J-PAKE Based Mutual Authentication Model for EPC Networks

Cristina-Elena Vintilă, Victor-Valeriu Patriciu, and Ion Bica

Military Technical Academy, Romania

Abstract - The LTE architectural model developed by 3GPP proposed solutions to achieve high data rates, lighter network architectures and easier achievement of security requirements. Designed as a fully sustained IP network, the LTE provides unified access to a variety of services networks, via its EPC component. The core network of this LTE/4G architecture is designed to facilitate faster and more secure access to the services desired by the user, while providing a high level of predictability, control and charging for the services accessed. 4G architecture was designed in such a manner that it is also interoperable with existing 3G systems, as well as with non-3GPP systems. When describing such a flexible design, the security constraints cannot be neglected. The access to this 4G network is permitted only in a secure manner. The security of this network is based on its 3G predecessor and is no longer compatible with the 2G system.

This paper reviews some of the most command access solutions and model proposed for the 4G core network access. While describing the various designs, it also realizes a comparison between the models proposed and providing capture samples when available. In the second part, the paper proposes an authentication and key exchange model based on the J-PAKE algorithm and analyzes the security areas that can be improved if this model is used, along with its areas that need to be improved.

Key words – SAE, EPC, AKA, EAP-AKA, HSS, J-PAKE, PKI, key management, IMS

I. INTRODUCTION

The 4G architecture consists of two main components: the radio access network and the Evolved Packet Core. The radio network is represented by the eNodeB, the antenna and the air medium of transportation. The mobile devices connect to this antenna, which, in turn, has responsibilities in the mobile device authentication to the core network. The core network has several devices that deal with the signaling, traffic routing and prioritization and as well user authentication and charging. The most common core network devices are described in the following sections. This paper summarizes the most common authentication mechanisms for the access network and introduces the J-PAKE solution to secure access authentication. The model proposed has the cryptographic advantages resulted from the algorithms used, but also disadvantages in terms of computational overhead. While presenting the model, this paper also presents a brief comparative analysis between the model proposed and solutions inherited so far.

II. RESEARCH BACKGROUND

The EPC(Evolved Packet Core) system has multiple functional entities that describe its behavior and roles. These entities are logically separated, but they can reside on the same box, when the actual implementation decision comes into attention. Some other entities are logically and physically separated into different devices. One of the devices is called MME (Mobility Management Entity); this is the core network equipment responsible for UE management, for the mobility management when the UE is moving around the radio network and for choosing which equipment is going to deal with the data traffic for a particular UE. When the UE connects to an eNB via the LTE radio interface, the antenna first forwards all the traffic to the MME via the S1-MME logical IP interface, as this entity is connected to the HSS. The role of the MME is in this case to facilitate the verification of the UE’s authentication and authorization credentials, based on the UE’s identity and credentials stored by the HSS. Unlike its predecessor, the SGSN (Serving GPRS Support Node), the MME is a control-plane dedicated entity, it does not participate in any user-plane traffic flows. Another device is called SGW (Serving Gateway). This core network entity is responsible for routing the uplink and downlink traffic for the UE, as well as for the QoS enforcement of this user-plane traffic. It is both a control-plane and user-plane entity, similar to the SGSN and GGSN (Gateway GPRS Support Node) from the 3G architecture. When thinking about the mobility cases, as well as for the connection of a single UE to multiple networks, the SGW is a single point of contact for that UE to the 4G network. The PGW (Packet Data Network Gateway) is entity is responsible for connecting the 4G network to the Internet and/or other networks the UE may connect to: the operator intranet/extranet or a services network, like IMS (IP Multimedia Subsystem). This makes this entity the point of contact for the UE to that network, the PGW having the role of assigning an IP address to the UE; this IP address may be assigned from a local pool, this can act or facilitate the UE connectivity to a DHCP server and it can also facilitate the obtaining of an address via the destination network, a procedure called IP-CAN. This entity is also doing the QoS policies enforcement, as it is indicated by the PCRF settings. As mentioned earlier in the SGW brief description, a single UE may be connected to more than just one network. When this situation appears, there can be more than one PGW serving that UE; nevertheless there is only one pair of MME and SGW at a moment in time, serving a particular UE. The PGW is also the mobility anchor of the UE (User Equipment), when this user moves around the network. The PCRF (Policy Charging and Rules Function) is a database. This entity is connected to the PGW and has a very important role in the IP-CAN procedures, as well as in the QoS policy definition. This entity behaves distinctively when it is located in the Home Network, versus when it is located in the Visited Network. Therefore, we can refer to the PCRF as being either H-PCRF (Home Network PCRF) or V-PCRF (Visited Network PCRF). Essentially, the PCRF is a database just as the HSS, only that is contains information related to the QoS and charging policies for a specific UE. Its interfaces to the other network elements are also Diameter. The H-PCRF is connected to the PGW via the Rx interface. Another entity is the HSS (Home Subscriber Server). This entity is essentially a database. It contains all the information about a particular UE: IMSI (International Mobile Subscriber Identity), IMEI (International Mobile Equipment Identity), MSISDN (Mobile Subscriber Integrated Services Digital Network Number) and authentication information as AV (authentication vectors). This equipment is connected to the MME via the S6a interface, which is a Diameter based interface. The figure below represents a simplified 4G architecture that shows the core network devices, as well as the logical interfaces that link their functionality. It also represents an example of 3G connectivity to the 4G network.

The antenna is called eNodeB, and it is the user's first point of contact to the network. This antenna has important role in the UE admission to the network and security enforcement. It plays the role of an authentication relay agent for the user. In order to provide gradual integration for the operators, the 4G design permitted the connection of some of the 3G devices; the two types of segments interoperate, permitting the operator to integrate and test the 4G components on a step by step basis. The requirement for the 3G entities is to be able to interoperate with an SGW. The 3G portion of the network has multiple entities: the SGSN (Serving GPRS Support Node) is the homologous of the MME and part of the SGW in the 4G architecture, with the important difference that it does both signaling and user-plane, unlike MME which is a signaling-only entity. The GGSN (Gateway GPRS Support Node) is the homologous of the PGW in the 4G architecture and it is not present anymore in a mixed 3G-4G environment. U-TRAN stands for UMTS Terrestrial Radio Access Network, and it is composed of multiple antennas (NodeB devices) and a RNC (Radio Network Controller). It is the RNC that actually connects to the SGSN in order to authenticate the user. The procedures for both 4G access and 3G access are similar: UMTS-AKA.

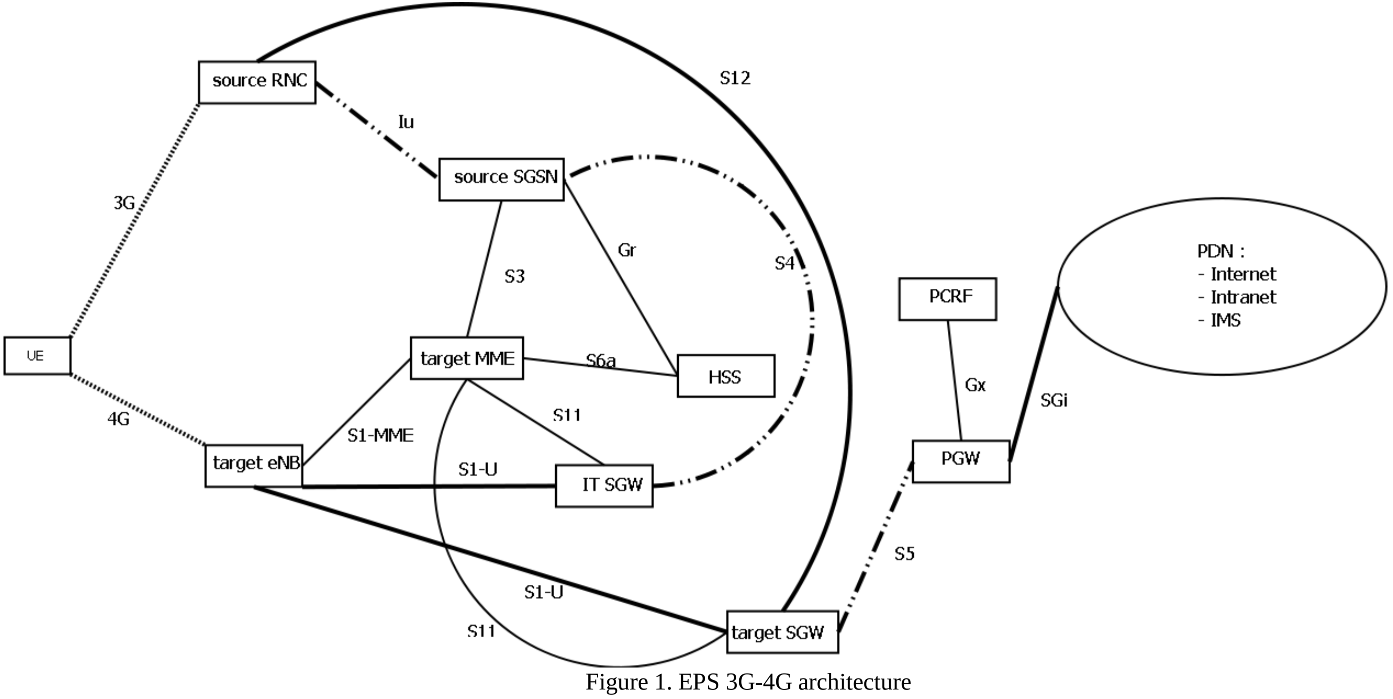

Figure 1. EPS 3G-4G architecture

The non-3GPP access may be any other form of access, like WLAN. This time the user authentication can no longer be realized via the classic authentication procedure AKA. Instead, there is a separate architecture of 3GPP-AAA servers that does the authentication of non-3GPP access users using the EAP-AKA procedure. The entities present in this case are the 3GPP AAA (Authentication, Authorization and Accounting) server, a 3GPP AAA Proxy Server, which is used when the user is in roaming and an ePDG (Evolved Packet Data Gateway). The ePDG is the peer the UE establishes a security communication with when it authenticates to the network. The ePDG authenticates the user by accessing the AAA servers. The access to the 4G core network can be classified as non-roaming and roaming access. It can also be classified by the type of access network: 4G, 3G, 2.5G, non-3GPP. The roaming scenarios on their own can be further classified as having home routed traffic (meaning that the PGW is located in the home network), local breakout with home operator's application functions only (the PGW is in the visited network and the user does its signaling and data traffic via the visited PDN – this is the case of a voice mail application) and local breakout with visited operator's application functions only (this is the case where the home and visited operators have an agreement to provide services to each other's users; all the user's traffic is served by and routed through the visited network, while the home network only does the authentication and policy verification). It is not mandatory that the roaming scenarios are of any one type of the three types described; there can be a combination of architectures, where for certain functions the home network offers the services – like the voice mail, while some other services, like access to the Internet can be offered directly by the visited network. Also, the same network operator may have one type of architectural interconnection with one operator, while having a different connection with another operator. Another type of scenario is local breakout scenario, with both home operator's and visited operator's application functions. Some of the services are offered by the home network, while others are offered by the visited operator. In this case there are three users, all connecting from roaming, one is a native 4G device, the other is a 3G device and the third is a non-3GPP device, a laptop that connects via WiFi.

III. ACCESS SECURITY

The security requirements for the 4G networks are classified according to the areas above and most of the security requirements are summarized in [6]. 4G design, following the 3G design, has delimited five main security areas, as follows:

i. Network Access Security – the concern of this area regards the possibility and conditions for granting access to the core network for the users accessing the 4G core via 4G, 3G or non-3GPP access points; the scope of this area includes user identification, authentication process and services provisioning;

ii. Network Domain Security – this area describes the secure interoperation between the EPC entities; the protocols that appear at this level are IPsec (recommended by Specs to take place within an operator's premises) and TLS (usually for inter-operator secure communications); these protocols appear also when doing interoperation with 3G entities or with non-3GPP entities;

iii. User Domain Security – this domain deals with the secure access to the mobile stations

iv. Application Domain Security – the applications run in an end-to-end fashion: from the mobile device past the core network, to the services network; the end-to-end security of these applications is under the scope of this security domain, along with its various dedicated security structures

v. Visibility and Configurability of Security – this domain of security is more of an informational sector; the target of this domain is the user information about the security features available on the mobile device: whether or not they are functioning properly and also which of and why the security features are mandatory for the secure operation of that mobile device

This article is under the scope of the Network Access Security domain, and it analyzes the security aspects that appear in the moment of the UE connection to the 4G network. The eNodeB, being the access point into the network, has a large variety of security requirements, concerning the protection in terms of integrity and confidentiality for the radio traffic, integrity protection and confidentiality of both the signaling and the user-plane from its side to the core network. Both 3G and 4G network authentication mechanisms rely on the 3G UMTS-AKA process, and the EPS-AKA improves some of its aspects. Both of the 3G and 4G models provide mutual authentication, but they also have some flaws. There are at least two security concerns related to the EPS-AKA process (inherited from UMTS-AKA and from the generic AKA process essentially). One of them states that the initial authentication process does not provide identity protection for the IMSI; the second one states that the AKA process does not have the PFS (Perfect Forward Secrecy) property. It is considered a security risk to send the IMSI over the air, by the UE to the eNodeB; instead a GUTI (Global Unique Temporary Identity) is stored temporarily by the UE and this identity is sent over the air to the eNB. In the handover cases, the target MME receives this GUTI in the TAU (Tracking Area Update) message, identifies the source MME and contacts it via the S10, asking it for the IMSI. The two entities verify each other for the accuracy of the information exchanged. Once the MME has the actual IMSI, it continues the UE's registration to the HSS via the S6a interface – Diameter. This process takes place also in the handover to/from the 3G networks; the target MME or target SGSN takes essentially the same steps to locate the real IMSI. In cases when the source entity is no longer available or when the user has to re-attach to the network, the device resends the IMSI over the network. Although this is a rare case, it proves that the registration process is vulnerable, at least theoretically, to man-in-the-middle attacks.

A. The Proposed Model

The PFS property cannot be achieved as per the defined EPS-AKA process. This paper proposes the usage of an existing algorithm created specifically to improve the security of the key authentication process. This algorithm is called J-PAKE (Authenticated Key Exchange by Juggling) [19]. This algorithm is very similar to Diffie-Hellman, in that it aims to prove the ownership of a shared secret. The secret is never sent over the wire, it is its possession that is being proved via this exchanged. J-PAKE is a two round exchange, providing the following security properties:

- *off-line dictionary attacks resistance*: it does not leak any information that allows an attacker to search for the password off-line;
- *forward secrecy:* the information remains protected even if the original shared secret was disclosed;
- *known-key security:* even is a session key is disclosed, the information protected with other session keys is not accessible;
- *on-line dictionary attacks resistance:* an on-line attacker can only test one password per execution.

This protocol requires two computational rounds and 14 exponentiations, but it is much stronger and requires a smaller exponent to generate its keys. The figure below describes the proposed J-PAKE based authentication mechanism.

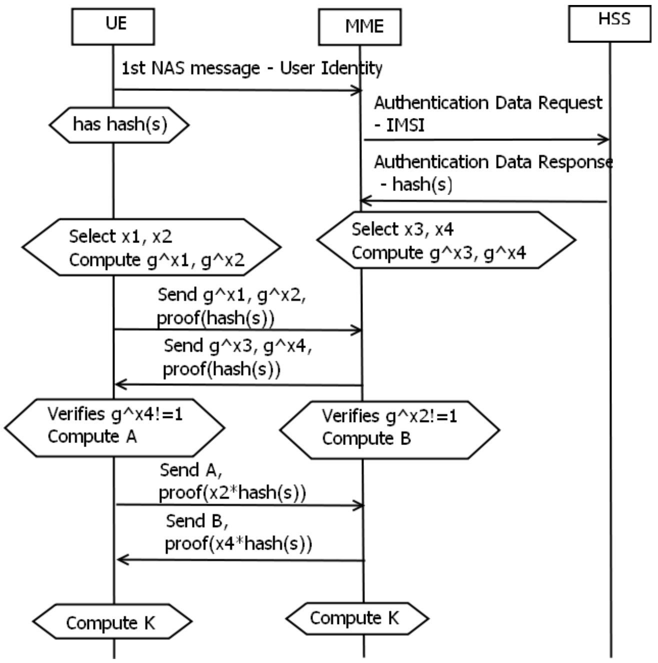

Figure 2. J-PAKE authentication mechanism for mobile devices

This procedure takes advantage of the J-PAKE system, but still follows the EPS-AKA outline described in the 3GPP specifications. The UE sends a NAS message to the MME, via the eNB, presenting its identity. The MME contacts the HSS and presents it the IMSI of the UE. The HSS locates and validates the IMSI, then it sends the MME a hash of the shared secret it has with that UE. The shared secret is here called s; s never actually leaves the UE, nor the HSS database. The authentication mechanism based on J-PAKE will actually use the hash of the shared secret as proof of secret knowledge. Following the J-PAKE algorithm, both the UE and the MME, independently, select 4 variables: x1 and x2 are selected by the UE, while x3 and x4 are selected by the MME. These variables are elements in a group G, subgroup of Z_p^*, and we consider q a prime of the group and g a group generator. Both UE and MME have the same (G,g). x1 and x3 belong to this group and may be also null, but x2 and x4 cannot be null. UE and MME send each other the values of the g^x1, g^x2 and the proof of the secret hash (the UE), while the MME sends the g^x3, g^x4 and the proof of the secret hash. On receiving the messages, each verifies that the second value received is not 1, which means that the x2, x4 values are not null. Then the UE computes A=g^(x1+x3+x4)*x2*hash(s) and sends this value along with the secret proof. The MME, on its turn, computes a value B=g^(x1+x2+x3)*x4*hash(s) and sends the UE this value, along with the secret proof. On receiving the value B, the UE computes a value called K=(B/(g^(x2*x4*hash(s))))^x2, which should equal g^(x1+x3)*x2*x4*hash(s). The MME computes K=(A/(g^(x2*x4*hash(s))))^x4, which should equal g^(x1+x3)*x2*x4*hash(s). If these are true, both the UE and the MME have proven the possession of the shared secret and from the value K they can now derive a session key, let’s call this k. This k can be further used a base row key for deriving the CK and IK keys. This way, the key generation and distribution defined by the 3GPP specifications remain unchanged.

This algorithm assures the secrecy and dictionary attacks protection for the authentication mechanism, which increases the security of the key generation and distribution process that follows. It is not based on PKI, so it is simply to implement.

In the classic EPS-AKA scheme, the MME retrieved a set of Authentication Vectors from the HSS, each having a RAND, AUTN, XRES and K-ASME. The MME forwards the RAND and the AUTN parameters to the UE. The UE verifies the AUTN, then computes the RES and sends it back to the MME. The MME verifies that the RES is the same as the XRES. If this happens, the two entities, the UE and the network, are mutually authenticated. This procedure, just as the one proposed above in this paper, does not provide IMSI protection. But the one above provides PFS due to the J-PAKE algorithm. The EPS-AKA procedure is represented in Figure 3 below.

The scheme proposed above can be improved so that it also provides IMSI protection, but is outside the scope of this article. In order to have the authentication mechanism structured, 3GPP has developed separate standards for the authentication schemes; the overall architecture is called GAA (Generic Authentication Architecture) and it has two components: the shared secret design, called GBA (Generic

Bootstrapping Architecture) and the digital certificates version, called SSC (Support for Subscriber Certificates).

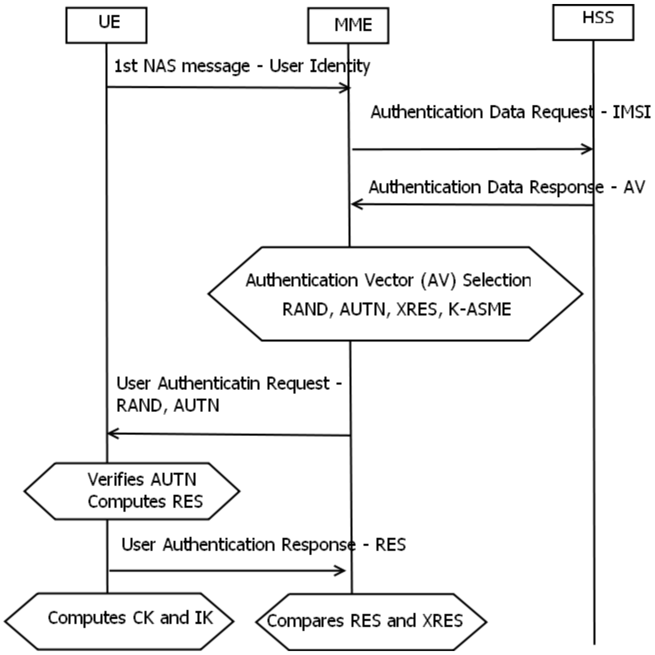
UE
MME
HSS
1st NAS message - User Identity
Authentication Data Request - IMSI
Authentication Data Response - AV
Authentication Vector (AV) Selection
RAND, AUTN, XRES, K-ASME
User Authenticatin Request -
RAND, AUTN
Verifies AUTN
Computes RES
User Authentication Response - RES
Computes CK and IK
Compares RES and XRES

Figure 3. EPS-AKA procedure

.

B. IMS authentication

The IMS system is a network external to the 4G. The PGW is connected to the Proxy component of the IMS system, relaying the authentication of the user to this remote network. The IMS is a complex design focused on providing not only VoIP, but mostly services to its subscribers. Figure 4 shows a simplified IMS architecture.

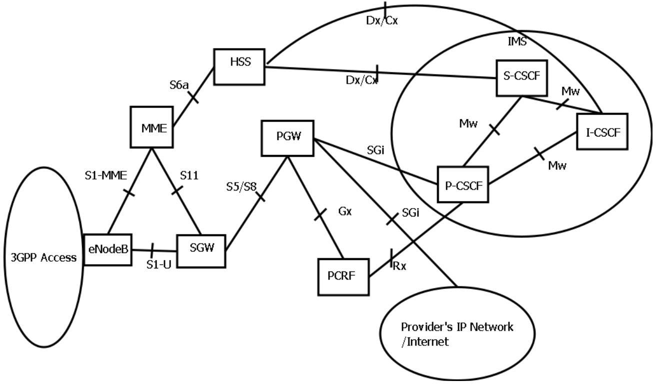

Figure 4. Simplified IMS architecture

The CSCF (Call Session Control Function) is a functionality core on its own. It deals with the authentication of the subscribers in the HSS, as well as with the SIP session establishment and SIP call management. The CSCF core has three elements: a proxy (P-CSCF), a serving entity (S-CSCF) and an interrogating entity (I-CSCF). The P-CSCF is the first point of contact in the IMS network, whether the user is in the home network or in roaming; it is also the entity sitting in the signaling path, being able to do message inspection, can do compression of the SIP header (SigComp) and it is the one establishing IPSec sessions to the UE at the registration time, being also the entity that manages the IPsec SA (Security Associations). If it includes a PDF (Policy Decision Function) component, it can also do media-plane QoS enforcement and bandwidth management. It interacts with the PCRF to determine the QoS requirements for that specific subscriber and inform the PGW about these QoS policies. The P also performs emergency session deletion. The I-CSCF is another component located at the edge of the administration domain, where the other servers locate it by doing DNS interrogations, as it uses NAPTR, DNS and SRV records. It has the role of interrogating the HSS and finding out which S is the HSS allocating for a specific user. From the HSS, it is the I-CSCF that obtains the next hop for the traffic, either an S-CSCF or an application server, where it also routes the other incoming requests. The S-CSCF entity is the central SIP server of the architecture, doing registration, inspection of the messages (as it sits in the message path) and it decides the SIP-AS (Application Server) which serves a certain service request. In its turn, the S is assigned to the UE by the HSS. Being in the path of the messages, the S is also responsible for the charging records generation. When it connects to the HSS database, the S downloads a service profile for a user public identity and then uses this profile in order to decide which is the best SIP-AS to delegate as serving this subscriber; this AS may be in the IMS system, in the CS domain or in another IP domain. The S is also responsible for all the routing decision regarding a subscriber: it is the entity that converts the MSISDN number to a SIP URI, as the IMS network only routes packets based on the SIP URI, then forwards these packets to their proper destination.

The authentication of the SIP user to the IMS system is done via the SIP IMS-AKA procedure, very similar to the EPS-AKA. The entire message flow is tunneled over GTPv1-U encapsulation in the 4G access network. These SIP packets flow between the UE – eNB (via the LTEu radio interface), then SGW (via the S1-U interface), to the PGW (via the S5/S8 interface), then routed over the Internet or provider's network to the P-CSCF. The P forwards the packets to the I-CSCF. This in turns connects to the HSS to have an S-CSCF assigned to this subscriber, and when this happens, the I will contact this S to manage the UE. Any further requests or call are going to be handled by this same S, which every I will look for when receiving a packet from the UE. It is very possible that the I change during a session, this is why each I will have to ask the HSS for the address of the persistent S when serving a subscriber. Without detailing the actual SIP and Diameter messages exchange, the representation of the IMS-AKA process is described in the Figure 5.

C. Message samples

The following samples are from an IMS-AKA procedure. The initial Register message has no authentication information; it is a SIP message, which leaves the mobile device, and same when reaching the P-CSCF entity. This message is encapsulated in GTPv1-u headers when passing through the 4G network. The example in this simulation is an IPv6 device that uses UDP to connect to the IMS network.

```
Session Initiation Protocol
Request-Line:   REGISTER   sip:open-ims.test
SIP/2.0
Method: REGISTER
Request-URI: sip:open-ims.test
Message Header
Via:                              SIP/2.0/UDP
[2001::10]:1143;rport;branch=z9hG4bK127541166
3890
From: <sip:11111@open-ims.test>;tag=6334
To: <sip:11111@open-ims.test>
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
CSeq: 901 REGISTER
Max-Forwards: 70
Allow:  INVITE,  ACK,  CANCEL,  BYE,  MESSAGE,
OPTIONS, NOTIFY, PRACK, UPDATE, REFER
Contact:
<sip:11111@[2001::10]:1143;transport=udp>;exp
ires=600000;+deviceID="3ca50bcb-7a67-44f1-
afd0-994a55f930f4";mobility="fixed"
User-Agent:     IM-client/OMA1.0     Mercuro-
Bronze/v4.0.1624.0
P-Preferred-Identity:        <sip:11111@open-
ims.test>
Supported: path
P-Access-Network-Info:   ADSL;eutran-cell-id-
3gpp=00000000
Privacy: none
Content-Length: 0
```

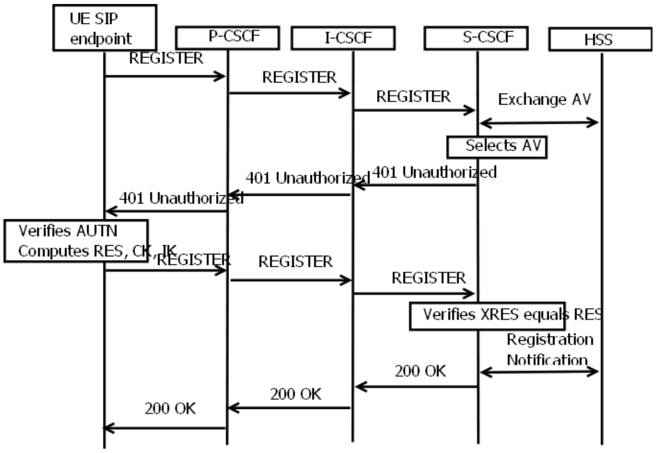

Figure 5. IMS-AKA

The response is a final negative response (401), indicating that the problem is on the sender side. This also indicates that the request cannot be processed at the server side, usually because the message either contains a bad syntax or that server cannot answer it. In this case, the 401 is an indication that the User Agent should re-attempt the registration, but this time including its authentication credentials in the request.

```
Session Initiation Protocol
Status-Line:  SIP/2.0  401  Unauthorized  -
Challenging the UE
Message Header
Via:                              SIP/2.0/UDP
[2001::10]:1143;rport=1143;branch=z9hG4bK1275
411663890
From: <sip:11111@open-ims.test>;tag=6334
SIP from address: sip:11111@open-ims.test
SIP from address User Part: 11111
SIP from address Host Part: open-ims.test
SIP tag: 6334
To:                         <sip:11111@open-
ims.test>;tag=925746a962736b96138042b427df654
9-2212
SIP to address: sip:11111@open-ims.test
SIP to address User Part: 11111
SIP to address Host Part: open-ims.test
SIP   tag:   925746a962736b96138042b427df6549-
2212
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
CSeq: 901 REGISTER
Path: <sip:term@pcscf.open-ims.test:4060;lr>
Service-Route:          <sip:orig@scscf.open-
ims.test:6060;lr>
Allow:  INVITE,  ACK,  CANCEL,  OPTIONS,  BYE,
REFER,  SUBSCRIBE,  NOTIFY,  PUBLISH,  MESSAGE,
INFO
Server:   Sip   EXpress   router   (2.1.0-dev1
OpenIMSCore (i386/linux))
Content-Length: 0
WWW-Authenticate:     Digest     realm="open-
ims.test",
nonce="qxZ3KUqjXlvgogK8aNtyHL4yoDzYBwAAFNpK0Y
llC1w=", algorithm=AKAv1-MD5, qop="auth,auth-
int"
Authentication Scheme: Digest
realm="open-ims.test"
nonce="qxZ3KUqjXlvgogK8aNtyHL4yoDzYBwAAFNpK0Y
llC1w="
algorithm=AKAv1-MD5
qop="auth
```

The new authentication message sent by the UE looks like this:

```
Session Initiation Protocol
Request-Line:   REGISTER   sip:open-ims.test
SIP/2.0
Message Header
Via:                              SIP/2.0/UDP
[2001::10]:1143;rport;branch=z9hG4bK127541166
3891
From: <sip:11111@open-ims.test>;tag=6334
To: <sip:11111@open-ims.test>
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
CSeq: 902 REGISTER
Max-Forwards: 70
Allow:  INVITE,  ACK,  CANCEL,  BYE,  MESSAGE,
OPTIONS, NOTIFY, PRACK, UPDATE, REFER
Contact:
<sip:11111@[2001::10]:1143;transport=udp>;exp
```

```
ires=600000;+deviceID="3ca50bcb-7a67-44f1-
afd0-994a55f930f4";mobility="fixed"
User-Agent:     IM-client/OMA1.0     Mercuro-
Bronze/v4.0.1624.0
Authorization:    Digest    algorithm=AKAv1-
MD5,username="11111@open-
ims.test",realm="open-
ims.test",nonce="qxZ3KUqjXlvgogK8aNtyHL4yoDzY
BwAAFNpK0Yl1C1w=",uri="sip:open-
ims.test",response="974679fa1f988670b52ebd3b0
58cf42a",qop=auth-in
P-Preferred-Identity:        <sip:11111@open-
ims.test>
Supported: path
P-Access-Network-Info:   ADSL;eutran-cell-id-
3gpp=00000000
Privacy: none
Content-Length: 0
```

And this time the response should be a successful 200 OK.

```
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK - SAR succesful
and registrar saved
Message Header
Via:                             SIP/2.0/UDP
[2001::10]:1143;rport=1143;branch=z9hG4bK1275
411663891
From: <sip:11111@open-ims.test>;tag=6334
To:                          <sip:11111@open-
ims.test>;tag=925746a962736b96138042b427df654
9-5b6b
Call-ID: M-50a5456166f246b78f081ac2453ee4ea
CSeq: 902 REGISTER
P-Associated-URI: <sip:11111@open-ims.test>
Contact:
<sip:11111@172.20.1.1:1143;transport=udp>;exp
ires=600000
Path: <sip:term@pcscf.open-ims.test:4060;lr>
Service-Route:        <sip:orig@scscf.open-
ims.test:6060;lr>
Allow:  INVITE,  ACK,  CANCEL,  OPTIONS,  BYE,
REFER,  SUBSCRIBE,  NOTIFY,  PUBLISH,  MESSAGE,
INFO
Server:   Sip   EXpress   router   (2.1.0-dev1
OpenIMSCore (i386/linux))
Content-Length: 0
```

According to this model, the J-PAKE system may be used to provide key exchange in a secure manner to IMS and 4G as well. It is possible to apply this to the IMS authentication case, but taking into account that is has two rounds, the result would be two sets of transactions between the UE and the IMS core, via the entire system. To provide the 4G system with this type of secure mechanism, the messages would be similar to the following example. The 4G systems use NAS (Non-Access Stratum) as a transport protocol between the UE and the MME. This protocol encapsulates the authentication messages exchange between the UE and the MME. In return, the MME is the authenticator of this UE, forwarding the user's credentials to the HSS. The transport for the NAS is RRC over the air interface and S1-AP between the eNB and the MME. After the MME processes the authentication information from the NAS message, it copies it to the Diameter exchange with the HSS. The entire protocol structure is described in Figure 6. An example of a NAS header containing the security information for the UE is the following:

```
Non-Access-Stratum (NAS)PDU
    0010   ....   =   Security   header   type:
Integrity protected and ciphered (2)
    ....  0111  =  Protocol  discriminator:  EPS
mobility management messages (7)
    Message authentication code: 0x00000000
    Sequence number: 2
    0110 .... = EPS bearer identity: 0x06
    ....  0010  =  Protocol  discriminator:  EPS
session management messages (2)
    Procedure transaction identity: 0
    NAS   EPS   session   management   messages:
Activate dedicated EPS bearer context request
(0xc5)
    0000 .... = Spare half octet: 0
    ....  0101  =  Linked  EPS  bearer  identity:
EPS bearer identity value 5 (5)
```

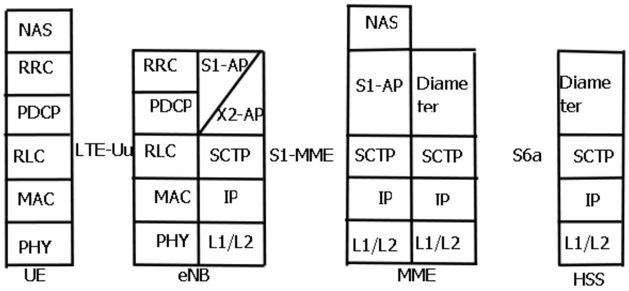

Figure 6. LTE access stack – Control-plane

D. *Advantages and Disadvantages of the Model*

The advantages of this model are related to the security features of the key exchange protocol used. The main requirements for the authentication, as indicated by the 3GPP, remain valid; the actual secret key between the UE and HSS is never transmitted of the wire or over the air. The UE has the secret key on the UICC and can at any moment create a hash of this key; same presumption is also valid for the HSS. At the moment the UE registers and the MME finds out about the UE attempt to authenticate, it forwards the IMSI of this mobile device to the HSS. The HSS locates the identity, retrieves the secret key and produces a hash of this key, that it then forwarded to the MME. The MME plays the role of the actual authenticator. From now on, all the key exchange is hashed with the secret key hash, in order to achieve mutual proof that that each participant is in the possession of the key or a hash of it.

As any model, this also has disadvantages. One of them resides in the implementation challenge. The mobile device market is various and complex; it is very difficult to achieve uniformity, especially in the permissive case of 4G. The implementation of this authentication model, based on a key exchange algorithm, would require some modifications in the classical functionality of the HSS process, as well as for the MME functionality as an authenticator. No other aspects of the stack presented in Figure 6 would require implementation changes. Further more, once this type of authentication is in place, a new authentication framework can be derived on top of it. As this algorithm also provides key exchange, the mobile device can have a session key useful for further security methods in its operation. Once this UE is successfully connected to the network and has a shared session key with the MME, it can secure any further signaling traffic to this MME. The handover case would be a situation where the session key must be re-negotiated, but the overhead introduced by this scenario should not be significant.

IV. Conclusions and Future work

This paper presented the overall 4G and IMS architectures, using one of the scenarios most commonly encountered, where the UE is in the home-network. The UE authenticates to the 4G network, using MME as a proxy to the HSS. Then, when trying to access an application server, it may use the GAA architecture, either in GBA mode – using a shared secret located on the UICC and on the HSS, or using SSC – a PKI portal that assigns digital certificates to the UICC.

This paper proposed a secure authentication scheme based on the J-PAKE algorithm, trying to overcome some of the AKA vulnerabilities.

The first step that follows this paper is to propose an authentication procedure for the SIP endpoints that relies only on 4G authentication architectures, then compare the solution to the classic SIP-IMS.

References:

[1] TS 23.401 – GPRS Enhancements for E-UTRAN access - http://www.3gpp.org/ftp/Specs/archive/23_series/23.401/

[2] TS 23.122 – NAS Functions related to Mobile Stations in idle mode http://www.3gpp.org/ftp/Specs/archive/23_series/23.122/

[3] TS 36.300 – E-UTRAN Overall Description - http://www.3gpp.org/ftp/Specs/archive/36_series/36.300/

[4] TS 43.022 – Functions of the MS in idle mode and group receive mode - http://www.3gpp.org/ftp/Specs/archive/43_series/43.022/

[5] TS 25.304 – UE Procedures in idle mode and procedures for cell reselection in connected mode - http://www.3gpp.org/ftp/Specs/archive/25_series/25.304/

[6] TS 33.401 – SAE – Security Architecture - http://www.3gpp.org/ftp/Specs/archive/33_series/33.401/

[7] TS 33.310 – Network Domain Security; Authentication Framework - http://www.3gpp.org/ftp/Specs/archive/33_series/33.310/

[8] TS 33.102 – 3G Security Architecture- http://www.3gpp.org/ftp/Specs/archive/33_series/33.102/

[9] RFC 5516 - Diameter Command Code Registration for the Third Generation Partnership Project (3GPP) Evolved Packet System (EPS) http://tools.ietf.org/html/rfc5516

[10] TS 29.272 – MME related interfaces based on Diameter – http://www.3gpp.org/ftp/Specs/archive/29_series/29.272/

[11] Tech-Invite - http://tech-invite.com/

[12] TS 29.294 – Tunneling Protocol for Control plane (GTPv2-C) – http://www.3gpp.org/ftp/Specs/archive/29_series/29.274/

[13] TS 33.220 – Generic Authentication Architecture; Generic Bootstrapping Authentication – http://www.3gpp.org/ftp/Specs/archive/33_series/33.220/

[14] TR 33.919 – Generic Authentication Architecture – System Overview – http://www.3gpp.org/ftp/Specs/archive/33_series/33.919/

[15] TS 33.221 – Support for Subscriber Certificates - http://www.3gpp.org/ftp/Specs/archive/33_series/33.221/

[16] "Efficient Remote Mutual Authentication and Key Agreement with Perfect Forward Secrecy" – Han-Cheng Hsiang, Weu-Kuan Shih, Information Technology Journal 8 – 2009, Asian Network for Scientific Information

[17] RFC 4187 – EAP Method for 3GPP AKA - http://tools.ietf.org/html/rfc4187

[18] RFC 2631 – Diffie-Hellman Key Agreement Method - http://tools.ietf.org/html/rfc2631

[19] "Password Authenticated Key Exchange by Juggling" – J-PAKE – 2008, F. Hao, P.Ryan, Proceedings of the 16th International Workshop on Security Protocols, 2008 - http://grouper.ieee.org/groups/1363/Research/contributions/hao-ryan-2008.pdf

[20] http://www.openimscore.org/

[21] "Fast and Secure Handover Schemes Based on Proposed WiMAX over EPON Network Security Architecture" - Wen Gu, Stamatios V. Kartalopoulos, and Pramode K. Verma, WSEAS Transactions, Issue 2, Volume 9, February 2010

[22] "A Secure and Efficient Protocol of Multiple Session Keys Generation" - Chang-Kuo Yeh, WSEAS Transactions, Issue 5, Volume 9, May 2010

[23] "Evolving to IMS as the Convergence Platform" - Mustafa Shakir, WSEAS AIBE, August 2010

[24] TS 24.301 - Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) – http://www.3gpp.org/ftp/specs/archive/24_series/24.301/