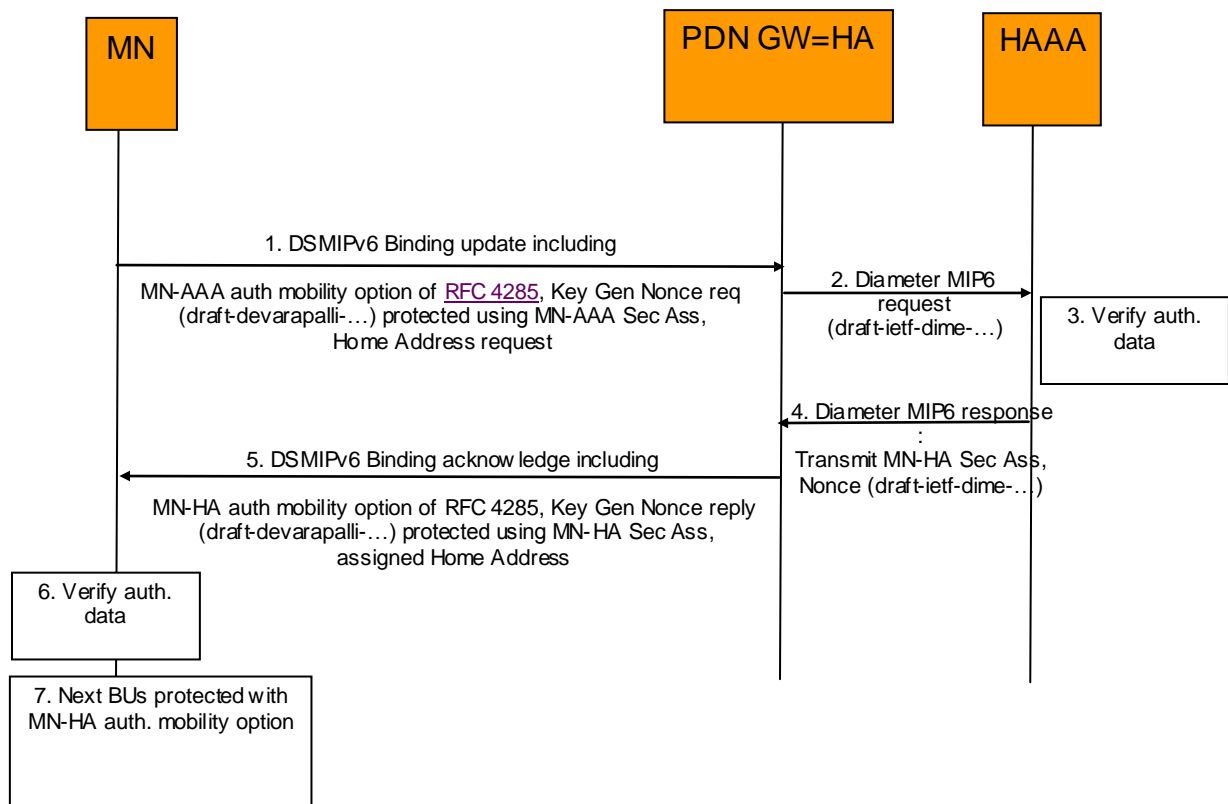
Figure 8: Bootstrapping using Mobile IP options

Description of the information flow in Figure 8:

1. When the Mobile Node (MN) does not yet share a key with the Home Agent (HA) the MN sends a DSMIPv6 Binding Update (BU) including the MN-AAA authentication mobility option. The MN also includes a Key Generation Nonce Request Option. If the MN does not yet have a Home Address (HoA) it also includes the Home Address Request Option in the BU. The MN shall include the Mobility Message Replay Protection Option defined in RFC 4285 [8] containing a timestamp.

2. When the Home Agent receives a BU with the MN-AAA mobility message authentication option, the HA forwards the BU to the AAA server for authentication.

3. The AAA server authenticates the BU by verifying the message authentication code in the MN-AAA authentication mobility option, using the MN-AAA shared key and the timestamp in the Mobility Message Replay Protection Option.

4. Upon successful authentication of the BU, the AAA server sends the parameters of the MN-HA security association (key, algorithm) to the HA. The AAA server also returns a nonce and algorithm identifier in the Key Generation Nonce Reply Option.

5. The HA sends a Binding Acknowledge (BA) message protected with the MN-HA security association received from the AAA server to the MN. The HA forwards the Key Generation Nonce Reply Option as part of the BA. The HA also includes the Assigned Home Address Option in the BU if the MN requested a HoA. The HA checks the validity of the timestamp and, if necessary, includes an indication of a timestamp mismatch, as described in RFC 4285 [8]. In the latter case, HA deletes the MN-HA security association after sending the BA.

6. The MN generates the MN-HA key from the MN-AAA key and the nonce. The MN then verifies the BA using the MN-HA authentication mobility option. If the BA contains an indication of a timestamp mismatch the MN resends the BU from step 1, but with the message authentication code in the MN-AAA authentication mobility option computed over the corrected timestamp.

7. For subsequent BUs, the MN uses the established MN-HA security association and does not include an MN-AAA authentication mobility option.

7.4 Network based Mobility

7.4.1 PMIP

7.4.1.1 Introduction

This section looks at how PMIP messages need to be protected within the Evolved Packet Core and how PMIP protection needs to be handled if the PMIP messages originate from a trusted non-3GPP network node.

This analysis is based on draft-ietf-netlmm-proxymip6-06.txt [11] from which in particular the sections 4 and 11 have been used from a security viewpoint.

7.4.1.2 Overview of PMIP usage in 3GPP

(From S3-070756)

PMIPv6 defines a MAG (Mobile Access Gateway) and an LMA (Local Mobility Anchor) from which the LMA will be integrated in the PDN Gateway or Serving Gateway (for the roaming case).
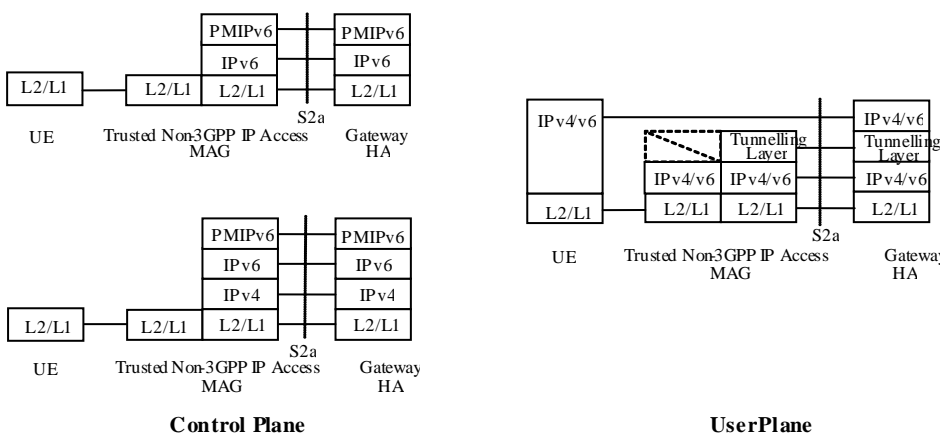

Figure 9: Protocols for MM control and user planes of S2a for the PMIPv6 option

TS 23.402v130 section 5 is relevant in this respect and specifies that PMIPv6 may be used on following reference points:

*   **S2a**: Between a node in the trusted non-3GPP access network (Foreign agent) and the LMA (Home Agent)

*   **S2b**: Between the ePDG and the LMA (Home Agent).

TS 23.402v130 section 4.2.1 mentions the use of PMIP based **S5** reference point between the Serving Gateway and the PDN Gateway. The S5 reference point may also apply GTP, and is an intra-operator interface. PMIP usage over S5/S8b is currently included in the description of PMIP use over S2b, and (see section 5.4.2.4.3 TS 23.402) in case of roaming, the S-GW is the LMA for PMIP procedure in S2b between the ePDG and the S-GW and the PDN GW is the LMA for PMIP procedure in S8b between the S-GW and the PDN GW. In addition, PMIP over S5/S8b is discussed in section 5.4.2.6 TS 23.402 for E-UTRAN access.

7.4.1.3   PMIP trust model

PMIPv6 is an IETF based network-based mobility management mechanism, and has applied the same trust model properties as the use of GTP for mobility management in UMTS and the EPC (for the S5 and S2b reference points). This means the MAG i.e. the Serving Gateway (S5) or ePDG (S2b), is sufficiently trusted by the LMA to register only those Mobile Nodes that are attached.

However when the MAG is located in a trusted non-3GPP network (S2a), there is a little bit of a difference to the current 3GPP or PMIPv6 draft [11] trust model where a 3GPP network component (SGSN, S-GW) is trusted to register only attached MNs. Here, the MAG could e.g. be located in a WLAN AP which can much more easily be tampered with than an SGSN or S-GW. The implication of this scenario is for ffs (see also proposed decision at the end of this section).

The trust between the LMA and the MAG is verified by the LMA by allowing only those MAGs to perform Binding Updates which are known by the LMA i.e. by the use of IKEv2 authentication. This measure defends against a Network Node trying to impersonate another MAG, and thus will protect against Denial-Of-Service attacks from the Mobile Node's viewpoint.

The PMIPv6 draft [11] recognizes the threat of a compromised MAG that would send PMIP messages on behalf of a Mobile Node with a Mobile Node not present on the local link. From section 11 of [PMIPv6 draft]:

"To eliminate the threats related to a compromised mobile access gateway, this specification recommends that the local mobility anchor before accepting a Proxy Binding Update message for a given mobile node, should ensure the mobile node is definitively attached to the mobile access gateway that sent the binding registration request.

The issues related to a compromised mobile access gateway in the scenario where the local mobility anchor and the mobile access gateway in different domains, is outside the scope of this document. *This scenario is beyond the applicability of this document.*"

The last sentence from the extract is an indication for the fact that the S2a use is not covered by PMIPv6 draft [11] and needs additional considerations.

Although required by PMIPv6 draft [11] it is unclear how the LMA should be able to verify that the MN has attached, rather this seems to be a property of the PMIP model that the MAG is trusted to apply those requirements. The authorization mechanisms on the MAG-LMA interfaces are inadequate for this.

The effect of a potential misuse by the MAG could be limited to those MAGs on which the Mobile Node is authorized to attach. This authorization shall then be verified by the LMA. However, this explicit authorization-check may be cumbersome to administrate per user (and therefore not very effective), and if not administrated per user but per roaming partner, the authorization check rather takes place between the MAG and the LMA (via the lack of shared secrets for IKEv2, or certificate authorization checks), and this fits the PMIP trust model applying to S5 and S2b.

Extending PMIPv6 by involving the UE in order to produce a fresh user involvement on the MAG that can be used towards the LMA, is a contradiction to the design guidelines of PMIPv6: "This protocol enables mobility support to a host without requiring its participation in any mobility related signaling." Furthermore verifying the user involvement would also increase the amount of signaling needed. So there is a trade-off between trust/security and amount of signaling.

NOTE 1: For the other network based mobility management protocols e.g. GTP this has worked well in the past. The operator should be able to trace down suspicious registrations as long as the links are secured (physical or by NDS/IP).

In case of S5, the node implementing the MAG may already be trusted to receive an EPS security context for a user, without proof of user involvement.

NOTE 2: In case S-GW and MME are implemented on the same physical node.

The risk caused by a misuse of the received key material is greater than the risk due the use of the PMIPv6 trust model. Verifying user involvement during mobility management registration would need to involve an additional authentication verifiable by the LMA only such that the compromised MAG cannot impersonate the user, where then we are back to the DSMIPv6 solution.

Conclusion:

a) use PMIPv6 as defined by IETF [draft-ietf-netlmm-proxymip6-06.txt] for S5 and S2b

b) if the trust relation between the MAG and the LMA is not there then additional security measures are needed. These security measures are for ffs.

7.4.1.4 Security measures on the Reference points between the LMA and the MAG that have a trust relation

PMIPv6 draft [11] section 4 recommends the use of IPsec ESP in Transport Mode (RFC4303) as default security mechanism for integrity protection and data origin authentication for PMIP messages and IKEv2 end-to-end between the MAG and the LMA to establish IPsec security associations. Confidentiality protection of PMIP messages is not required.

Section 5.5.1 allows the use of one security tunnel between the MAG and the LMA instead of a dynamic set-up.

"The bi-directional tunnel is established after accepting the Proxy Binding Update request message. The created tunnel may be shared with other mobile nodes attached to the same mobile access gateway and with the local mobility anchor having a Binding Cache entry for those mobile nodes. Implementations MAY choose **to use static tunnels** instead of dynamically creating and tearing them down on a need basis."

Therefore alternatives to the IKEv2 usage like NDS/IP (TS 33.210) should still be possible (RFC 2406 and IKEv1) and can provide the same security services.

The only difference is the hop-by-hop approach with SEGs (requiring tunnel mode towards the SEG), which should not be a problem in viewpoint of security if the network owning the SEG and the LMA is sufficiently trusted. The use of TS 33.310 is needed when LMA and MAG belong to a different operator.

The PDN gateway may already implement IKEv1/IPsec for protecting the signaling towards the AAA/HSS in case of DSMIPv6 and may already implement IKEv2 in case that such mechanism would be selected for DSMIPv6 protection towards the Mobile Node (which is for ffs at SA3#49). The ePDG already requires IKEv2 implementation towards the UE.

Conclusion:

SA3#49 agreed that the choice between IKEv1 (as defined by NDS/IP) or IKEv2 (as proposed by PMIPv2] for PMIP message protection between the MAG and the LMA needs further study

a) Both IKEv2 and IKEv1 can provide the necessary security features.

b) Referring to NDS/IP (TS 33.210) and NDS/AF (TS 33.310) allows a hop-by-hop security model.

c) The difference between RFC2406 [which is referred by NDS/IP] and RFC4303 [which is referred by PMIPV6] is not essential for the decision.

7.4.1.5 The need for using strong access authentication with Proxy Mobile IP

Clause 7.4.1.3 discusses the need for trust of the LMA in the correct operation of the MAG Trust in the MAG means that the LMA can be ensured that the operation of MAG is not somehow influenced by an attacker. Clause 7.4.1.4 discusses the security on the reference point between the MAG and the LMA. Security on this reference point ensures that PMIP messages are originating from a trusted entity, and that no attacker could tamper with them in transit. This subclause discusses an additional requirement for the secure operation of PMIP: strong access authentication. In the context of PMIP, the authentication scheme shall be considered sufficiently strong by all stakeholders involved, in particular by the operators of MAG and LMA. In EPS the LMA is the PDN GW owned by a 3GPP EPS operator. This implies that the authentication scheme shall satisfy also 3GPP security requirements, i.e. it shall use a USIM.

PMIP is based on the assumption that a MAG can securely identify which user is attached to the access network served by the MAG This secure identification is realised by access authentication. If access authentication was weak then an

attacker could impersonate a user in the access network. If this happened, a MAG would report in good faith to the LMA that a certain user was present in the access network, while in fact the attacker was present. This could result in Denial of Service to the impersonated user through the use of PMIP because all traffic destined to this user would then be routed to a wrong destination.

An impersonation attack exploiting a weakness in access authentication could occur by attacking any part of the access network. Neither the trusted operation of the MAG nor the security on the reference point between the MAG and the LMA would prevent such an attack if access authentication was weak. In this sense, the requirement of using strong access authentication with PMIP is complementary to the requirements addressed in clauses 7.4.1.3 and 7.4.1.4.

Section 4 of TR 33.922 requires USIM-based authentication also for non-3GPP access. Currently, AKA is the only authentication scheme known to use the USIM. As AKA-based authentication is considered sufficiently strong, also the requirement introduced in this subclause is considered fulfilled in EPS.

Conclusion：

When PMIP is used within EPS, strong access authentication is required. In EPS and as per clause 4 of TR 33.922, this requirement is fulfilled since the USIM-based authentication for non-3GPP access is mandated. The USIM-based authentication implies the use of the AKA protocol, which is considered sufficiently strong.

7.4.1.6   No trust relation between LMA and MAG on S2a

NOTE：This section describes the case when there is no trust relation between the MAG and the LMA. However, what this section describes is not aligned with the assumption of TS33.402v100 section 9.3.1.2.

7.4.1.6.1   Security risks

MAG lies in the trusted non-3gpp IP access system in S2a. There may be no trust relation between the MAG and the LMA since they may belong to different operators. In this case, a compromised MAG may make an attack to UE in other MAG's domain. Also, a compromised MAG may send fake PBU message to update the binding of UE who is served by other MAG. In this case,

-the victim UE cannot receive the data since the data is routed to the compromised MAG;

-the compromised MAG can eavesdrop the data of UE who is served by other MAG;

-the compromised MAG may send a large amount of PBU to make the LMA in burden and a DoS attack may occur;

PMIPv6 [draft-ietf-netlmm-proxymip6-11] defines to use IPsec to protect PBU/PBA. However, the prerequisite is that there should be trust relation between the MAG and the LMA. PMIPv6 security mechanism cannot work for the condition of no trust relation between the MAG and the LMA.

7.4.1.6.2   Possible measures

One possible way is to have the mapping between the UE and the serving MAG in one of network servers. When a MAG sends a PBU to a LMA, the LMA can ask this server to check whether this MAG is currently serving the UE. In this way, it will be avoided that a compromised MAG represents UE served by other MAGs to send the fake PBU.

UE should run an EAP-AKA with MAG before PMIPv6 procedure. The AAA server in UE's home network can record which MAG executed EAP-AKA procedure. In the meanwhile, AAA can keep the mapping between UE and its serving MAG. In this way, when a MAG sends a PBU message to a LMA, the LMA can ask the AAA server to have a check whether this MAG is serving the UE in the current time according to the identity of UE in PBU message. When UE moves to other MAG, AAA should know the change since AAA will be involved in changing MAG's procedure. So the AAA can update the mapping between UE and the serving MAG.

Editor's Note: Another solution is that AAA sends a key to MAG which is related to the UE after EAP-AKA procedure. UE will participate in the EAP-AKA. So the MAG can obtain this key only when this MAG really serves the UE. This key can be used to protect the integrity of PBU messages. LMA interacts with AAA to check the integrity of PBU message. In this way, a compromised MAG cannot get the related key. So it can not send valid PBU message. When UE moves to other MAG, AAA should know the change since AAA will be involved in changing MAG's procedure. So the AAA can update the related key and send the key to the current serving MAG. This solution may need clarify and FFS.

7.4.2   NetLMM

In Network based Localized Mobility Management (NetLMM) the Localized Mobility Anchor (LMA) is configured with a globally routable network prefix which the IP address assigned to UE is composed of, and packets to/from the UE are tunnelled between LMA and Mobile Access Gateways (MAGs). MAG shares the same network prefix as LMA's one, therefore, when the MN moves from one MAG to another, neither the subnet nor the MN IP address are changing. Here the LMA handles the packets incoming from Internet to the operator's domain. Each MAG is configured with the information needed to contact the LMA. This is also depicted in Figure 10.
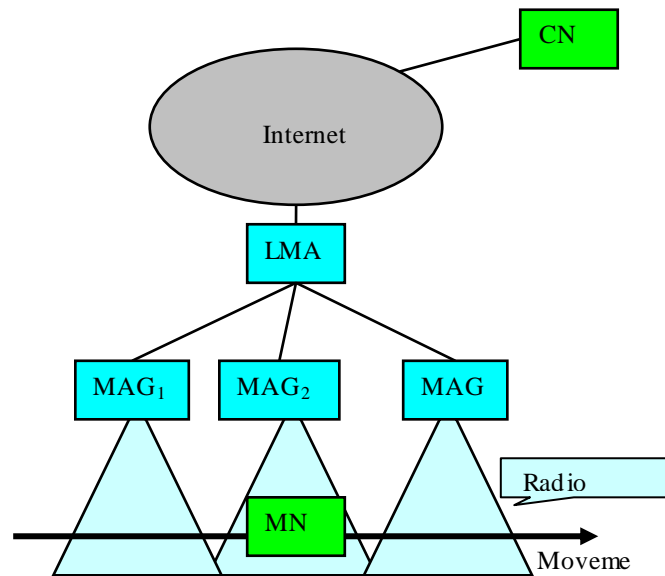

Figure 10: Proxy mobility protocol scenario

NetLMM does not bring any additional security threats. The protocol does face the general security threat of IP address ownership that is valid for all mobility protocols. Solution for this threat is to:

-     Secure Link Layer attachment (Packet Data Protocol Context secured by 3G AKA)

-     IP address allocation by the network over secured attachment.

For NetLMM the countermeasure regarding the security threats in Section 7.1 are:

-     IP address ownership

-     Enforce IP address ownership at network attachment. IP address is allocated by network (e.g., DHCP, PDP) over secure network attachment (e.g., 3G AKA). IP address binding is enforced during communication.

-     (D)DoS attack

-     Attack on forwarding resources

-     Requires knowledge of the network prefix allocated for MNs

-     Outside Correspondent Node and MNs are aware

-     Attack on control plane endpoint resources

-     Requires knowledge of the anchor point IP address

-     NetLMM LMA IP address is hidden from MNs and outside CNs.

-     NetLMM shall be resilient to DoS because only the forwarding resources can be attacked. Those can be dealt with by over-provisioning the forwarding capacity.

Editor's note: further details should be added.

8 Specific aspects of security for mobility between 3GPP access systems and non-3GPP access systems

8.1 Security for mobility between pre-SAE 3GPP access systems and non-3GPP access systems

It needs to be clarified in the course of the work on SAE mobility to what extent mobility, and, in particular the related security aspects involving pre-SAE 3GPP access systems require a different handling. The goal is, of course, to minimise or completely avoid the differences, but it is currently not clear in how far this goal can be achieved.

8.2 Security context transfer between 3GPP and trusted non-3GPP access networks

Security context is the information on the current state of a UE in the serving system required to re-establish the security association in the target system. Security context includes

1. Agreed security algorithms between the UE and the serving network,

2. Agreed/derived encryption and/or integrity protection keys and key identifiers.

3. Security association related information like key lifetime, sequence number, count values etc.

4. The temporary identity issued by the serving network

NOTE: In 3GPP, temporary identity is used by the target network to identify the serving network, but it's FFS for handover between 3GPP and non-3GPP networks whether temp IDs to be used for identifying the pervious access network.

As 3GPP has already adopted security context transfer procedures for optimizing authentication during handover, it is reasonable for SAE to enable security context transfer between the 3GPP and non-3GPP networks.

Editor's note: the content of security context is FFS.

8.3 ANDSF Security

8.3.1 General

ANDSF (Access Network Discovery and Selection Function) is a mechanism of access network discovery and selection. It is provided in order to control the UE's inter-system handover decisions and in order to reduce the battery consumption for inter-system mobility. See TS23.402 for more details. However, the privacy of UE and the operator needs to be protected if private information will be sent between UE and ANDSF server. Reusing GBA and PSK TLS to establish SA between UE and ANDSF server will be easily implemented by both operators and vendors. PSK TLS can be used for the security association between UE and ANDSF server. It can provide confidentiality and integrity protection for ANDSF security.
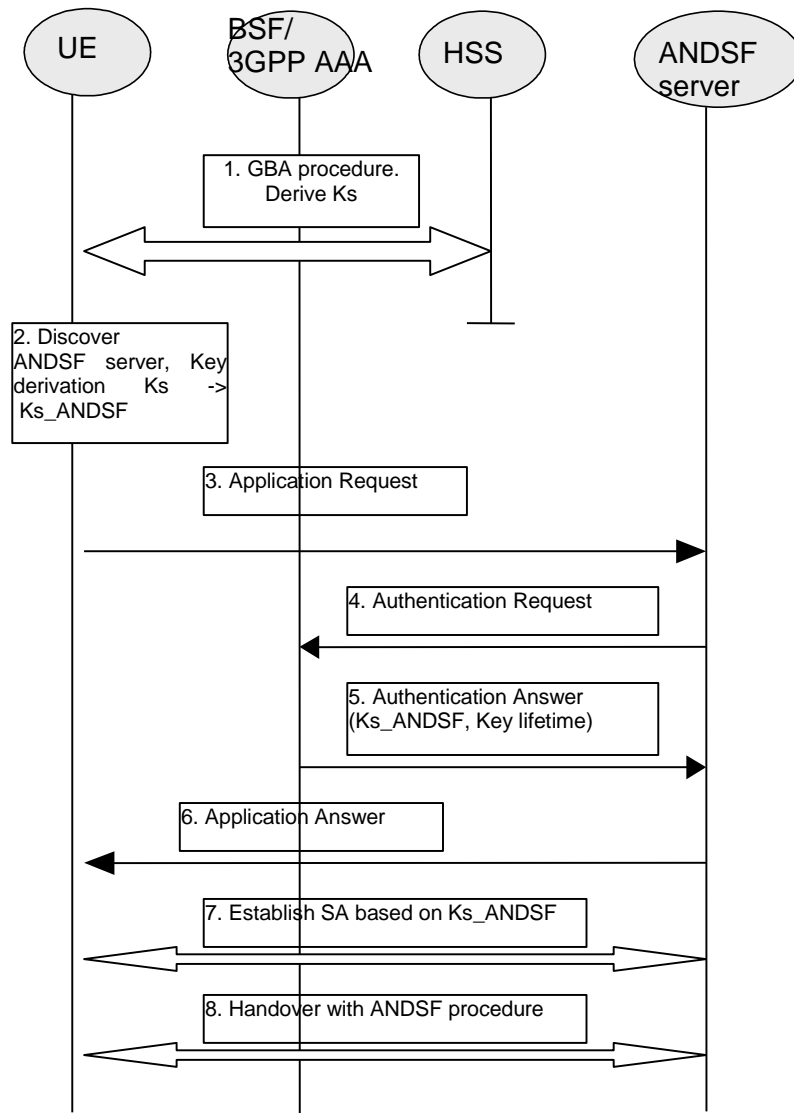
8.3.2 Procedure

Figure 11: ANDSF security using GBA

1. The UE and the BSF will process bootstrapping procedure. The master key Ks will be derived in this procedure.

Editor's note: It is FFS if 3GPP AAA can be the BSF in this scenario to be easily deployed by the operator.

2. The UE discovers the ANDSF server. See more details in TS23.402. Then the UE derives the Ks_ANDSF.

3. The UE starts communication with ANDSF server. UE sends application request to ANDSF server.

4. ANDSF server sends authentication request to the BSF for the key,

5. The BSF derives the Ks_ANDSF based the master key Ks. The derivation function is the same with Ks_NAF. And then BSF sends Ks_ANDSF and the key lifetime to the ANDSF server.

6. ANDSF server will inform UE that it gets the key Ks_ANDSF and can continue the ANDSF function,

7. The UE and the ANDSF server establish the security association based on the Ks_ANDSF. The detailed method i.e. PSK TLS, can be referenced to TS24.109.

Editor's note: It is FFS which method can also be used to establish the security association between the UE and the ANDSF server.

8. The UE and ANDSF server runs handover with ANDSF procedure after the SA was successfully established to protect the communication between them.

Annex A:
RFC 3957

From RFC 3957: "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. …[RFC3957] 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."

Appendix B of RFC3957 contains message flows for Requesting and Receiving Key Generation Nonce:

    MN   FA   AAA Infrastructure

    <--- Advertisement-----

    (if needed)

        -   RReq+AAA Key Req.-->

    --- RReq + AAA Key Req.--->

    <--- RRep + AAA Key Rep.---

    <-- RRep+AAA Key Rep.--

Annex B:
Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2006-02					Creation of document	0.0.0	0.0.1
2006-07					Revision of the document	0.0.1	0.0.2
2006-11					Revision of the document	0.0.2	0.0.3
2007-05					Including 3.1of S3-070399	0.0.3	0.0.4
2007-07					Including 2.1of S3-070506, and S3-070531	0.0.4	0.0.5
2007-10					Including S3-070748 and S3-070820, S3-070732 and S3-070756	0.0.5	0.1.0
2007-12					Including S3a070980.	0.1.0	0.2.0
2008-02					Including S3-080049, S3-080129.	0.2.0	0.3.0
2008-03					Correct the release number.	0.3.0	0.3.1
2008-04					Including S3-080362.	0.3.0	0.4.0
2008-06					Including S3-080725, S3-080765.	0.4.0	0.5.0
2008-09					MCC clean up for presentation to SA	0.5.0	1.0.0
2008-12					MCC clean up for presentation to SA for approval	1.0.0	2.0.0
2008-12					SA approved version and renumbering to 33.822	2.0.0	8.0.0