# Formal Analysis of A Novel Mutual Authentication and Key Agreement Protocol

Ja'afer M. AL-Saraireh
Applied Science University
Amman 11961, Jordan
Saleh S. Saraireh
Philadelphia University
Amman 11961, Jordan
Mohammad S. Saraireh
Mutah University
Mutah 61710, Jordan
Mohammad M. AL Nabhan
Jarash University
Amman 11961, Jordan

**ABSTRACT**

This research work analyzes the universal mobile telecommunication system (UMTS) authentication and key agreement (AKA) protocol, which suffers from the traffic bottleneck at home location register and authentication center (HLR/AuC). In addition, serving network has no capability to authenticate mobile station. To overcome these problems a new security scheme has been proposed which provides a more efficient and a secure authentication between mobile station and home networks, the proposed protocol called Efficient AKA (E-AKA).

The E-AKA uses a temporary key to enable visitor location register and serving network (VLR/SN) to authenticate mobile station (MS) without intervention of HLR/AuC. To analyze and validate the security of the proposed protocol, the BAN (Burrows, Abadi and Needham) logic is used. The results show that the E-AKA protocol is more robust than the current AKA protocol.

**Keywords:** 3G, Authentication, Security, Mobile Station, and BAN.

## 1. INTRODUCTION

Authentication is used to provide security services in wireless mobile networks, it is considered as an initial process to authorize a mobile terminal for communication through secret credentials [1]. The authentication process provides a reasonable level of security, but it overloads the network with significant signalling traffic and increases the call setup time [1].

The current mechanism for security authentication in 3G system is known as AKA protocol. In this mechanism a secret key (***K***), and cryptographic algorithms are shared between ***MS*** and HN [1, 2]. The AKA protocol has many weaknesses such as, the transmission between the ***HN*** and ***SN*** is usually expensive, the authentication vectors (***AVs)*** consume network bandwidth for each transmission from authentication centre to ***SN*** [3], the storage space overhead occurs in ***SN***, and bottleneck at ***HN***, the ***HN*** is responsible for generating authentication vectors upon receipt of requests from all ***SN***.

Responding to the weakness mentioned above, by referring to the current authentication method and improving the proposed scheme, this research work proposes a novel efficient and secure authentication scheme. Furthermore, the objective and security of the proposed scheme are analyzed by the formal analytical process of the BAN logic.

This paper is organized as follows. Section 2 illustrates the UMTS AKA. The literature review is presented in section 3. In section 4, the efficient and secure AKA scheme is described. Formal analysis for the proposed scheme by using BAN logic is introduced in section 5. The paper is concluded in Section 6.

## 2. UMTS AKA PROTOCOL

In AKA protocol, each MS shares secret key (***K***), and cryptographic algorithms - include three message authentication codes $f_1$, $f_1$*and $f_2$ and four key generation functions $f_3$, $f_4$, $f_5$ *and* $f_5$*- with its ***HN*** [1, 4].

The goals of the UMTS AKA protocol are, a mutual authentication between user and the network; an establishment of a cipher key and an integrity key; and established cipher and integrity keys [1, 4].

There are two phases in AKA protocol, the first phase is the generation and distribution authentication vectors from the ***HN*** to the ***SN***, and the second phase is the authentication and key agreement procedure between the MS and the SN [2, 5]. An overview of UMTS AKA is shown in figure 1 [6].

Mobile station (***MS***) sends authentication request to the ***SN***, which includes International Mobile Subscriber Identity ***(IMSI)***. ***SN*** passes this authentication request to ***HN***. ***HN*** sends authentication data response to ***SN***, which include authentication vector (***AV***). Each authentication vector has five components: random number (***RAND***), expected response (***XRES***), cipher key (***CK***), integrity key (***IK***) and authentication token (***AUTN***). The authentication vectors are ordered by the sequence number $SQN_{HLR}$. The authentication vector is generated according to the following steps [6, 7]:

i. ***HN*** set ***SQN*** to $SQN_{HN}$ and generates ***RAND***.
ii. ***HN*** computes the following values: ***XRES***, ***CK***, ***IK***, ***AK,*** and ***MAC***
iii. ***HN*** assembles the authentication token $AUTN = (SQN \oplus AK || AMF || MAC)$ and the authentication vector (***RAND,XRES, CK, IK, AUTN***)
iv. ***HN*** increments $SQN_{HLR}$ by 1.

***SN*** is receiving response from ***HN*** and then storing ***AV***. The ***SN*** selects the $i^{th}$ authentication vector ***AV(i)***, and sends (***RAND (i), AUTN(i)***) to ***MS***. Each authentication vector is efficient for one authentication process [6].

***MS*** is receiving ***RAND*** and ***AUTN*** from ***SN***. ***MS*** computes and retrieves the anonymity key ***AK***, ***SQN,*** expected message authentication code ***XMAC***. The ***MS*** compares ***XMAC*** with ***MAC*** which is included in ***AUTN***. If they are different, then ***MS*** sends failure message to the ***SN***. Otherwise, ***MS*** checks that the received ***SQN*** is in the correct range. If the ***SQN*** is not in the correct range, then ***MS*** sends failure message to the ***SN***. Otherwise, if the ***SQN*** in correct range, the ***MS*** computes ***RES*** and sends it to ***SN***. Lately, ***MS*** computes ***CK*** and ***IK.***

***SN*** is receiving authentication response from ***MS***. ***SN*** compares the received ***RES*** with ***XRES*** in authentication vector. If ***RES*** is matching ***XRES***, then authentications is successfully completed and select the ***CK*** and ***IK*** from authentication vector. If ***RES*** is unequal ***XRES***, ***SN*** sends authentication failure to the ***HN***.

## 3. RELATED WORK

The UMTS AKA protocol has the problem of the bandwidth consumption between ***SN*** and ***HN***. It is attractive to choose a suitable length (***L***) value for ***AV*** in the third generation mobile networks. So, many techniques are developed to minimize the authentication signalling cost and network bandwidth consumption by selecting dynamic length (***L***) for an authentication vector [1, 5, 6, and 8]. But with this improvement by [5, 9] there are still a bandwidth consumption [6].

The technique of Lin and Chen basically estimated the number of authentication requests in current visited network based on the number in the previous visited network. Whereas the method of AL-Saraireh and Yousef, estimated the number of authentication requests in current visited network based on the history of mobile movements and the arrival rate for events [5].

Juang and Wu proposed an efficient 3GPP AKA with robust user privacy. A temporary key to authenticate ***MS*** and prevent the location privacy attack is used. In this proposed protocol, the ***VLR*** initiates the authentication process by sending a random number to the ***MS*** without using any ***MAC***. [10] Therefore denial of services (DoS) attack is possible. Additionally, the proposed protocol has seven steps.

A new UMTS AKA protocol called EAKAP is proposed in [11]. The EAKAP combines identification stage and AKA stage of UMTS AKA protocol. The problem in EAKAP is that the size of messages between ***MS, VLR/SGSN*** and ***HLR/AuC*** is increased. Therefore; the consumption of bandwidth is occurred. Subscriber identity/location confidential and non-repudiation services are solved by [12], the proposed scheme integrates symmetric and public key cryptosystem. An Enhancement for UMTS AKA protocol is proposed by Harn and Hsin used hash chaining technique instead of using ***AVs*** [9].

## 4. THE EFFICENT SCHEME E-AKA PROTOCOL

E-AKA is used to eliminate the security weakness involved with UMTS AKA. E-AKA is considered as a secure and an efficient authentication scheme. In the E-AKA scheme ***VLR/SN*** has the capability to authenticate the user without intervention of ***HLR/HN***.

The E-AKA uses a new key generation functions called $f_x$ to generate the temporary key (***TK***). The $f_x$ function produces a 128 bits or higher bits to provide high level of security. In the proposed protocol, the ***SN*** is able to authenticate the ***MS*** after the initial authentication has been performed. The proposed authentication protocol contains two operation modes for initial and subsequent authentication. The first mode is registration and distribution of authentication information (Initial Authentication) and temporary key (***TK***) from the ***HLR/HN*** to the ***VLR/SN***. The second mode is the authentication and key agreement procedure (Subsequent authentication) performed between the ***MS*** and the ***VLR/SN***.

Figure 2 and 3 describe authentication mechanism for the proposed protocol. The authentication procedure is described as follow:

Step 1: Authentication Request Message:

When ***MS*** needs authentication to network, to access or use to use the network services, the initial authentication is carried out as follow:

1.1 ***MS*** generates random number $(Rand_{MS})$,
1.2 ***MS*** computes the Message Authentication Code $MAC_{MS} = f_1(K, Rand_{MS})$,
1.3 ***MS*** sends ***IMS,*** $Rand_{MS}$ and $MAC_{MS}$ as authentication request to ***VLR/SN***.

Step 2: Authentication Request Message:

***VLR/SN*** passes this authentication request to ***HLR/HN***.

Step 3: Authentication Response Message:

Receiving the authentication request and then verification procedure is performed by ***HLR/HN***. A response message is generated. The following operations are carried by ***HLR/HN***:

3.1 Compares and computes expected message authentication code for mobile station $(XMAC_{MS})$ to verify the received message.

$$XMAC_{MS}=f_1(K, Rand_{MS})$$
$$XMAC_{MS} ?= MAC_{Ms}$$

If mismatching occurs then the registration will fail otherwise it will execute the next steps.

3.2 Generates $SQN_{HLR}$ and $RAND_{HLR}$.

3.3 Computes expected response $XRES_{HLR} = f_2(K,RAND_{HLR})$, Anonymity Key $AK_{HLR} = f_5(K,RAND_{HLR})$, Message Authentication Code $MAC_{HLR} = f_1(K,SQN||RAND_{HLR}||MAF)$, where ***MAF*** is Message Authentication Field and authentication token $AUTN_{HLR} = (SQN \oplus AK_{HLR}||AMF||MAC_{HLR})$ where $\oplus$ is exclusive OR operation.

3.4 Computes temporary key $TK = f_x(K,RAND_{HLR})$.

3.5 Sets response messages and sends it to ***VLR/SGSN***, including one authentication vector ***AV***. This ***AV*** consists of four components: $RAND_{HLR}$, $XRES_{HLR}$, ***TK*** and $AUTN_{HLR}$.

$$AV = RAND_{HLR}|| XRES_{HLR}||TK|| AUTN_{HLR}$$

Step 4: Authentication Response Message:

Receiving the response message from ***HLR/HN***, ***VLR/SN*** will invoke the authentication to the ***MS***. ***VLR/SN*** will achieve the following:

4.1 Stores the ***TK***, $AUTN_{HLR}$ and generates $Rand_{VLR}$.

4.2 Computes $MAC_{VLR}=f_1(TK, MAC_{HLR}||Rand_{VLR})$ where the $MAC_{HLR}$ retrieved from $AUTN_{HLR}$ which stored in previous step.

4.3 Computes $AUTN_{VLR} = (SQN_{HLR} \oplus AK_{HLR}||AMF||MAC_{VLR})$

4.4 ***VLR/SN*** sends $AUTH_{VLR}$, $Rand_{VLR}$ and $Rand_{HLR}$ to ***MS***

Step 5: Authentication Response Message:

When ***MS*** receives the messages, the ***MS*** will achive the following:

5.1 Computes $TK=f_x(K, Rand_{HLR})$.

5.2 Verifies that the received sequence number ***SQN*** is in the correct range. If the ***MS*** considers the sequence number to be not in the correct range, it sends synchronization failure back to the ***VLR/SN*** including an appropriate parameter, and abandons the procedure.

5.3 Computes ***XMAC*** for ***HLR*** and ***VLR.***

$XMAC_{HLR} = f_1(K, AK_{MS} \oplus (SQN_{HLR} \oplus AK_{HLR})||Rand_{HLR}|| AMF)$ where $Rand_{HLR}$ and ***AMF*** are retrieved from $AUTN_{VLR}$

$XMAC_{VLR} = f_1(TK,XMAC_{HLR}||Rand_{VLR})$.

If $XMAC_{VLR}$ is equal $XMAC_{VLR}$ then ***HLR/HN*** and ***VLR/SN*** are valid,

5.4 Computes an $XRES = f_2(TK, Rand_{VLR})$

5.5 Sends ***XRES*** to ***VLR/SN***. While, the ***MS*** computes an integrity key as $IK = f_3(TK, Rand_{VLR})$ and a cipher key as $CK = f_4(TK, Rand_{VLR})$ to realize securely communication with ***VLR/SN*** subsequently.

Step 6: Authentication Response Message:

***VLR/SN*** receives the messages from ***MS*** and verifies whether ***RES*** is identical to the ***XRES***. If it is true, the whole authentication is successfully completed. If it is false, the authentication is failed.

After the initial authentication, both the ***VLR/SN*** and ***MS*** obtain the authentication result from the ***HLR/HN*** and share some secret information. Here, the ***VLR/SN*** caches some authentication information, which can be used in subsequent authentication without intervention of ***HLR/HN***.

After initial authentication, the ***VLR/SN*** has the ability to authenticate the ***MS*** in subsequent authentication. If the ***MS*** remains in the same ***VLR/SN*** and requests services, then the user should ask for subsequent authentication. ***MS*** similarly generates an authentication request message, which should contain the information shared between the ***MS*** and ***VLR/SN***; the ***VLR/SN*** uses this information to authenticate the ***MS***. ***VLR/SN*** authenticates ***MS*** by using temporary key ***TK***.

As mentioned above, the ***VLR/SN*** has cached information needed to authenticate ***MS***. After authenticating the ***MS***, the ***VLR/SN*** sends a response message containing the authentication result to the ***MS***. The ***MS*** receives the response message and learns whether the authentication was successful or not. The subsequent authentication is described as follows:

Step 1: Authentication Request Message

***MS*** sends authentication request to ***VLR/SN***

Step 2: Authentication Request Message

When ***VLR/SN*** receives the request message, ***VLR/SN*** will do the following:

2.1 Generates $Rand_{VLR}$

2.2 Computes authenticate token $AUTN = SQN \oplus AK||AMF||MAC$

Where $AK = f_5(TK,RAND)$, and $MAC = f_1(TK,SQN||RAND||MAF)$.

2.3 Sends ***AUTN*** and ***RAND*** to ***MS***.

Step 3: Authentication Response Message

When ***MS*** receives the response message, ***MS*** will achieve the following:

3.1 Computes and retrieves the $AK = f_5(TK, Rand)$, $SQN = (SQN \oplus AK) \oplus AK)$, and $XMAC = f_1(SQN, RAND, AMF)$

3.2 Compares ***XMAC*** with ***MAC*** which is included in ***AUTN***. If ***XMAC*** is not equal to ***MAC*** then ***MS*** sends failure message to the ***VLR/SN***, else if ***XMAC*** is equal ***MAC*** then ***MS*** checks that the received ***SQN*** is in the correct range i.e. $SQN > SQN_{MS}$. If ***SQN*** is not in the correct range then ***MS*** sends failure message to the ***VLR/SN***, else if it is in the correct range, then ***MS*** computes the Response $RES = f_2(TK, RAND)$, and $CK = f_3(TK, Rand)$. After that, it sends ***RES*** to ***VLR/SN.***

Step 4: Authentication Response Message

***VLR/SN*** receives the messages from ***MS*** and verifies whether ***RES*** is identical to the ***XRES***. If it is true, the whole authentication is successfully completed. If it is false, the authentication is failed.

## 5. FORMAL ANALYSIS OF E-AKA

BAN logic represents a powerful tool to describe and validate authentication protocols. In this research work BAN logic is used to formalize and prove the security of the proposed protocol. BAN Logic [13] is a formal method for verifying that two principles (MS, VLR/SN, HN/HLR) are entitled to believe they are communicating with each other. It is based on an agreed set of deduction rules for formally reasoning about the authentication protocols and is often referred to as logic of authentication [7, 13, and 14].

### 5.1. BAN LOGIC NOTATION AND DEDUCTION RULES

The definitions of BAN logic and their implications are presented below (*P* and *Q* are network agents, *X* is a message, and *K* is an encryption key) [7, 13, and 14]:

- $P \models X$ : Denotes that *P* believes *X*. *P* may act as though *X* is true.
- $P \lhd X$ : Denotes that *P* sees *X*. Someone has sent *P* a message containing *X*. *P* can read *X* and can repeat it in other messages.
- $\#(X)$ : Denotes that *X* is fresh. *X* has not been sent in a message at any time before the current run of the protocol.
- $P \Rightarrow X$ : Denotes that *P* control *X; P* has jurisdiction over *X*. P is a trusted authority on the truth of X.
- $P \mid\sim X$ : Denotes that *P* said *X*. At one time, *P* transmitted (and believed) message *X*, although *P* might no longer believe *X*.
- $P \models Q \mid\sim (X, Y) / P \models Q \mid\sim X$ :
- $P \xleftrightarrow{K} Q$ : Denotes that *K* is a good shared key for communication between *P* and *Q*, and it will never be discovered by any principal except for *P* or *Q*.
- $\overset{K}{\mapsto} P$ : Denotes that *K* is the public key of *P*.
- $\{X\}_K$ : Denotes that *X* is encrypted with key *K*.
- $\frac{P}{Q}$ : Means if *P* is true then *Q* is true.

Some deduction rules that are used in the analysis of proposed scheme are described as follow [7, 14, and 15]:

- **Message meaning rules:** this rule concerns the interpretation of messages. This rule helps to explain the origin of the messages. For shared keys:

$$\frac{P \models P \xleftrightarrow{K} Q, \quad P \lhd \{X\}_K}{P \models Q \mid\sim X}$$

- **Nonce verification rules:** this rule checks that a message is recent, and also checks if the sender still believes in it. $\frac{P \models \#(X), \quad P \models Q \mid\sim X}{P \models Q \models X}$
- **Jurisdiction rules:** This rule states what it means for a principal to be the trusted authority on the truth of X.

$$\frac{P \models Q \mid\Rightarrow X, \quad P \models Q \models X}{P \models X}$$

- **Seeing rules:** This rule says that a principal sees all the components of every message it sees, provided that the principal knows the necessary key

$$\frac{P \lhd (X, Y)}{P \lhd (X)}$$

$$\frac{P \models P \xleftrightarrow{K} Q, \quad P \lhd \{X\}_K}{P \lhd X}$$

- **Belief rules:** The rule states that a principal believes a collection of statements if and only if it believes

each of the statements individually.

$$\frac{P \mid\equiv (X, Y)}{P \mid\equiv (X)}$$

The following steps of BAN logic has been used to analyze the proposed protocol:

i. The proposed protocol is transformed into idealized form
ii. Identify our initial assumptions in the language of BAN logic
iii. Use the postulates and rules of the logic to deduce new predicates
iv. Interpret the proved statements by the process? Have the goals met?

### 5.2. SECURITY PROOF

By using the notation and deduction rules in section 5.1, the protocol security can be proved. The original version of the proposed scheme without idealization form is as following:

Message 1

$$MS \rightarrow VLR / SN : IMSI, Rand_{MS}, MAC_{MS}$$

Message 2

$$VLR / SN \rightarrow HLR / HN : IMSI, Rand_{MS}, MAC_{MS}$$

Message 3

$$HLR / HN \rightarrow VLR / SN : Rand_{HLR}, XRES_{HL} R, TK, AUTH_{HLR}$$

Message 4

$$VLR / SN \rightarrow MS : Rand_{VLR}, Rand_{HLR}, AUTH_{VLR}$$

**Step 1: Idealized Form:** The ideal form of protocol using BAN logic is:

$$HLR / HN \lhd (IMSI, Rand_{Ms}, MAC_{MS})$$

$$VLR / SN \lhd (Rand_{HLR}, XRES_{HLR}, TK, AUTH_{HLR})$$

$$MS \lhd (Rand_{VLR}, Rand_{HLR}, AUTH_{VLR})$$

**Step 2: Initial Hypothetical:** The initial supposition on the protocol as follows**:**

$$MS \xleftrightarrow{K} HLR / HN$$

The temporary key is used in proposed E-AKA protocol to reduce the traffic between ***HLR/AuC*** and

**Step 3: Final Goal Set:**

$$MS \mid\equiv MS \xleftrightarrow{K} HLR / HN \ldots\ldots\ldots\ldots\ldots (G1)$$

$$MS \mid\equiv MS \xrightarrow{TK} VLR / SN \ldots\ldots\ldots\ldots\ldots (G2)$$

**Step 4: Form Analysis of Proposed Protocol:**

According to initial assumption $MS \xleftrightarrow{K} HLR / HN$ and message meaning rule $\frac{P \mid\equiv P \xleftrightarrow{K} Q, \quad P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$, it can be deduced the first goal as follows:

$MS \mid\equiv HLR / HN \mid\sim XMAC_{HLR}$, Use $MAC_{MS} = XMAC_{HLR}$ to obtain the following $MS \mid\equiv MS \xleftrightarrow{K} HLR / HN$ which is the first goal (G1)

To deduce the second goal (G2):

$MS \mid\equiv \xrightarrow{TK} VLR / SN$. By using the following three rules

1. First goal
   $MS \mid\equiv MS \xleftrightarrow{K} HLR / HN$ and
2. Seeing rule:
   $\frac{P \mid\equiv P \xleftrightarrow{K} Q, \quad P \lhd \{X\}_K}{P \lhd X}$ and
3. Jurisdiction rule:
   $$\frac{P \mid\equiv Q \mid\Rightarrow X, \quad P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$
   to obtain

$MS \mid\lhd \xrightarrow{XMC_{VLR}} VLR / SN$, use $MS \mid\equiv VLR / SN \mid\sim MAC_{VLR}$ and $MAC_{VLR} = XMAC_{VLR}$ to obtain the following: $MS \mid\equiv \xrightarrow{TK} VLR / SN$ which is the second goal (G2).

According to the given analysis, the proposed protocol can be considered secure.

## 5. CONCLUSION

In this research work, the current UMTS authentication and key agreement protocol have been analyzed, and showed that it has set of weaknesses. The new authentication scheme provides a solution for these weaknesses. The proposed protocol provides a mutual authentication between mobile station and its home network and serving network. The signalling traffic is reduced between home network and serving network by using temporary key. The serving network has capabilities to authenticate mobile station without intervention from home network. The proposed protocol has been improved and formalized by using BAN logic.

## 6. REFERENCES

1. Al-Saraireh J. & Yousef S., (2006) "A New Authentication Protocol for UMTS Mobile Networks", *EURASIP Journal on wireless communications and networking,* Vol. 2006, pp1-10.

2. Zhang M. & Fang Y., (2005) "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", *IEEE Transactions on wireless communications*, Vol. 4, No. 2, pp734–742.
3. Lin Y & Chen Y., (2003) "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network", *IEEE Transactions on Wireless Communications*, Vol. 2, No. 3, pp493-501.
4. Huang Y., Shen Y., Shieh S., Wang H. & Lin C., (2009)"Provable Secure AKA Scheme with Reliable Key Delegation in UMTS", *Secure Software Integration and Reliability Improvement, 2009. SSIRI 2009. Third IEEE International Conference,* Vol. 2009, pp243-252.
5. Al-Saraireh J. & Yousef S., (2007) "Analytical Model: Authentication Transmission Overhead between Entities in Mobile Networks", *Elsevier, Computer Communications Journal*, Vol. 30, No. 9, pp1713-1720.
6. Al-Saraireh J., (2011) "Efficient and Secure Authentication and Key Agreement Protocol", *International Journal of UbiCom (IJU),* Vol. 2, No. 2.
7. Li H., Guo S., Zheng K., Chen Z. & Cui J., (2009) "Improved Adoptable Scheme for Authentication and Key Agreement", *IEEE International Conference on Management and Service Science (MASS 2009)*, pp. 1-4, print ISBN: 978-1-14244-4638-4, DOI: 10.1109/ICMSS.2009.5301997
8. GPP TS 33.102 V8.0.0, (2008) "3GPP Technical Specification Group Services and System Aspects, 3G Security, Security Architecture (Release 8)", *3rd Generation Partnership Project.*
9. Harn L. & Hsin W., (2003) "On the security of wireless network access with enhancements", *in Proceedings of the 2003 ACM workshop on Wireless security, San Diego, USA, Sep. 19 2003*, pp88–95.
10. Juang W.S. & Wu J.L., (2007) "Efficient 3GPP Authentication and Key Agreement with Robust User Privacy Protection", *IEEE Communications Society, Proceedings of the WCNC*.
11. Farhat F., Salimi S. & Salahi A., (2009) "An Extended Authentication and Key Agreement Protocol of UMTS", *Information Security Practice and Experience, Lecture Notes in Computer Science*, Vol. 5451/2009, pp230-244, DOI: 10.1007/978-3-642-00843-6_21
12. Min-Shiang H., Song-Kong C. & Hsia-Hung O., (2010) "On the security of an enhanced UMTS authentication and key agreement protocol", *European Transactions on Telecommunications*. DOI: 10.1002/ett.1460
13. Burrows M., Abadi M., & Needham R., (1989) "A logic of Authentication", *Digital Systems Research Center.*
14. Zhang J., Chen G., & Deng F., (2008) "A New Mutual Authentication and Key Agreement Protocol for Mobile Communications", *International Conference on Wireless Communications, Networking and Mobile Computing (IEEE WICOM 2008)*, pp. 1-3. ISBN 978-1-4244-2107-0, DOI: 10.1109/WiCom.2008.2124
15. Chang C., Pan H., Jia H., (2008) "A Secure Message Communication Protocol". *International Journal of Automation and*


Received: May 2011. Accepted: Sep. 2011.

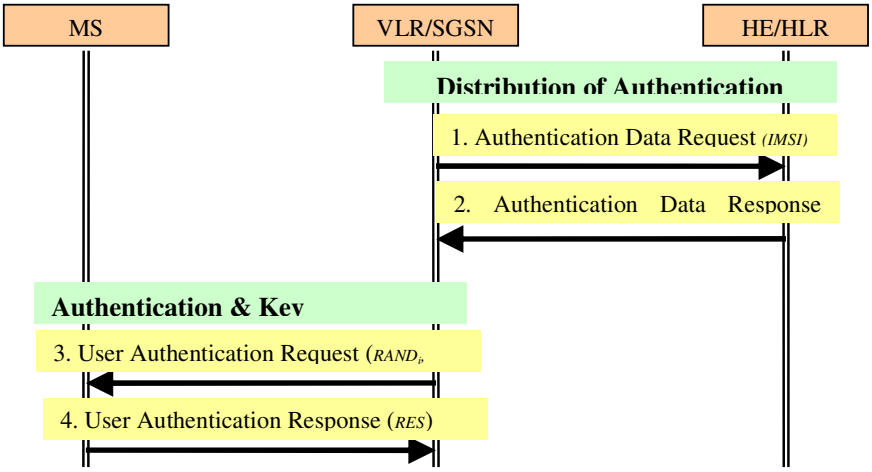


Figure 1: The Authentications and key agreement protocol.

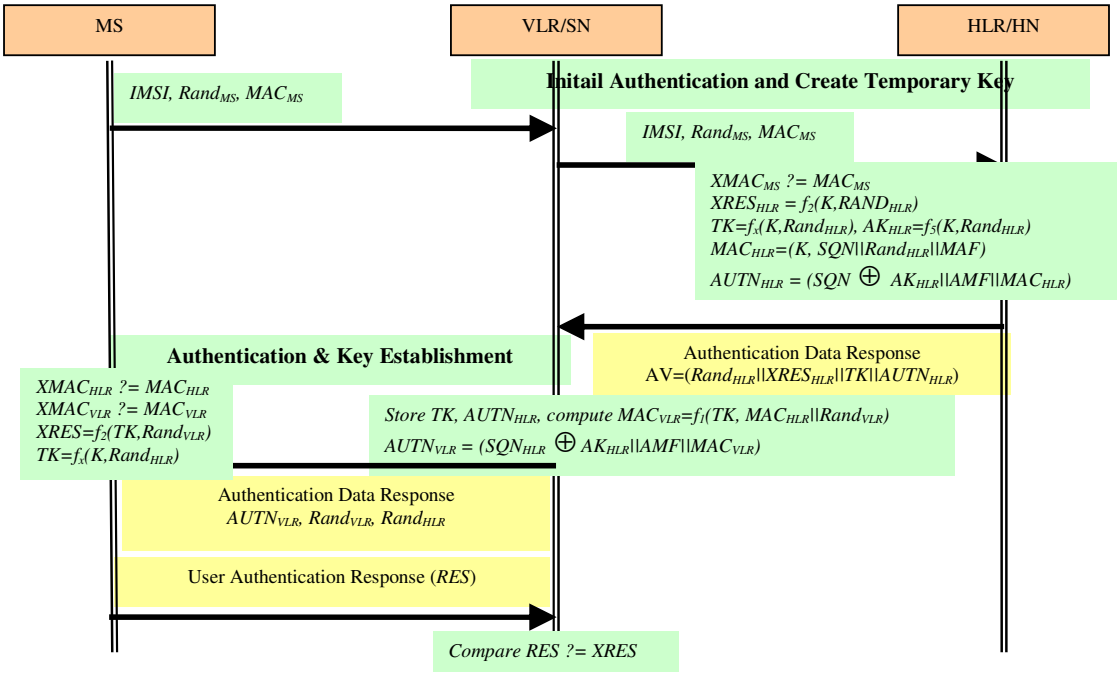


Figure 2 Registration and distribution of authentication information (Initial Authentication) in EAKA

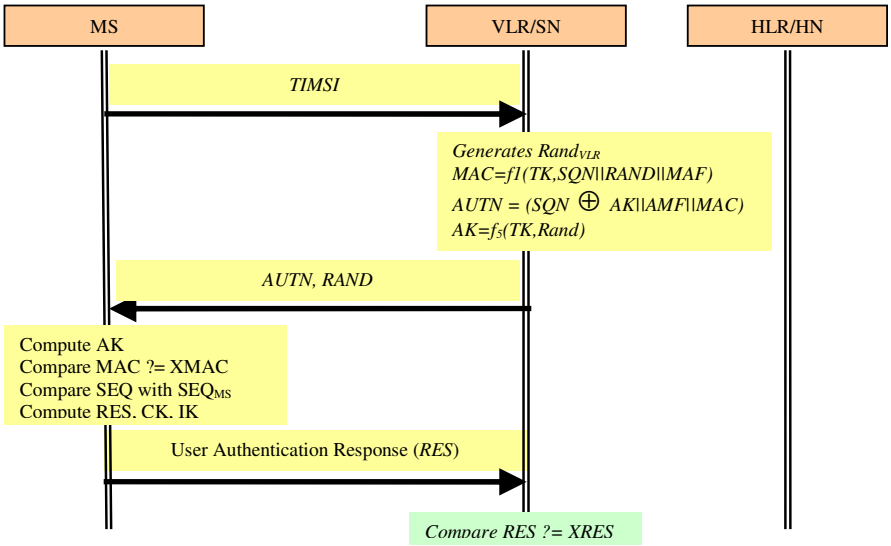


Figure 3 Subsequent authentications in EAKA