# New Authentication and Key Agreement Protocol for LTE-WLAN Interworking

Ahmed H.Hassanein
Elect& Comm. Eng. Dept.
AASTMT, Cairo, Egypt

Ahmed A. Abdel Hafez
Elect. & Comm. Eng. Dept
Military Technical College,
Egypt

Abd El-Hamid A. Gaafar
Elect. & Comm. Dept
AASTMT, Cairo, Egypt .

## ABSTRACT

New cellular networks are capable of providing high mobility, whereas WLANs are known for having relatively higher bandwidths. Therefore, interworking cellular networks with WLANs offers ubiquitous data services and relatively high data rates across modern networks. This interworking will enable a user to access new cellular services via a WLAN, while roaming within a range of hotspots. To provide secure 3G-WLAN interworking in the SAE/LTE architecture, Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) is used. However, EAP-AKA has several vulnerabilities. This paper analyzes vulnerabilities in LTE-WLAN interworking and proposes a new authentication and key agreement protocol based on EAP-AKA.

## Keywords

LTE, Interworking, 3G-WLAN.

## 1. INTRODUCTION

The Third Generation Partnership Project (3GPP) made a study to improve the UMTS 3G mobile system standard to cope with future requirements. Goals of this study included improving efficiency, lowering costs, reducing complexity, improving services, making use of new spectrum opportunities and better integration with other open standards (such as WLAN and WiMAX) which are considered as non 3GPP accesses, the (3GPP) called this study LTE/SAE. The new radio access network is referred to as the ‘Evolved UTRAN’ (E-UTRAN) [1][2]. 3GPP specified a new Packet Core, the Evolved Packet Core (EPC) network architecture to support the E-UTRAN through a reduction in the number of network elements, simpler functionality, but most importantly allowing for connections and hand-over to other fixed line and wireless access technologies, giving the service providers the ability to deliver a seamless mobility experience.

Interworking is important as LTE allows different deployment options for the operators. Clients supporting multiple-access technologies, including LTE, need to have continuous access to the network for good user experience. For example, a client using 3G data may enter an LTE hotspot and thus be handed over to it for a higher data throughput.

The integration needs a secure authentication mechanism to protect the system and to protect the user data. The SAE/LTE architecture reuses EAP-AKA [4], [14] to provide secure 3G-WLAN interworking. When a subscriber attempts to access WLAN, the subscriber sends the International Mobile Subscriber Identity (IMSI) through Network Access Identifier (NAI) to the Access Point (AP). EAP-AKA is based on UMTS-AKA [3]. For this reason, EAP-AKA may have the vulnerabilities of both, the UMTS-AKA and the 3G-WLAN interworking.

This paper analyzes the vulnerabilities of the EAP-AKA and proposes a new authentication and key agreement protocol based on EAP-AKA [4][5] to overcome the analyzed vulnerabilities of EAP-AKA.

The rest of the paper is organized as follows: Section 2 presents the security architecture for Non-3GPP access to EPS. Section 3 gives brief on ECDH-Elliptic curve Diffie Hellman. Section 4 explains overview of EAP-AKA and its vulnerabilities. In Section 5, a new authentication and key agreement protocol based on EAP-AKA is proposed. In Section 6 presents the security analysis of the proposed protocol. Section 7 gives a short brief about the future work that will be done. Finally, Section 8 presents the conclusion.

## 2. SECURITY ARCHITECTURE FOR NON-3GPP ACCESS TO EPS

Long Term Evolution (LTE) standards define 3GPP’s fourth-generation (4G) high-speed packet data network [1]. The LTE network involves the evolution of both the radio infrastructure and the mobile packet core to support high data rates.

The radio infrastructure evolution is known as the evolved UMTS Terrestrial Radio Access Network (eUTRAN), and the packet core evolution is known as the Evolved Packet Core (EPC). The total system evolution is known as the Evolved Packet System (EPS).

The EPC supports access to the network through non-3GPP radio networks, such as Wi-Fi networks.Non-3GPP means that these accesses which not specified in the 3GPP

Non-3GPP accesses can be split into two categories:

- Trusted non-3GPP which can connect directly to the EPC.
- Un-trusted non-3GPP which can connect to the EPC via a network entity called the evolved packet data gateway (ePDG).

These un-trusted networks require that the mobile node’s bearer traffic be delivered in a secure fashion.

The architecture [6][7] defines an enhanced Packet Data Gateway (ePDG) that resides between the un-trusted access network and the EPC shown in fig 1.

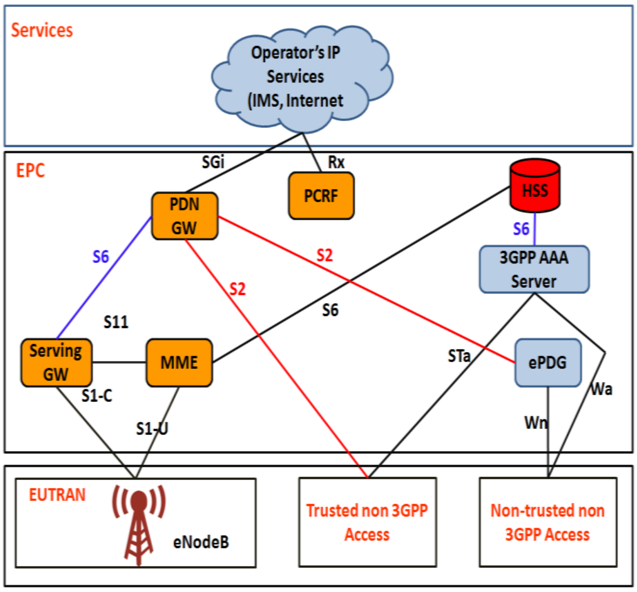

**Fig1: Architecture of non-3gpp accesses**

This ePDG provides confidentiality of the mobile node identity and encryption of data flows when the mobile node is sending traffic from within the un-trusted network.

Authentication of the mobile node is done by using Extensible Authentication Protocol–Authentication and Key Agreement (EAP-AKA), was developed as a secure authentication mechanism through Universal Subscriber Identity Module (USIM) for 3GPP devices connected to an IP network, such as Wi-Fi.

## 3. ECDH-ELLIPTIC CURVE DIFFIE HELLMAN

ECDH is a key agreement [8][9] protocol that allows two parties to establish a shared secret key that can be used for private key algorithms. Both parties exchange some public information to each other. Using this public data and their own private data, these parties calculates the shared secret. Any third party, who does not have access to the private details of each device, will not be able to calculate the shared secret from the available public information. An overview of ECDH process is defined below.

For generating a shared secret between **A** and **B** using ECDH, both have to agree up on Elliptic Curve domain parameters over field $\boldsymbol{F_2^m}$.

The domain parameters are:

- m: is an integer defined for finite field $F_2^m$ .
- f(x): is the irreducible polynomial of degree *m* used for elliptic curve operations
- a,b: are the parameters defining the curve chosen for cryptographic operations.
- *n*: is the order of the elliptic curve.

Both ends have a key pair consisting of a private key *d* (*a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter*) and a public key:

$Q = d * G$ (1)

*G :the generator point, an elliptic curve domain parameter.*

Let ($d_A$, $Q_A$) be the private key - public key pair of A and ($d_B$, $Q_B$) be the private key - public key pair of B.

- The end A computes:

  $K = (x_K, y_K) = d_A * Q_B$ (2)

- 2. The end B computes:

  $L = (x_L, y_L) = d_B * Q_A$ (3)

- Since $d_AQ_B = d_Ad_BG = d_Bd_AG = d_BQ_A$
- Therefore K = L and hence $x_K = x_L$ (4)
- . Hence the shared secret is $x_K$ (5)

Since it is practically impossible to find the private key $d_A$ or $d_B$ from the public key K or L, it's not possible to obtain the shared secret for a third party.

## 4. EAP-AKA

When the UE attempts to access Non-3GPP such as WLAN, the EAP-AKA [4] is used to support LTE-WLAN interworking.

The protocol and its vulnerabilities will be illustrated in this section, fig 2 shows the procedure of EAP-AKA.

### 4.1 Procedure

EAP- AKA provides mutual authentication between the user equipment (UE) and authentication, authorization and accounting (AAA) server.

Fig. 2 shows procedure of EAP-AKA that performs a procedure of authentication and key agreement between the cellular network and Non-3GPP.

From step 1 to 4 the connection is established with EAP request/identity and the subscriber is identified to the home subscriber server(HSS). From step 5 to 6, the AAA server requests again the user identity as immediate nodes can modify user identity (IMSI) included in EAP response/identity message. Therefore, if the UE receives EAP request/AKA identity message, the UE should send EAP response/AKA identity message which must contain the same user identity included response/identity message to the AAA server. The

AAA server will use user identity received from EAP response/AKA-identity message in the rest of the authentication and key agreement procedure. In Step 7, the AAA server checks the WLAN access profile and verifies that the subscriber is authorized to use the WLAN service.

From step 7 to 15 the challenge/response mechanism is applied to perform the mutual authentication between the AAA server and the UE.As the result of the success of the mutual authentication the master session key (MSK) is sent to the AP with success message.

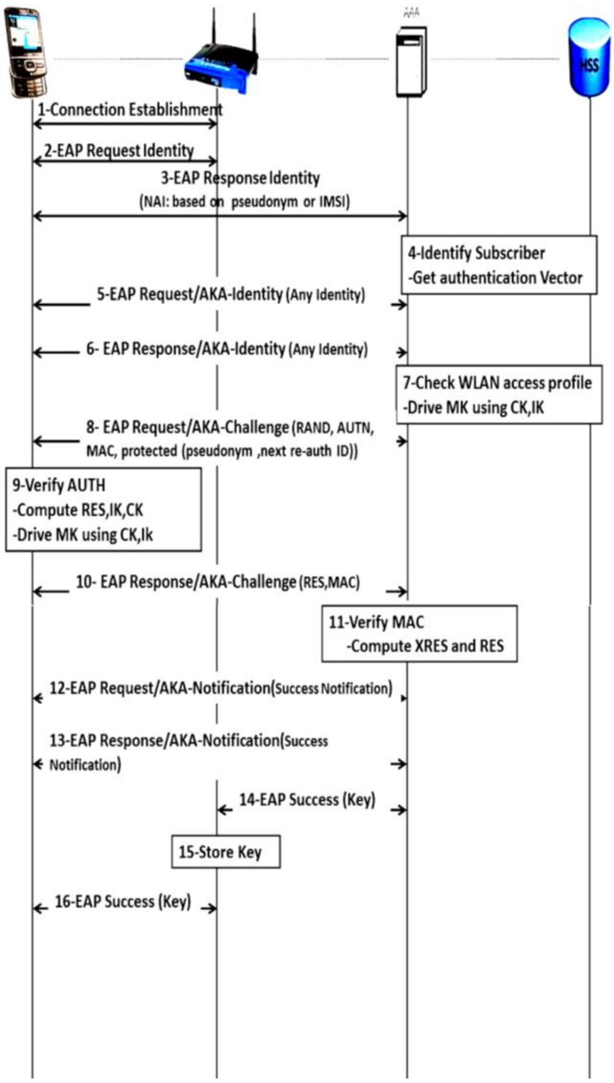
AAA
HSS
1-Connection Establishment
2-EAP Request Identity
3-EAP Response Identity
(NAI: based on pseudonym or IMSI)
4-Identify Subscriber
-Get authentication Vector
5-EAP Request/AKA-Identity (Any Identity)
6- EAP Response/AKA-Identity (Any Identity)
7-Check WLAN access profile
-Drive MK using CK,IK
8- EAP Request/AKA-Challenge (RAND, AUTN, MAC, protected (pseudonym ,next re-auth ID))
9-Verify AUTH
-Compute RES,IK,CK
-Drive MK using CK,Ik
10- EAP Response/AKA-Challenge (RES,MAC)
11-Verify MAC
-Compute XRES and RES
12-EAP Request/AKA-Notification(Success Notification)
13-EAP Response/AKA-Notification(Success Notification)
14-EAP Success (Key)
15-Store Key
16-EAP Success (Key)

**Fig2: Procedure of EAP-AKA**

## 4.2 EAP-AKA Vulnerabilities

### *4.2.1 Disclosure of User Identity (IMSI).*

The IMSI is sent from the UE to the AAA server as plain text, an attacker can capture the IMSI during the EAP-AKA procedure. The attacker can impersonates the UE afterwards and send the IMSI to the AAA server to gain some information .Also knowing the IMSI can be used in tracking the UE.

### *4.2.2 Man-In-The-Middle Attack.*

An attacker can impersonate an access point (AP) to receive EAP success message with master session key (MSK) from AAA server, causes man-in-middle attack.

### *4.2.3 Bandwidth Consumption.*

AAA server requests the user identity twice [step (3),(6)] before the challenge/response procedure ,which causes additional bandwidth consumption.

### *4.2.4 Perfect Forward Secrecy*

EAP-AKA uses symmetric key K shared between UE and home subscriber server (HSS) to perform integrity, authentication and key agreement. The encryption key (CK), Integrity key (IK), Master key (MK) and Mater Session Key (MSK) were generated using K. For this reason, disclosure of K will lead to the disclosure of all other generated keys. That is, EAP-AKA does not provide perfect forward secrecy (PFS).

### *4.2.5 Sequence Number (SQN) Synchronization*

If the received sequence number (SQN) is not in correct range, the UE should perform SQN synchronization procedure, which causes more bandwidth consumption.

# 5. PROPOSED PROTOCOL

Hyeran Mun et al. [10] proposed an authentication protocol based on ECDH, but their protocol depends on a lot of computations, which affect the performance of the system .The following proposed protocol (fig. 3) will reduce the number of computations needed to complete the procedure while maintaining the same level of security as Hyeran Mun et al. protocol and will also prevent disclosure of MSK in the air interface between UE and AP.

## 5.1 Assumptions

In our proposed protocol, we assume the following:

- A secure channel is established between the AAA server and the HSS.
- The UE can identify the ID of AAA server and AP in which the UE in its range of coverage.

## 5.2 Procedure

- **Step 1.** UE searches for the ID of the intended AP, when it finds the AP, the UE sends start message to start the authentication mechanism.
- **Step 2.** The AP requests the UE Identity.
- **Step 3.** The **UE** will do the following:
  a) Generates a random value (RAND)
  b) Generates a temporary key ($K_{TEMP}$) by encrypting the random value using the pre-shared key between the the UE and the home server.

  $K_{TEMP}= E_{K_{UE\text{-}HSS}} (T_U)$

  c) Encrypts its ID (IMSI), concatenated with the timestamp $T_{U1}$.

  $ID_{enc}=E_{K_{TEMP}} (IMSI||T_U)$.

  d) UE sends its encrypted ID ($ID_{enc}$), timestamp ($T_U$), ID of the access point ($ID_{AP}$) and the ID of the home server ($ID_{HSS}$) to the HSS.
- **Step 4.** The **HSS** will do the following:
  a) Retrieves a plain header in the $ID_{enc}$ called (key-indicator) and finds the corresponding key to the indicator ($K_{UE\text{-}HSS}$).
  b) Calculates $K_{TEMP}$=E $_{K_{UE\text{-}HSS}}$ (TU).
  c) Decrypts $ID_{enc}$ , retrieves timestamp ($T_U$) and compare it to the ($T_U$) received in step (5) and checks that ($T_U$) is the same.
  d) Generates a random number ($N_{HSS}$).

e) Computes $AUTH_{AAA}$ as follows:

$AUTH_{HSS}$=

$MAC_{\mathbf{K}_{UE\text{-}HSS}}$ $(N_{HSS}||ID_{HSS}||ID_{AP}||ID_{AAA})$

- **Step 5.** HSS Sends ( $N_{Hss}$ ,$K_{TEMP}$ ,$ID_{AP}$, $AUTH_{HSS}$) to the $WLAN_{AAA}$ .
- **Step 6.** The $\mathbf{WLAN_{AAA}}$ will do the following:

a) Stores $K_{TEMP}$ and $ID_{AP}$.

b) Generates a random value ($N_{AAA}$).

c) Computes:

$AUTH_{AAA}$=

$MAC_{K_{TEMP}}(N_{AAA}||N_{HSS}||ID_{HSS}||ID_{AP}||ID_{AAA})$.

d) Generates a random value ***a*** and computes ***aP*** on ***E***.

- **Step 7.** The $WLAN_{AAA}$ Sends the ($N_{HSS}$,$N_{AAA}$,$AUTH_{AAA}$,$AUTH_{HSS}$,***aP***) to the UE.
- **Step 8.** The **UE** will do the following**:**

a) Authenticate HSS by verifying $AUTH_{HSS}$.

b) Authenticate $WLAN_{AAA}$ by verifying $AUTH_{AAA}$.

c) Generates a random number ($N_{UE}$).

d) Generates a random value ***b*** and computes ***bP*** on ***E***.

e) Computes $K_{UE\text{-}AAA}=f_{K_{TEMP}}(\boldsymbol{abP})$.

f) Computes

$AUTH_{UE}$ =

$MAC_{K_{UE\text{-}AAA}}$

$(N_{UE}||N_{AAA}||N_{HSS}||ID_{HSS}||ID_{AP}||ID_{AAA})$.

g) Computes CK, IK, and MSK.

- **Step 9.** UE Sends ($AUTH_{UE}$ , ***bP*** , $N_{UE}$) to $WLAN_{AAA}$ server.
- **Step 10.** The $\mathbf{WLAN_{AAA}}$ will do the following**:**

a) Computes $K_{UE\text{-}AAA}=f_{K_{TEMP}}(\boldsymbol{abP})$.

b) Authenticates UE by verifying $AUTH_{UE}$.

c) Computes CK, IK and finally MSK.

- **Step 11.** The $WLAN_{AAA}$ sends the MSK concatenated with $ID_{AP}$ with EAP success message to the AP ,and also sends the MSK concatenated with $ID_{AP}$ encrypted with $K_{UE\text{-}AAA}$ to the UE, so the MSK will not be compromised in the air interface between the AP and the UE .
- **Step 12.** The AP stores the MSK and forwards ($MSK||ID_{AP}$) with the EAP success message to the UE.
- **Step 13.** The UE decrypts the MSK received from the AP and verifies if it is equals the MSK calculated in step (7) and also verifies that the $ID_{AP}$ received equals the $ID_{AP}$ sent in step (3).If the verification is correct, then the procedure of the authentication and key agreement is successful and the UE can use WLAN services securely via the MSK.

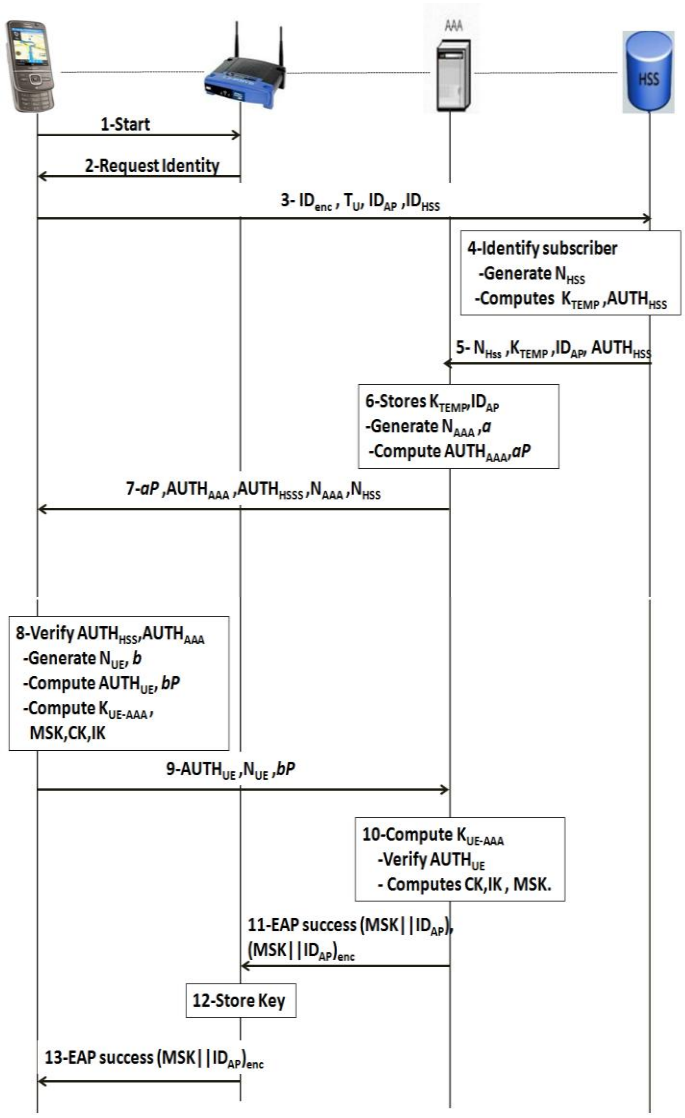

**Fig 3: Proposed protocol**

# 6. ANALYSIS AND COMPARISON

## 6.1 Security Analysis

### *6.1.1 User identity Protection (encrypted IMSI)*

The user identity is protected and can't be captured by attackers. The UE generates $ID_{enc}$ concatenated with a timestamp. The timestamp protects the temporary ID from being captured and send in later time.

### *6.1.2 Secure Against Man-In-The-Middle Attack.*

The attacker cant retrieve the IMSI from the IDenc as it does not possess the encryption key (KUE-HAAA), and the attacker can't re-send the IDenc in later time due to the presence of the timestamp.

### *6.1.3 Provide Perfect Forward Secrecy (PFS)*

The proposed protocol uses ECDH in generating session key, so revealing KUE-HSS will not lead to revealing any of the session keys, as there is no relation between KUE-HSS and the elliptic curve keys. Moreover the MSK in the last step of the authentication and key agreement procedure is sent encrypted using KUE-HSS to avoid disclosure of MSK in the air interface.

### 6.1.4 *Provide Mutual Authentication*

UE authenticates $\text{WLAN}_{\text{AAA}}$ and HSS: The UE can authenticate $\text{WLAN}_{\text{AAA}}$ and HSS by verifying $\text{AUTH}_{\text{AAA}}$ and $\text{AUTH}_{\text{HSS}}$ respectively, which occurs in step (8).

WLANAAA and HSS authenticate UE: The HSS verifies the encrypted IMSI of the UE, and the $\text{WLAN}_{\text{AAA}}$ verifies $\text{AUTH}_{\text{UE}}$.

### 6.1.5 *Secure Against Replay Attack*

The HSS verifies that the timestamp (TU) is in the correct range that occurs in step (6) ,that makes the proposed protocol secure against replay attacks.

## 6.2 Performance Analysis

### 6.2.1 *Reduce number of computations*

The number of computations needed to complete the authentication and key agreement procedure are decreased in comparison to Hyeran Mun et al. protocol.

The number of computations and exchanged messages in both protocols are shown in the following table.

**Table 1. Performance comparison**

| **Proposed protocol** | **Number of exchanged messages** | **Number of computations** |
|---|---|---|
| | 8 | 27 |
| **Hyeran Mun et al. protocol** | 8 | 32 |

### 6.2.2 *Elimination of SQN Synchronization*

The proposed protocol does not use SQN mechanism in synchronization which is a great add to the bandwidth consumption.

### 6.2.3 *Use of Elliptic Curve Deffie-Hellman(ECDH):*

The proposed protocol combines ECDH with symmetric key cryptosystem to provide secure communication between 3G and Non-3GPP. ECDH provides the same security properties and uses fewer resources than other public key cryptosystems with certificates. In the proposed protocol, the UE and the AAA server only stores and manages a, b, aP, and bP.

## 7. Future work

The performance of the proposed protocol will be examined in the LTE environment using the OPNET simulation tool, to ensure that the protocol will not affect the quality of service.

## 8. Conclusion

In this paper, the vulnerabilities of EAP-AKA used in 3G-WLAN interworking were presented and a new authentication and key agreement protocol based on EAP-AKA was proposed. The proposed protocol combines ECDH with symmetric key cryptosystem to overcome different vulnerabilities of EAP-AKA. The proposed protocol provides PFS to enhance the security, mutual authentication between the UE and the AAA server and between the UE and the HSS, and resistance to replay attack, with fewer computations compared to other protocols using ECDH.

## References

[1] Third Generation Partnership Project (3GPP), 3GPP TS 33.401 v8.1.1 “3G System Architecture Evolution (SAE): Security architecture (Release8)”, October 2008

[2] Third Generation Partnership Project (3GPP), 3GPP TS 33.821 v1.0.0 “ Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE) (Release 8)” , December 2007

[3] Third Generation Partnership Project (3GPP), 3GPP TS 33.102 v8.0.0 “3G Security: Security Architecture (Release 8)”, June 2008

[4] J. Arkko, H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, IETF RFC 4187, January 2006

[5] Third Generation Partnership Project (3GPP), 3GPP TS 23.234 v8.1.0 “3G security: Wireless Local Area Network (WLAN) Interworking Security (Release 8)”, March 2008

[6] Third Generation Partnership Project (3GPP), 3GPP TS 33.402 v8.3.0 “Architecture Enhancements for non-3GPP accesses (Release 8)”, September 2008

[7] *LTE Security* Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niemi © 2010 John Wiley & Sons, Ltd

[8] Cryptography and Network Security, William Stallings© 2007 Prentice Hall.

[9] Elliptic Curve Cryptography An Implementation Guide http://tataelxsi.com/whitepapers/ECC_Tut_v1_0.pdf.

[10] Hyeran Mun, Kyusuk Han, and Kwangjo Kim, "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA", 2009 IEEE Wireless Telecommunications Symposium .