An Analysis of Secure Interoperation of EPC and Mobile Equipments

Cristina-Elena Vintilă, Victor-Valeriu Patriciu, Ion Bica
Military Technical Academy, Bucharest, Romania
cvintila@ixiacom.com, vip@mta.ro, ibica@mta.ro

***Abstract* - 4G architecture is the latest 3GPP development when it comes to mobile networks design and optimization. Designed initially for data, but having a flexible architecture, 4G is capable of integrating IMS, this way bringing in voice and services. 3GPP wanted to facilitate the migration from 3G and non-3GPP solutions to the 4G design, therefore the core network components of 4G are capable of interacting with 3G core network devices, provided these ones have an interoperability feature. This way, even 3G or non-3GPP devices are capable of using the 4G services. Nevertheless, one of the biggest issues when interoperating these solutions and devices is the security aspect. This paper reviews some of the most common access methods and summarizes the security concerns that raise in each case. The 4G security design is a very powerful solution for authenticating the users, even though it has some shortcomings that can be addressed.**

Keywords – SAE; EPC; AKA; EAP-AKA; HSS; J-PAKE; PKI; key management; security context.

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. This core network has several devices that deal with the signaling, traffic routing and prioritization and as well user authentication and charging [1]. The most common core network devices are the following: MME – Mobility Management Entity (that deals with user registration to the network, control-plane or signaling of user's traffic patterns permissions and manages the mobility of the user from one area to the other), SGW – Serving Gateway (this entity does both signaling and user-plane and it is the tracking area entity – where tracking area is a group of cells the user may camp on), PGW – Packet Data Network Gateway (this is the device that connects the 4G network to the intranet or to the Internet, it deals with traffic routing and prioritization based on the PCRF rules for a particular customer; it is also the mobility anchor of the UE – User Equipment, when this user moves around the network), PCRF – Policy Charging and Rules Function (a policy database of a customer's subscription to the operator) and HSS – Home Subscriber Server (a database that contains the mobile device identity and credentials) [9]. Figure 1 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 and non-3GPP connectivity to the 4G network.

The eNodeB, or the antenna, in the 4G architecture is the user's first point of contact to the network. The 4G mobile device identifies the antenna and tries to connect to it, asking for permission. The antenna then plays the role of an authentication relay agent for the user. The 4G architecture has been designed in such a matter that it can operate with 3G mobile devices, as long as the 3G parts of the network have the capability of communicating with the SGW [3]. The 3G portion of the network has multiple entities: the SGSN – Serving GPRS Support Node (this 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), GGSN – Gateway GPRS Support Node (this is the homologous of the PGW in the 4G architecture) and the U-TRAN. 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.

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 [6]. The entities involved in this case are the 3GPP AAA server, a 3GPP AAA Proxy Server, which is used in case where the user is in roaming and an ePDG – Evolved Packet Data Gateway. The AAA acronym stands for Authentication, Authorization and Accounting. The ePDG has an important role in the user authentication; this entity is the peer the UE establishes a security communication with. 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 – Packet Data Network- – 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

 ISBN: 978-1-61208-127-4

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. Figure 1 presents a *local breakout scenario, with both home operator's and visited operator's application functions*. This means that 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.

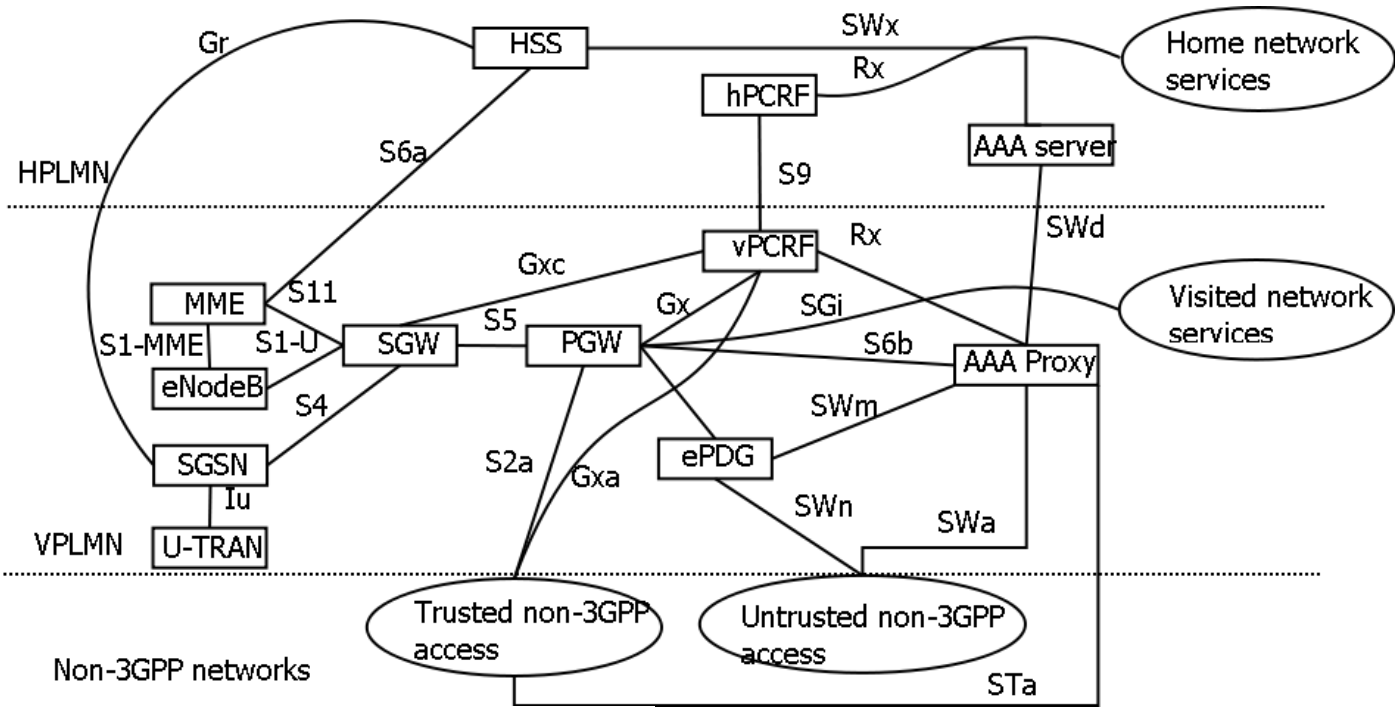

Figure 1. EPS roaming architecture with local breakout

The next two sections describe the security architecture of the 4G network, summarizing the security domains of this architecture, as well as it analyzes the three types of access to this network. The types of access are 4G radio access (via native 4G mobile stations), 3G compatible radio access and non-3gpp access via technologies like WLAN of WiFi.

II. SECURITY ARCHITECTURE AND REQUIREMENTS

The security architecture involves most of the devices, in less or greater measure. 4G design specifies 5 security areas:

- Network Access Security: this area deals with granting access to the (core) network only to those users that prove their identity, that identity matching a network's registered user, with valid authentication credentials and with a subscription that allows services to be delivered to this user
- Network Domain Security: this area deals with the secure interoperation between the Evolved Packet Core (EPC) network entities; most of these entities of a 4G network are already represented in Figure 1, as well as some of the 3G devices, like SGSN; this security is described by the protocols involved in securing the communications between EPC nodes: IPsec (recommended by Specs to take place within an operator's premises) and TLS (usually for inter-operator secure communications)
- User Domain Security: this area deals with the secure access to the mobile stations
- Application Domain Security: this area is concerned with how to secure the communication between the applications that reside on the user's mobile device and the core network application servers; as a layer 7 application, this area may implement a large variety of security structures
- Visibility and Configurability of Security: this is an informational area, for the user; the subscriber must have constant access to the information concerning the security features available on his device, whether or not they are functioning properly and whether or not they are required for the secure operation of a certain service

The security requirements for the 4G networks are classified according to the areas above and most of the security requirements are summarized in [6]. The eNodeB, being the access point into the network, has a large variety of security parameters and classes that must be verified and certified in order to assure a secure operation. These classes are the *setup and configuration* (this class deals with the secure communication in terms of confidentiality and

integrity between the eNB and the EPC, over the S1-MME and S1-U interfaces, between eNBs, over the X2 interface, with the secure setup configuration of the eNB and the secure software update), *key management inside the eNB* (as the eNB participates in the user equipment authentication process, it also stores some of the keys derives from the authentication process; these keys should be stored on a secure environment and never leave it, except in the situations specifically mentioned by the Specs), *handling of the user-plane traffic* (this data is transmitted over the S1-U interface to the SGW and via X2-U interface between eNBs; securing this data means assuring its confidentiality, integrity and protection against replay attacks), *handling of control-plane traffic* (this signaling transmissions take place over S1-MME interface towards the MME and via the X2-C interface between eNBs; securing this data means assuring its confidentiality, integrity and protection against replay attacks).

III. NETWORK ACCESS SECURITY

A. 4G mobile device access

As per [6], the preferred access method for the 4G mobile devices is AKA, named EPS-AKA – Evolved Packet System Authentication and Key Agreement, compatible with 3G UMTS – AKA authentication system, but not compatible with the 2G SIM, nor a SIM application on a UICC. The purpose of the AKA is to produce master keying material for protection of 3 classes of traffic: user-plane traffic, RRC – Radio Resource Control and NAS – Non Access Stratum. The exact procedure for deriving and distributing the keys is not important at this point. There are 6 keys that result from this process: K-eNB, K-NASint, K-NASenc, K-UPenc, K-RRCint and K-RRCenc. The AKA procedure is represented in the picture below.

This exchange is triggered by the UE connecting to an antenna. The antenna (called eNodeB) is forwarding to the MME the identity declared by the UE. At the very first attach, this is usually the IMSI – International Mobile Subscriber Identity, afterwards it is a temporary identity called GUTI – Global Unique Temporary Identity. The MME then contacts the HSS, sending the UE's identity over Diameter. If it finds the identity, the HSS responds with a set of AVs – Authentication Vectors (called generically Authentication Data). An AV contains 4 fields: the RAND – a random challenge string, an AUTN – an authentication token, an XRES – expected authentication response and a session key for the traffic between MME and HSS, named K-ASME – Key for Access Security Management Entity, which in our case is the role assumed by the MME. The MME forwards, via eNB, the RAND and AUTN to the UE. The UE authenticates the network using the AUTN and computes the RES – Response, which is sent back to the MME. The MME compares the RES and XRES and, if they match, the UE is considered authenticated.

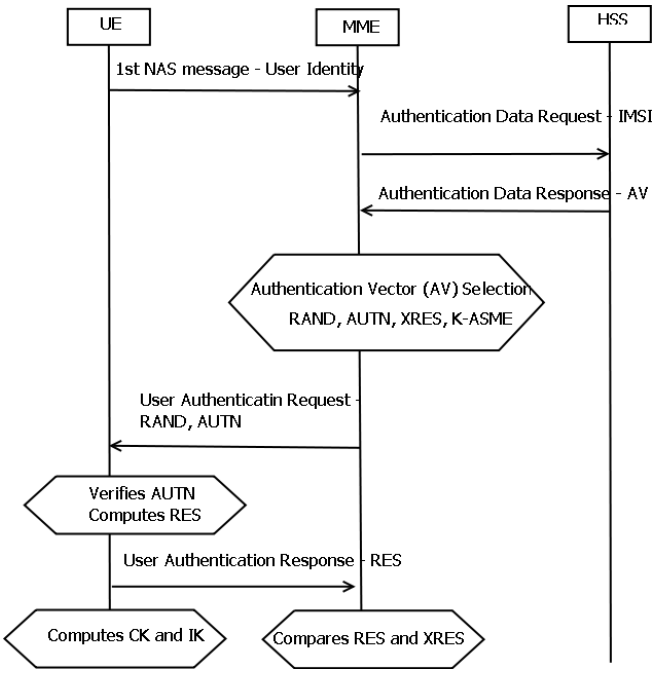

Figure 2. EPS-AKA procedure

There are at least 2 security issues related to the EPS-AKA process. One of them appears at the first Initial Attach of the User Equipment, when the user's identity IMSI is sent unencrypted over the air and the second one is the lack of PFS – Perfect Forward Secrecy property of the AKA algorithm. The identification of any subsequent requests a particular user may make to the network is done via a temporary identity called GUTI. The new MME reads this identifier from the UE's message (TAU – Tracking Area Update, for instance), contacts the previous MME in order to obtain the IMSI and then does the actual UE authentication to the HSS. The messages exchanged between the UE and the MME all pass through the eNB. These messages are GTPv2-C packets via the S1-MME interface. The AKA process continues over the S6a interface, where the information is encapsulated in Diameter protocol packets. The actual user-plane, after leaving the radio domain, is forwarded by the eNB directly to the designated SGW, over the S1-U interface, where the encapsulation is GTPv1-U. The keys derived by the AKA process are used over the air interface, then between the eNB and the MME. Traffic protection between the eNB and the SGW is a network domain security field of activity.

There have been multiple research projects done in order to improve the security and speed up the authentication process. Some of these projects are already patented and used in industry: SPEKE algorithm for the authentication between the BlackBerry device and the BES – BlackBerry Enterprise Server. The SPEKE is very similar to Diffie-Hellman, with the exception that the hash of the password is used as the group generator. Still, this method has a lot of vulnerabilities and technical limitations. There is yet another project that was very well received by the

 ISBN: 978-1-61208-127-4

cryptographic community. This is called J-PAKE [19]. It overcomes the vulnerabilities of both Diffie-Hellman and EKE – SPEKE methods. J-PAKE provides *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) and *on-line dictionary attacks resistance* (an on-line attacker can only test one password per execution). Even though this protocol requires two computational rounds and 14 exponentiations, it is much stronger and requires a smaller exponent to generate its keys.

This method is not yet used in the mobile industry, even though it is lightweight and applicable to the mobile devices characteristics. This protocol can be used along with AKA to provide efficient end-to-end cryptography for the 4G core network services, like the ones provided by IMS – IP Multimedia Subsystem, as well as instead of AKA in the 4G authentication protocol. Besides the fact that it is strong with regards to the 4 security aspects listed above, this method does not require a PKI implementation, which makes it more flexible and easier to use.

B. 3G mobile device access

The 3G security requirements and procedures are described in [8]. The solution used for authentication in the 3G design is the predecessor of the EPS-AKA. It is called UMTS-AKA and is uses the same methods. When authenticating to a 4G network, the user equipment is still connecting through a 3G access network. In the 4G E-UTRAN, the eNB has the entire access control role as an antenna (doing both signaling and data) and it is managed by an MME device, which has only signaling role: authentication, management and mobility management. The 3G U-TRAN design had a pool of antennas managed by a RNC (Radio Network Controller) and it was the SGSN device that did the mobility management, the authentication and also data-plane. The 3G design got simpler in the 4G, creating a smarter antenna and completely segregating the control and data planes in separate entities: MME and SGW. So, in order to effectively connect to a 4G core, the design must keep the SGW in place, as an essential core device, and define the 3G-4G delimitation on the S4 interface, between the SGSN and the SGW. This way, the SGSN still manages the 3G UE, does its authentication and manages also its mobility to the 4G network, but the actual traffic is forwarded to the SGW, and then the PGW in order to be routed to the Internet/Intranet or IMS behind the PDN the user connected to. The authentication of a 3G device is done by the SGSN, which interacts with the HSS over the Gr interface, which is Diameter based.

The interoperability issues between the 3G and 4G devices appear when the UE is moving from 3G cover to 4G cover and viceversa. It is very possible that the HSS already sent multiple AVs to the UE, and this one stores many of them, so that at a certain moment in time, it authenticates/re-authenticates using one of them, at its choice. The security association that exists between a mobile device and the network is called security context. In EPS, this context is composed of 2 other security contexts: the AS – Access Stratum and NAS – Non-Access Stratum contexts, which are sets of keys between the entities participating in the AKA process, which will provide hop-by-hop security (confidentiality and/or integrity and/or replay protection) for radio bearers, signaling and user-plane traffic. All the entities must be able to do Security Context management, and mostly the UE must be able to store multiple security contexts. It can be a legacy security context (a context created after the UMTS-AKA process from 3G) or a native EPS security context (results from the EPS-AKA procedure) or it may be a mapped security context, where the keys have been generated from the EPS-AKA process, but they are going to be used in a 3G communication (partial native context). As there can be multiple security contexts at one time in the UE and network, only one can be in effect (this one is called current security context); the others are non-current contexts. Table 1 summarizes the states and types of security contexts.

TABLE I. SECURITY CONTEXTS

AGE/EFFECT	CURRENT	NON-CURRENT
FULL	NATIVE / MAPPED	NATIVE
PARTIAL	X	NATIVE

Note that there is possible one single transformation, that is from a partially native security context, there can be generated a fully native context, but not the other way around.

There are multiple scenarios that assume 3G-4G interaction. One case is when the UE moves from the 4G network towards the 3G network, procedure called RAU – Routing Area Update, which can take place when the UE is either in ECM-IDLE mode or in ISR – Idle Signaling Reduction. When the UE is in ECM-CONNECTED mode, the procedure is called handover. As this article describes a 3G mobile connecting to a 4G network, we will detail the procedures required when a device moves from a 3G network towards a 4G network. These are also divided into procedures that apply when the device is in ECM-IDLE (specifically the TAU – Tracking Area Update procedure) and the handover from UTRAN to E-UTRAN. With regards to security, these procedures translate into a mapping of the old/previous security context into a new security context. As the case discussed involves 3G to 4G mobility, the old security context may or may not provide the (new) MME with the UE identity:

a) It may send a temporary identity that was being used in the 3G context: the UE sends in the TAU Request its former P-TMSI identity used in the 3G context, in the form of an old GUTI IE; this implies that the TAU request is integrity-protected, but not encrypted, and also implies the

UE sending to the MME more information about its previous security context:

- the KSI, P-TMSI and RAI, so that the (new) MME can find the (old) SGSN
- a P-TMSI signature
- a 32bit Nonce

b) It may not include the previous temporary identity, case where the AKA process takes place again

In case of the handover, the process has 2 steps:

a) Signaling handover using a mapped EPS security context

b) Subsequent NAS signaling to determine whether an EPS context can be used – in the cases where the network and UE security properties and requirements don't match – this usually takes place at the first MME change mobility process

Figure 3 describes a basic 3G to 4G handover process. The process is presented in more details in [6].

C. Non-3GPP mobile device access

A WLAN UE, like a laptop, may also connect to a 4G network, provided it supports EAP-AKA procedures and that the network has an AAA proxy and an 3GPP AAA server. The figure below describes the EAP-AKA process that takes place when a laptop connects via WLAN to a 4G core network.

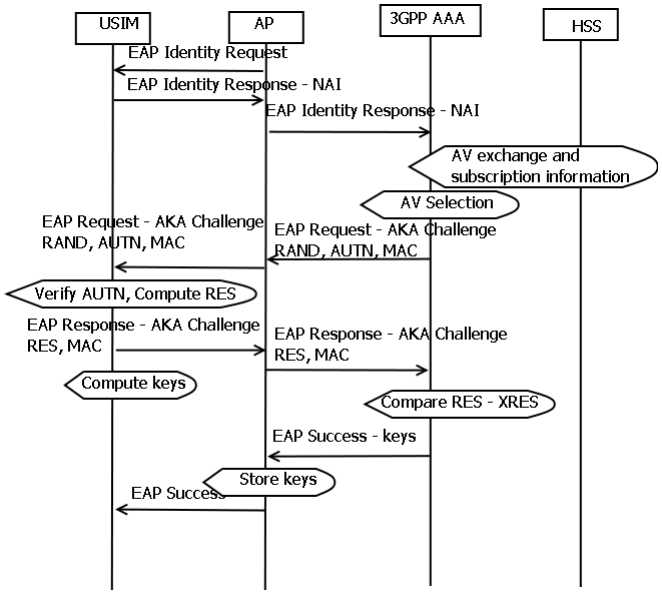

Figure 3. EPS EAP-AKA

The abbreviations and notations have the same meaning as for the classical AKA procedure. The only difference here is that this entire AKA negotiation takes place over the EAP – Extensible Authentication Protocol, an authentication framework used with success in protocols like 802.1x for layer 2 authentication in both wired and wireless technologies, as well as for upper layer security procedures like EoU – EAP over UDP.

The EPS-AKA system is essentially the same as the UMTS-AKA system. However, there are a several distinctive improvements, with regards to both security level and negotiation speed. The EPS-AKA process includes in the authentication the network ID, which means the protection of the mobile station from a fake antenna attack; this solution is not present in the UMTS-AKA system. Both of the 3G and 4G systems provide user ID protection only after the attach process completes (during re-register or during handover process): the IMSI is not protected at Initial Attach. Another improvement of the 4G AKA is the keying hierarchy, which determines the storage of the K-ASME in the MME. This means that the NAS traffic is also protected, between the UE and the MME, which does not happen in the 3G system, where the SGSN stores only the CK and IK for the user-plane traffic. Both the 3G and 4G systems protect the AS level traffic in terms of ciphering and integrity protection. Another key difference between the 3G and 4G is that the former allows the 2G interaction with regards to security. 4G system does no longer allow for handover to 2G systems, considering the security level of this system is not high enough. Also, the 4G system design permits for handover of non-3GPP devices, which was not previously permitted in the 3G system.

IV. Conclusions and Future work

Interoperating in the 4G worlds is a complex task, as a large variety of devices, coming from all over the standards and implementations ask for connectivity and for services. The 4G operators must be sure to protect their network and also their customers, with the minimum overload, for both the network and the user equipments. This paper reviewed only 3 basic types of access to the 4G core network. These are the native EPS – 4G mobile access, the traditional UMTS – 3G access, and a generic WLAN device. The very first step when deciding whether to serve or not a potential customer is to make sure this is a valid customer, and not an attacker. Looking from the user perspective, you want to make sure you are not connecting to a rogue network, and that your data remains private. 4G provides and requires mutual authentication. This is done natively via EPS-AKA procedure and can also be mapped from a legacy UMTS-AKA procedure. The WLAN device can enter 4G if it supports EAP-AKA and if the 4G network has 3GPP AAA capabilities.

The university world has come up with newer, faster and more secure procedures for doing mutual authentication. One of these procedures is derived from the PEKE algorithm and it is called J-PAKE. This simple method is very appropriate for applications in a mobile world, so it may be a revolutionary alternative to the way we do mutual authentication, even as an alternative to AKA or as a more

 ISBN: 978-1-61208-127-4

secure proof of knowledge before doing AKA key derivation.

This article is just one of a series of articles that debate the way 4G accomplished its 5 Security Domains duties, discussing the access security. This work continues with the analysis of the security issues that appear at mobility. There are a lot of mobility scenarios, both in Connected and Idle modes, as well as between 3G and 4G, that test the security of a 4G network.

REFERENCES

[1] TS 23.401 – GPRS Enhancements for E-UTRAN access - http://www.3gpp.org/ftp/Specs/archive/23_series/23.401/ [last access: February 2011]

[2] TS 23.122 – NAS Functions related to Mobile Stations in idle mode http://www.3gpp.org/ftp/Specs/archive/23_series/23.122/ [last access: February 2011]

[3] TS 36.300 – E-UTRAN Overall Description - http://www.3gpp.org/ftp/Specs/archive/36_series/36.300/ [last access: February 2011]

[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/ [last access: February 2011]

[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/ [last access: February 2011]

[6] TS 33.401 – SAE – Security Architecture - http://www.3gpp.org/ftp/Specs/archive/33_series/33.401/ [last access: February 2011]

[7] TS 33.310 – Network Domain Security; Authentication Framework - http://www.3gpp.org/ftp/Specs/archive/33_series/33.310/ [last access: February 2011]

[8] TS 33.102 – 3G Security Architecture- http://www.3gpp.org/ftp/Specs/archive/33_series/33.102/ [last access: February 2011]

[9] RFC 5516 - Diameter Command Code Registration for the Third Generation Partnership Project (3GPP) Evolved Packet System (EPS) http://tools.ietf.org/html/rfc5516 [last access: February 2011]

[10] TS 29.272 – MME related interfaces based on Diameter - http://www.3gpp.org/ftp/Specs/archive/29_series/29.272/ [last access: February 2011]

[11] Tech-Invite - http://tech-invite.com/ [last access: February 2011]

[12] TS 29.294 – Tunneling Protocol for Control plane (GTPv2-C) - http://www.3gpp.org/ftp/Specs/archive/29_series/29.274/ [last access: February 2011]

[13] TS 33.220 – Generic Authentication Architecture; Generic Bootstrapping Authentication - http://www.3gpp.org/ftp/Specs/archive/33_series/33.220/ [last access: February 2011]

[14] TR 33.919 – Generic Authentication Architecture – System Overview - http://www.3gpp.org/ftp/Specs/archive/33_series/33.919/ [last access: February 2011]

[15] TS 33.221 – Support for Subscriber Certificates - http://www.3gpp.org/ftp/Specs/archive/33_series/33.221/ [last access: February 2011]

[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 [last access: February 2011]

[17] RFC 4187 – EAP Method for 3GPP AKA - http://tools.ietf.org/html/rfc4187 [last access: February 2011]

[18] RFC 2631 – Diffie-Hellman Key Agreement Method - http://tools.ietf.org/html/rfc2631 [last access: February 2011]

[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 [last access: February 2011]

[20] TS 33.234 – WLAN – 3G interworking security - http://www.3gpp.org/ftp/specs/archive/33_series/33.234/ [last access: February 2011]

 ISBN: 978-1-61208-127-4