# Novel technique for Authentication & Encryption in Next Generation Networks

Aleksandar Tudzarov[1], Goce Stefanov[2], Saso Gelev[3],
*Faculty of Electrical Engineering, Goce Delcev University – Stip, R.Macedonia*

***Abstract* — This paper focuses on providing of novel technique for authentication and encryption in Next Generation Mobile Networks. The novel technique uses higher level of authentication methods that offer more flexibility and are based on well developed and proven IT security standards. Implementation of proposed technique will simplify the authentication process and will bring more simplified and manageable authentication environment that will cover fix/mobile convergence and can scale for different level of service needed security. By combining of several protocols that are used in process of network authentication like DIAMETER/EAP methods with PKI as a bases for authentication and by adding new parts in authentication access network architecture like PANA and EAP-SMIL we have proposed new authentication technique that will improve and modernize authentication and encryption process in Next Generation Networks.**

***Keywords — NGN, Authentication, Encryption, PKI, Certificate, DIAMETER, PANA, EAP, IPSEC***

## I. INTRODUCTION

One of the main focuses of NGN (Next generation networks) is placed on the convergence of telecom and IT to develop a ubiquitous infrastructure that offers higher capacity to customers and creates new opportunities to interconnect smart objects. According to the requirements in NGN there will be a massive number of devices (e.g. sensors, actuators and cameras) with a wide range of characteristics. Integration of all these heterogeneous devices with different security needs on NGN poses new security challenges towards a secure, reliable and dependable infrastructure. The Authentication and Key-agreement (AKA) procedures for 2G, 3G and 4G generations of mobile network have mostly fulfilled the requirements of each of these generations. 1G established the foundation of mobile networks; 2G increased the voice connectivity capacity to support more users per radio channel; 3G introduced high-speed internet access; 4G provided more data capacity. One of the key expectations for NGN is to be the reference network for the Internet of Things (IoT) connectivity. Although it can be assumed that NGN will utilize a basic authentication such as 4G/LTE protocols, the use cases for NGN brings new requirements that the next generation AKA protocol must support. The collection of connected devices (or "things""), referred in literature as Internet of Things (IoT), will increase substantially and NGN must provide an adequate level of security, which in turn introduce novel security challenges for authentication of these devices. The current SIM cards, while providing strong key protection, are also imposing a hurdle for certain use cases, and is also a non-negligible cost. To maximize the usability of IoT devices, new approach that will enable full authentication and security without the need of hardware SIM (UICC) need to be developed. In massive deployments of devices, the existing AKA protocol is not suitable, as each device have to run the full AKA procedure. The AKA protocol has a central role in the security of mobile networks as it place a fundament for exchange of the parameters needed to form a security context that is agreed by the parties. The protocol provides mutual authentication between device and serving network, and establishes session keys. The authentication protocol used in 4G (EPS-AKA) which is the state of the art authentication protocol in mobile networks is almost identical to its predecessor used in 3G (introduced in the late 90s). A limitation of EPS-AKA is that, for each device that requires network access, the protocol requires massive signaling among the device, the local serving network and the device's remote home network. NGN needs to offer light-weight and flexible authentication protocols.

Furthermore, it can be foreseen that large enterprises already have an existing AAA infrastructure in place. To further minimize the costs with future NGN subscribers the best way is to allow reuse of the pre-existing identities as a basis for NGN access, i.e. a bring your own identity (BYOI) solution. This way of thinking imposes need of close cooperation between different authentication schemes and methods in IT and telecom world as the requirements of both worlds are reaching the convergence point. Today, in the world of fix and wireless telecommunications, techniques and processes for authentication and encryption are developed as a separate stream from main IT security development paths. This separation leads to implementation of different solutions for the same or similar authentication requirements by means of security. Moreover, certain implementations differ from each other so much that they are not compatible whit each other or even not interoperable. In order to achieve more future prove and flexible security in the new information era where telecommunication and information technology are collapsing into single technology domain, we propose implementation of novel technique that will combine most useful algorithms and

[1] Aleksandar Tudzarov, Faculty of Electrical Engineering, Goce Delcev University – Stip, R.Macedonia, E-mail: aleksandar.tudzarov@ugd.edu.mk

[2]Goce Stefanov, Faculty of Electrical Engineering, Goce Delcev University – Stip, R.Macedonia, E-mail: goce.stefanov@ugd.edu.mk

[3]Saso Gelev, Faculty of Electrical Engineering, Goce Delcev University – Stip, R.Macedonia, E-mail: saso.gelev@ugd.edu.mk

protocols to achieve convergent authentication techniques into technology domain by introducing technology agnostic procedures for authentication and encryption.

The basis of authentication in proposed architecture will be X.509 certificate that would be issued to each user and stored on some authentication medium (either eSIM – "embedded SIM" or embedded in some local security store). This authentication assumption will simplify the process for SIM changes (including eSIM which popularity is increasing and claims to be the new standard for all NGN authentication processes) while user changes network by simple secure download of new certificate and installing it in the store – already know procedures and protocols in IP world. These certificates will have to be issued and signed by Operators CA (Certificate Authority). In this way, increased level of security will be achieved.

Second step in the authentication will be using of secure and flexible protocols for exchanging of security messages that can offer authentication in converged fix/mobile environment, and can be flexible enough to offer exchange of security polices as well as basic service policies for proper handling of users payload traffic. This means that with finalizing of authentication procedure access units (Baseband processing modules or fixed network routing entities) can enquire basic routing policies for handling of the user traffic.

Third step of the authentication process (which is not directly related with authentication) should be encryption of the user payload traffic. Having in mind that proposed authentication process is based on using of Certificates; they can also be used for encryption of the traffic in unsecure fix or wireless environment.

Considering the principles set above proposed novel technique assumes using of PANA and EAP-SAML protocols for authentication in correlation with DIAMETER/EAP in the backend communication with authentication server for establishing the authentication ecosystem that will be used in the authentication and later in encryption process of the user communication. PANA refers to (Protocol for Carrying Authentication for Network Access). EAP-SAML refers to (Security Assertion Markup Language) over EAP (Extensible Authentication Protocol). SAML represents XML-based standard for exchanging of authentication and authorization data between security entities; that is between the entity that poses the identity and the one who provides the service. This standard is a product of the OASIS (Organization for the Advancement of Structured Information Standards). The use of this EAP method provides an opportunity for exchange of additional network policies between the authentication server and the authentication client that are needed in phase of establishment of network connectivity.

## II. DETAILED PROCESS FOR AUTHENTICATION AND ENCRIPTION

The process of authentication, authorization and exchange of policies when connecting to certain access network begins with the first phase, which is phase of initiation request for connection towards accessing network. In the second stage, a mechanism for authentication and authorization is activated. This process is accomplished through access network. The first step in achieving this goal is to check the user authentication parameters by the client. This involves verifying the authentication resources that for the proposed architecture based on user certificates involves checking the existence of the user certificate. In next step validity check of the certificate, its private and public keys and the validity of the issuer and its purpose is conducted. Once the validity of user parameters are determined, the flow continues through the process of authentication and authorization between the user and the network. Communication between them is based on PANA protocol where authentication of user preferences is performed through EAP-TLS or EAP-SAML. In this case, function of EAP client is performed by user client module, while function of authenticator is conducted by network module on NGN side where this module will be presented as DIAMETER server as it represents the central registry of user data and their profiles. Procedures for authentication and authorization of access technology in NGN are presented as step 3, 6 and step 9.

After the authentication process ends, network module will initiate the process of exchange of network policies and user parameters as presented in steps 12 and 15.

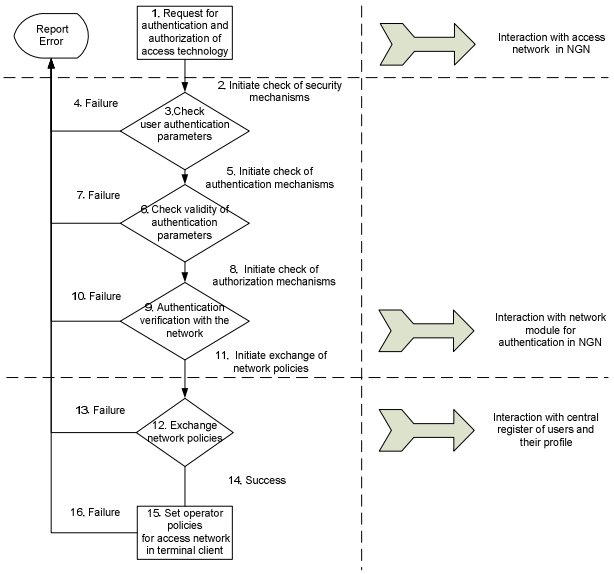


Fig 1. Block diagram for authentication and authorization of access technology of the architecture of PANA protocol

The process of authentication is based on EAP as basis for exchange of authentication in step 9. Authentication with EAP typically begins with a process of negotiation of EAP method. Once EAP authentication method is negotiated and accepted between network entities, a process of exchange of EAP authentication messages between the EAP client and the EAP server is started. When the process of authentication is completed, EAP server sends the EAP message to the EAP client, which confirms or denies the success of the authentication process. Authenticator is informed about the result of the authentication process through the AAA protocol. Based on this information authenticator can provide user access to the requested access network, or to continue to block access. Depending on the chosen EAP method, EAP authentication can be used in the derivation of keys by the EAP Client and the EAP server. Such keys can be

transported through the AAA protocol from the EAP server to the authenticator.

After completing of this procedure and getting derived EAP keys on the side of the terminal (EAP Client) and authenticator, the process of derivation of transport keys to protect access link transmission data can begin. In line with development of new method of authentication, as most suitable candidate for the proposed architecture we can mark EAP-SAML or EAP-TLS protocol, while in the field of transmission techniques for the transmission of EAP the PANA (Protocol for Carrying Authentication for Network Access) can be chosen as a protocol developed for transmission of EAP protocol over "any transport network".

### *A. NETWORK AUTHENTICATION OVER ACCESS NETWORKS*

PANA is a protocol designed by the IETF as a protocol that should provide transparent network authentication over data link network layer. Its goal is to ensure the establishment of any authentication protocol, over any transport technology (data link level). This goal is achieved by setting the EAP over IP at the transmission level. Along with this basic principle this protocol provides a number of additional and powerful functionalities, such as: separate NAP and ISP authentication, possibility of reuse of local security associations, fast reauthentication, and secure exchange of EAP messages, protocol extensibility by introducing additional protocol messages and so on. These functionalities of PANA protocol makes it suitable for use in procedures for authentication in heterogeneous networks. PANA protocol is set on the last IP link between PANA client (PaC) and PANA authentication agent (PAA). PAA client is set at controller for network access side in this case access network unit (wireless Baseband or fix access xDSL/GPON). This access controller attempts to bridge the AAA sessions between the client and the AAA server using PANA on one side (the client) and DIAMETER on the other side (to the AAA server). PANA platform, despite these network entities also defines other network entity called EP (enforcement point). EP control access in a manner that prohibits access of unauthenticated users to the network resources. EP entity should be placed at key locations in the network architecture (This would be Baseband/DU units or fixed network authentication routers) in order to allow full control of the traffic in both directions.

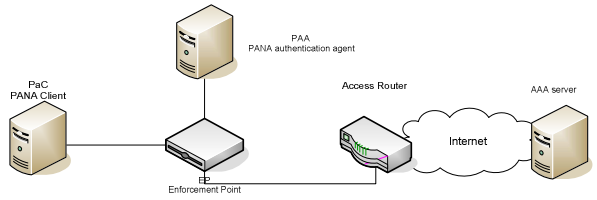


Fig 2. Overview of the architecture of PANA protocol

In most networks, the EP and the authentication agent (PAA) are collocated within a single network entity, but despite this, PANA protocol allows separation of these two functions in the architecture in different entities as shown in Figure 2.

PANA protocol in IP networks is defined as UDP based protocol that operates between two IP-based network entities on the same IP link on UDP port 716. It provides transmission of messages in a specified order as required by EAP specification. Transport message flow is shown in Fig 3. Initiation phase of the protocol consists of exchange of a series of messages with requests and responses. Some of the transmitted messages carry information between the client and the network, while others are used to manage the entire PANA authentication session.

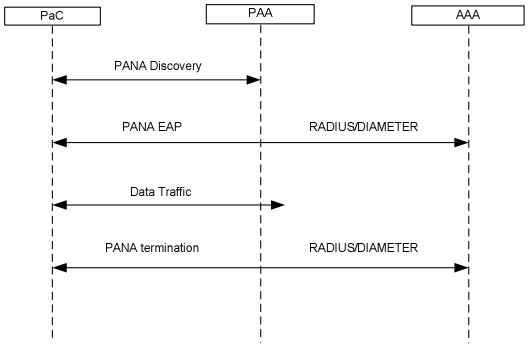


Fig 3. PANA protocol - Message flow

Discovery phase involves two possible scenarios. The first concerns the discovery initiated by PaC client that sends a message to detect PAA on access links, while the second refers to the discovery of PAA. After this process is finished authentication process goes on with exchange of series of PANA authentication messages that represent simple exchange of EAP messages over PANA protocol between the EAP client and EAP server. If authentication is successful, the message instantly imposes a common understanding of the identifier of the device (if the device is identified by its MAC or IP address) and associated level of protection of exchanged packets. Agreed identifier of PaC will be handed to the EP (Enforcement point) for performing of access control in the next phase. Meanwhile the two entities will decide whether to use the basic link-level encryption or IPSec for cryptographic user data protection (if EAP method enables derivation of cryptographic keys). [1], [2], [3]

Received keys are used to generate PANA SA (PANA security associations) that are used to protect the exchange of multiple consecutive PANA messages. In less secure environments it is expected that EAP methods that provide mutual authentication and generate cryptographic keys are chosen in order to protect the communication. [4], [5]

PANA protocol allows IPSec-based access control (which can be bases for encryption in wireless unsecure wireless/fixed transport) in a way that helps the IPSec protocol in the creation of IPSec security associations.

PANA protocol generates cryptographic keys upon completion of the EAP protocol for creating PANA security associations, but they cannot be used directly to create IPSec security associations. This relationship can be used as a basis for "pre-shared secret" for generating dynamic IPSec associations.

This approach leads to the use of IKE protocol for reuse of PANA security associations for IPSec associations. The keys are obtained by derivation of the PANA security association and as such are delivered to IKE protocol. This new IPSec associations are used further to create a

connections between the PaC and PAA, or EP entity for providing of authenticated or encrypted data transport.

Detail exchange message flow for described process above can be seen on Figure 4.

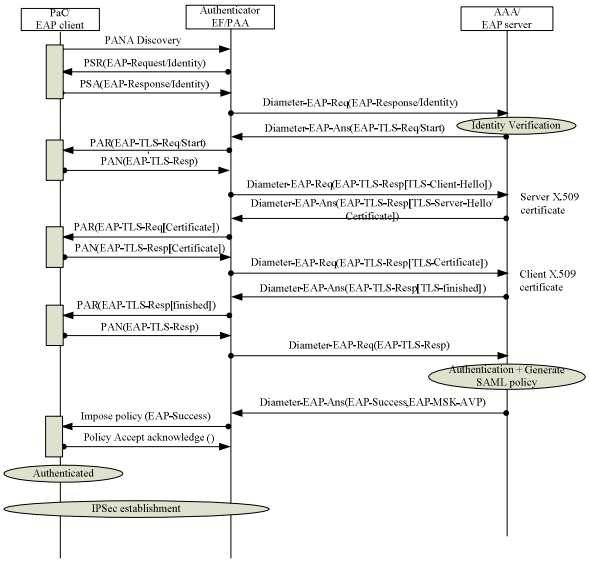


Fig 4. Exchange message flow in EAP-TLS over PANA and DIAMETER

### *B. NETWORK AUTHENTICATION ECOSISTEM FOR NEXT GENERATION NETWORKS*

Process of authentication and authorization based on PANA protocol as forefront for formation of authenticated encrypted connections is the basis of the design of the proposed technique for interworking among heterogeneous networks. First step in the process of achieving IP connectivity through access technologies is authentication. For authentication protocol in this case it is best to use EAP and as authentication method on top of it SAML will be used. As a transfer protocol for authentication between client and authenticator n this case PANA protocol can be used where user terminal will be treated as PaC and (Radio Baseband/fixed router – called Authenticator) as PAA. In the background, authenticator should achieve connectivity with certain "user database" server in the cloud, using DIAMETER as authentication protocol. In this way in the authentication process the user terminal acts as EAP client as long as User Database server acts as the EAP server. EAP session is established directly between these two entities. After successful authentication and authorization of user using the PANA protocol as described above and by using of IKE protocol process continues in the stage of formation of the IPSec connections between the two ends of the communication, the user terminal and PAA. Use of EAP-TLS as authentication protocol is due to the concept of security set in the new architecture. The security module by the client and PAA poses public certificates that consist of public and private cryptographic keys. These certificates are issued by Operator. There can be various ways how this can be done, but mainly it is based on setting up a public key infrastructure (PKI).

With the help of PKI each customer is associated with a X.509 certificate that has been issued for its use in this architecture. In the process of user authentication via EAP-TLS/EAP-SAML protocol check of the certificate parameters is performed for the user who in User Database is connected to the appropriate customer. If its authenticity and validity are determined and also the client that is represented by this certificate is entitled to use the appropriate service it will enable establishment of a link between client and PAA. In this process User Database performs authentication/authorization of access technology in order to determine whether it can be used in the interworking operation. This completes the client's authentication and authorization phase. [6],[7]

## III. CONCLUSION

In the presented paper new novel technique for authentication and transparent encryption process for next generation of networks was presented. As part of the proposed technique, processes for authentication and authorization while connecting to the access technologies were analyzed and innovative techniques are introduced. In this context as the basis of defined authentication process an independent mechanism for authentication and authentication procedures based on certificates was set. Presented process of authentication and authorization are based on PANA protocol as the vanguard of establishing authenticated IPSec tunnel. This technique is fundament in the design of the secure architecture for interworking in heterogeneous networks. In the next period we plan to conduct in deep analyses of the proposed algorithm (including simulation) to prove the fast convergence time of authentication scheme and to propose standard SAML exchange scheme for the NGN authentication exchange that need to cover all identified NGN security use cases till now and to offer easy extensibility for the future.

## REFERENCES

[2] Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[3] Oppliger, R., "Security Technologies for the World Wide Web", Artech House Computer Library, 2000.

[4] Yuan, R. and Strayer, T., "Virtual Private Networks", Addison-Wesley, 2001.

[5] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-panapana- 07 (work in progress), December 2004.

[6] A Olivereau, A.F. Gomez Skaremta, R.M Lopez, B Weyl, P. Brandao, P Mishra, c. Hauser, "An advanced Authorization Framework for IP-based B3G Systems", 14th IST Mobile & Wireless Communication Summit, Dresden 19-23 June 2005

[7] Toni Janevski, Aleksandar Tudzarov, Marko Porjazoski, Pero Latkoski, University "Sv. Kiril i Metodij", Faculty of Electrical Engineering and Information Technologies, "System for analyses of end-to-end quality of data services in cellular networks"

[7] Rosario Giustolisi, Christian Gehrmann, Markus Ahlström, and Simon Holmberg. "A Secure Group-Based AKA Protocol for Machine-Type Communications" 19th Annual International Conference on Information Security and Cryptology. November 30 - December 2, 2016, Seoul, Korea