A Security Extension Providing User Anonymity and Relaxed Trust Requirement in Non-3GPP Access to the EPS

Hiten Choudhury[1], Basav Roychoudhury[2], and Dilip Kr. Saikia[3]

[1] Dept. of Computer Science, St. Edmund's College, Shillong, India
hiten.choudhury@gmail.com
[2] Indian Institute of Management, Shillong, India
brc@iimshillong.in
[3] National Institute of Technology Meghalaya, Shillong, India
dks@nitm.ac.in

Abstract. Third Generation Partnership Project (3GPP) has standardized the Evolved Packet System (EPS) as a part of their Long Term Evolution System Architecture Evolution (LTE/SAE) initiative. In order to provide ubiquitous services to the subscribers and to facilitate interoperability, EPS supports multiple access technologies where both 3GPP and Non-3GPP defined access networks are allowed to connect to a common All-IP core network called the Evolved Packet Core (EPC). However, a factor that continues to limit this endeavor is the trust requirement with respect to the subscriber's identity privacy. There are occasions during Non-3GPP access to the EPS when intermediary network elements like the access networks that may even belong to third party operators have to be confided with the subscriber's permanent identity. In this paper, we propose a security extension that relaxes this requirement. Contrary to several other solutions proposed recently in this area, our solution can be adopted as an extension to the existing security mechanism. Moreover, it has to be implemented only at the operators level without imposing any change in the intermediary network elements. We also show that the extension meets its security goals through a formal analysis carried out using AUTLOG.

1 Introduction

The Third Generation Partnership Project (3GPP) has standardized the Evolved Packet System (EPS) as part of its Long Term Evolution/System Architecture Evolution (LTE/SAE) initiative. EPS supports the use of multiple access technologies though a common all-IP core network - the Evolved Packet Core (EPC) [5]. This opens up the potential to have a truly ubiquitous network, where communication can be possible among and across 3GPP access networks and non-3GPP access networks. Thus, one can move between 3GPP access networks and non-3GPP networks, like Worldwide Interoperability for Microwave Access (WiMAX), Wireless Local Area Network (WLAN), etc., and still be communicating using EPS.

A. Prakash and R. Shyamasundar (Eds.): ICISS 2014, LNCS 8880, pp. 226–244, 2014.

In 3GPP systems, each User Equipment (UE) is assigned with a unique and a permanent identity by the service provider called the International Mobile Subscriber Identity (IMSI) for identification. Knowledge of IMSI of a subscriber may allow an adversary to track and amass comprehensive profiles about the subscriber, thereby exposing him to various risks and overall, compromising his privacy. Thus, this identity is a precious information to be restricted to as few entities as possible to ensure user anonymity. In case of communication involving 3GPP and non-3GPP networks, like in any other case, this restriction needs to be ensured.

Non-3GPP access to EPS is classified into two categories, viz., trusted and untrusted. 3GPP does not specify as to which non-3GPP technologies be considered as trusted and which as untrusted; this decision is left to the operator. While using trusted non-3GPP access networks (non-3GPP AN), the UE connects directly with the EPC using the access network. For untrusted non-3GPP AN, an Internet Protocol Security (IPSec) tunnel is established between the UE and the EPC [4]. This tunnel provides end-to-end secure channel between the UE and EPC, thereby relaxing the need for trusting the (untrusted) access network with signaling/user data exchanged over it. The idea behind such relaxation in trust requirement is to enhance the reach of 3GPP system beyond 3GPP access networks, as it will simplify the requirement for agreements/pacts between 3GPP and non-3GPP operators.

While the non-3GPP access in EPS is aimed at enhanced 3GPP access across varied access networks, this also opens up certain vulnerability regarding assurance of anonymity. The Authentication and Key Agreement (AKA) protocol, used to provide access security to non-3GPP access to EPS, has occasions where the intermediary network elements like the non-3GPP AN (trusted or untrusted) has to be confided with the IMSI of the subscriber, and that too, by transmitting the IMSI over insecure radio link. Sharing of IMSI with an intermediary implies implicit trust on the latter, and would thus require trust relationships amongst the 3GPP and non-3GPP service providers, something that provisions of non-3GPP access envisaged to relax. Such trust relationship requirements restrict the wider premise of cross network accessibility, limiting the access only amongst the ones sharing such relationships. In addition, the transmission of IMSI over insecure radio link enhances the vulnerability, even in cases where the non-3GPP network is a trusted one.

In this paper, we propose a security extension to the AKA protocol using an end-to-end approach, whereby the knowledge of IMSI is restricted only to the UE and its Home Network (HN), the latter being the one assigning the same; i.e., the knowledge of IMSI is restricted to only the assigned and the assigner. This truly federates the requirement of trusting the intermediary network elements like the non-3GPP AN with the IMSI. The main contributions of the security extension proposed in this paper are: it enhances user anonymity as he moves across the network, and it allows setting up of a conducive platform for flexible on-demand use of access network resources without worrying about the trust relationships. It can be implemented with certain changes at the level of the operator and does

not need any intervention in the intermediary networks which might belong to other network providers; this will ease deployment of the extension as it can be implemented over existing system. To the best of our knowledge, there are no other proposal for enhancement of EPS-AKA which talks about restricting the knowledge of IMSI only to the UE and HN, thereby relaxing the requirement to trust the intermediary Serving Network (SN).

This paper is organized into seven sections: Section 2 provides a brief overview of access security for non-3GPP Access to the EPS, Section 3 highlights the vulnerability to identity privacy which can compromise user anonymity, Section 4 reviews some indicative work done in this area from the literature, Section 5 presents our proposed extension and its details, Section 6 provides a brief description of the results that we have obtained from a formal analysis of our proposal, and Section 7 concludes this paper.

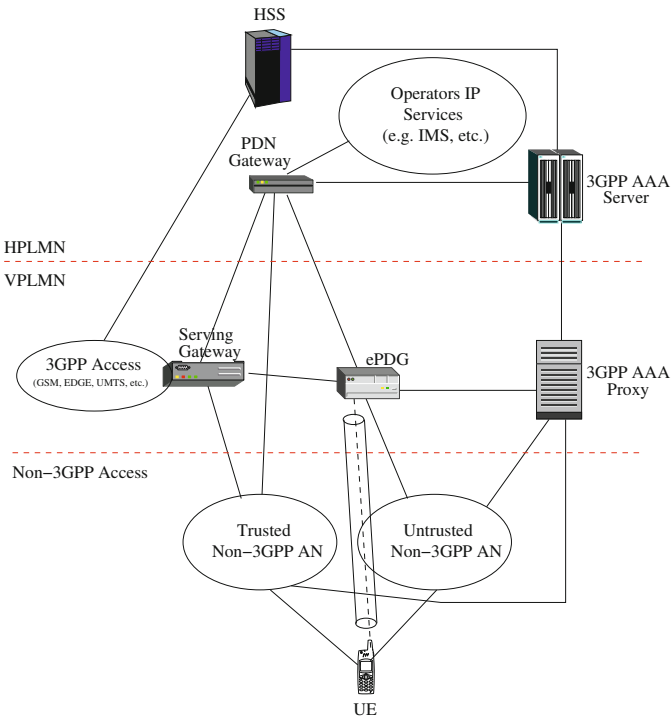

Fig. 1. Security architecture for non-3GPP access to the EPS

2 Access Security for Non-3GPP Access to the EPS

Fig. 1, depicts a simplified view of the security architecture for Non-3GPP access to the EPS. The 3GPP Authentication Authorization Accounting Server (3GPP

AAA Server) is located at the Home Public Land Mobile Network (HPLMN) - the home network of the UE. Its primary responsibility is to authenticate the subscriber, based on authentication information retrieved from the Home Subscription Server (HSS). The authentication signaling may pass via several AAA Proxies. The AAA Proxies, used to relay AAA information, may reside in any network between the Non-3GPP AN and the 3GPP AAA Server. The Packet Data Network Gateway (PDN GW) provides the UE with connectivity to the external packet data networks by being the point of exit and entry of traffic for the UE. The Serving Gateway (SGW), located at the Visitor Public Land Mobile Network (VPLMN) - the serving network, routes and forwards user data packets to and from that network. As mentioned earlier, a tunnel is set up between the UE and EPC for untrusted non-3GPP access; this IPSec tunnel is established between the Evolved Packet Data Gateway (ePDG) and the UE when the latter resides in an untrusted non-3GPP network.

The AKA protocol adopted to provide access security for trusted/untrusted Non-3GPP access to EPS is Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA) [4]. The EAP server for EAP-AKA is the 3GPP AAA Server residing in the EPC. We provide an overview of the use of EAP-AKA for trusted and untrusted Non-3GPP access in the following sub-sections:

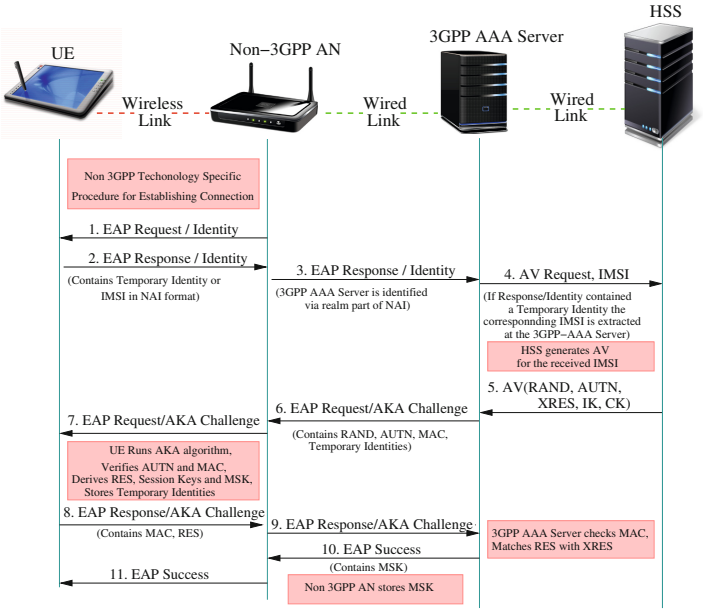

Fig. 2. Message flow during authentication in trusted non-3GPP access to the EPC

2.1 Trusted Non-3GPP Access

In trusted Non-3GPP access, the UE connects with the EPC directly through the Non-3GPP AN. For access security, the UE and the 3GPP AAA Server executes EAP-AKA protocol between them. At the end of a successful EAP-AKA, necessary key materials for secured communication between the UE and the non-3GPP AN are established. The message flows involved in the process is shown in Fig. 2.

At first, the UE establishes a connection with the Non-3GPP AN using a Non-3GPP AN technology specific procedure. The non-3GPP AN initiates the EAP-AKA procedure by sending an EAP Request/Identity message to the UE (Fig 2, Message 1). The UE responds with an EAP Response/Identity message back to the non-3GPP AN that contains the identity of the UE in Network Access Identifier (NAI) format [2] (Fig 2, Message 2). The transmitted identity may either be a temporary identity allocated to the UE in the previous authentication or, in case of the first authentication, the IMSI. This message is then routed towards the proper 3GPP-AAA Server through one or more AAA proxies identified with the help of the realm part of the NAI (Fig 2, Message 3). In case the NAI received from UE contains a temporary identity, the 3GPP AAA Server extracts the corresponding IMSI using a procedure explained in Section 2.3. The 3GPP-AAA server provides the IMSI to the HSS (Fig 2, Message 4) to procure authentication data for mutual authentication between the UE and the 3GPP-AAA server. The authentication data comprises of an Authentication Vector (AV) and contains a random part RAND, an authenticator token AUTN used for authenticating the network to the UE, an expected response XRES, a 128-bit Integrity Key IK, and a 128-bit Cipher Key CK.

$$AV = (RAND; AUTN; XRES; IK; CK) \tag{1}$$

The AUTN includes a sequence number SQN, which is used to indicate freshness of the AV. On receiving the AV from HSS (Fig 2, Message 5), the 3GPP-AAA Server derives new keying materials, viz. Master Session Key (MSK) and Extended Master Session Key (EMSK) using the IK and CK contained in the AV. Fresh temporary identities (fast re-authentication identity, pseudonym) may also be generated at this stage, using the mechanism explained in Section 2.3. The temporary identities are then encrypted and integrity protected with the keying material. The 3GPP-AAA server sends the RAND and AUTN contained in AV, a Message Authentication Code (MAC) generated using the freshly generated keying materials, and the encrypted temporary identities to the non-3GPP AN via an EAP Request/AKA-Challenge message (Fig 2, Message 6). The non-3GPP AN forwards these to the UE (Fig 2, Message 7). The UE runs UMTS algorithm [3] to verify the correctness of AUTN so as to authenticate the access network. If the verification fails, the authentication is rejected. If it is successful, the UE computes RES, IK and CK and derives the keying materials MSK and EMSK using these keys, and thereafter checks the received MAC with these keying materials. If encrypted temporary identities are received, the same are stored for future authentications. The UE then computes a new MAC value covering the

EAP message with the new keying material. This newly computed MAC value is sent via EAP Response/AKA-Challenge message to the Non-3GPP AN (Fig 2, Message 8), which in turn, forwards this message to 3GPP-AAA Server (Fig 2, Message 9).

The 3GPP-AAA Server checks the received MAC and compares XRES (received earlier from the HSS as part of AV) to the received RES. If all checks are successful, the 3GPP-AAA Server sends an EAP Success message to Non-3GPP AN through a trusted link (Fig 2, Message 10). The keying material MSK is also send with this message to the Non-3GPP AN; the latter stores this to set up secure communication with the authenticated UE. The Non-3GPP AN informs the UE about the successful authentication by forwarding the EAP Success message (Fig 2, Message 11). This completes the EAP-AKA procedure that is required to register the UE with the Non-3GPP AN, at the end of which the UE and the non-3GPP AN share keying material derived during the exchange.

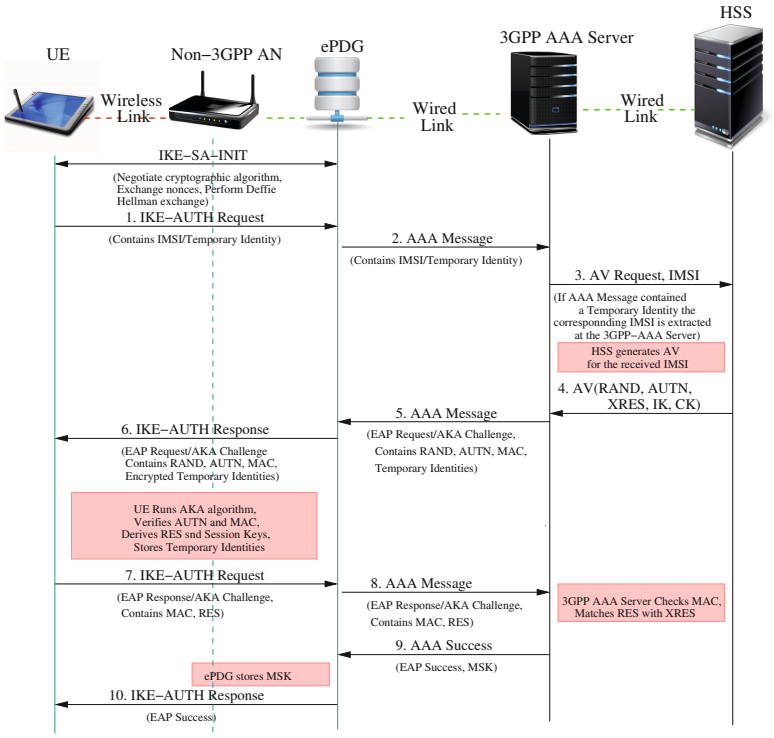

Fig. 3. Message flow during authentication in untrusted non-3GPP access to the EPC

2.2 Untrusted Non-3GPP Access

In case of untrusted Non-3GPP access, the UE does not connect directly to the EPC, but connects via the ePDG. The UE first establishes IPSec tunnel with the ePDG using Internet Key Exchange version 2 (IKEv2) protocol [22], and then performs the EAP-AKA explained in Section 2.1 using this tunnel. The message flows involved in such case is shown in Fig. 3.

The UE and the ePDG exchange a pair of messages (IKE-SA-INIT) to establish an IKEv2 channel in which the ePDG and UE negotiate cryptographic algorithms, exchange nonce and perform a Diffie Hellman exchange. With the IKEv2 secure channel in place, the UE sends its identity (compliant with NAI format, containing the IMSI or a temporary identity) to the ePDG (Fig 3, Message 1), which can only be decrypted and authenticated by the end points (i.e., the UE or the ePDG). The ePDG sends an authentication request message containing the UE identity to the 3GPP-AAA server (Fig 3, Message 2). For communication between ePDG and AAA-Server, the EAP-AKA messages are encapsulated in AAA messages. The 3GPP-AAA server fetches the AVs from the HSS (Fig 3, Message 4) as discussed in Section 2.1, and forwards the EAP message containing RAND, AUTN, MAC and encrypted temporary identities to ePDG (Fig 3, Message 5), the latter forwards this message further to the UE (Fig 3, Message 6). All messages between ePDG and UE are interchanged using IKE-AUTH messages. The UE checks the authentication parameters in the message received from ePDG and responds to the authentication challenge as in case of trusted non-3GPP access (Fig 3, Message 7). The ePDG forwards this response to the 3GPP-AAA server (Fig 3, Message 8). The 3GPP-AAA server performs the usual checks, and once successful, sends an EAP Success message and the keying materials to the ePDG (Fig 3, Message 9). The ePDG forwards the EAP Success message to the UE over the secure IKEv2 channel (Fig 3, Message 10). This completes the EAP-AKA exchange whereby the UE and the ePDG share keying material to be used for secure communication.

2.3 Temporary Identity Generation

An encrypted IMSI based technique is used to generate the temporary identities. Advanced Encryption Standard (AES) in Electronic Codebook (ECB) mode of operation is used for this purpose. A 128-bit secret key Kpseu is used for the encryption [4]. A specific Kpseu for generation of temporary identities is used for only a given interval determined by the operator. On expiry of this interval, a fresh Kpseu is used to generate the identities. This ensures the freshness of the key. Each key has a key indicator value associated with it, and this value is send along with the temporary identity, when the latter is used by UE for identity presentation. This allows the 3GPP-AAA server to use the correct Kpseu for linking the presented identity to the corresponding IMSI. The 3GPP-AAA Server should store a certain number number of old keys for interpretation of the received temporary identities that were generated using those old keys. The number of old keys maintained in the 3GPP-AAA server is operator specific, but

it must at least be one, else a just-generated temporary identity may immediately become invalid due to the expiration of the key.

3 Identity Privacy Vulnerability

In order to ensure identity privacy to the subscribers, the 3GPP-AAA Server generates and allocates temporary identities to the UE in a secured way (as discussed in Section 2). These temporary identities, instead of IMSI, are mostly presented by the UE for identity presentation. Two types of temporary identities are allocated to the UE, viz., a re-authentication identity and a pseudonym. The re-authentication identity is used for identity presentation during a fast re-authentication [4] and the pseudonym is used during an EAP-AKA. The UE does not interpret the temporary identities, it just stores and uses them during the next authentication. In-spite of the above, EAP-AKA has vulnerabilities whereby the permanent identity, i.e. the IMSI, might get compromised. Following are the scenarios when IMSI may get compromised during trusted non-3GPP access:

- The IMSI is transmitted in clear text through the radio link for identity presentation during the very first authentication
- A subscriber having a temporary identity from the 3GPP-AAA Server may not initiate any new authentication attempt for quite some time. If the user initiates an authentication attempt using an old temporary identity after the key used to generate the same has been removed from storage at the 3GPP-AAA Server, the latter will not be able to recognize the temporary identity. In cases when both fast re-authentication identity as well as pseudonym are not recognized, the 3GPP-AAA Server will request the UE to send its permanent identity. In response to such a request, the UE may have to transmit its IMSI to the Non-3GPP AN in clear text through the wireless link making the permanent identity accessible to eavesdroppers.
- A corrupt Non-3GPP AN may utilize the received IMSI for various kind of malicious activities or may pass this identity to an unreliable party.
- A malicious/fake Non-3GPP AN may also take advantage of the above situation by creating a spurious EAP Request/Identity message and by requesting the UE for its IMSI through this message; in response to which the unsuspecting UE that does not have a mechanism to authenticate the request at that time, will transmit its IMSI in clear text through the radio link.

In case of untrusted non-3GPP access, there are no threats against identity privacy from passive attackers like eavesdroppers due the IPSec tunnel set up between the UE and the ePDG. However, there exist the following threats from active attackers when sending the IMSI in the tunnel set-up procedure:

- The protected channel is encrypted but not authenticated at the time of receiving the user identity (IMSI). The IKEv2 messages, when using EAP, are authenticated at the end of the EAP exchange. So an attacker may

pose as a genuine ePDG and may request the UE for the IMSI. Although the attack would eventually fail at the time of authentication, the attacker would have managed to see the IMSI in clear text by then.
– The IMSI would be visible to the ePDG, which in roaming situations may be in the VPLMN. Such a vulnerability limits the home operator in interoperating with a VPLMN that belongs to an untrusted third party operator.

4 Related Work

In mobile networks, the need to protect the identity privacy of a subscriber even from intermediary network elements like the visitor access network is well established. Herzberg *et al.* [19] pointed out that in an ideal situation no entity other than the subscriber himself and a responsible authority in the subscriber's home domain should know the real identity of the user. Even the authority in the visited network should not have any idea about the real identity. Towards this, several schemes have been proposed with each of them following a varied approach.

Many of the proposed schemes employ public key infrastructure [29][26][20] [28][18][36], but due to their processor intensive nature, such solutions are not the best of solutions for 3GPP based mobile systems, as the UE may not have high processing and power capability.

The combination of both public key and symmetric key crypto system are also explored in many of the schemes. Varadharajan *et al.* [31] proposed three schemes using this hybrid approach. However, Wong *et al.* [33] found that they are vulnerable to several attacks. Another hybrid scheme was proposed by Zhu *et al.* that uses both public and symmetric key crypto systems [40]. However, in Zhu *et al.*'s scheme certain security weaknesses were detected, due to which several other improvements were proposed [25][34][7][37]. Recently, Zeng *et al.* demonstrated that because of an inherent design flaw in the original in Zhu *et al.*'s scheme, the latter and its successors are unlikely to provide anonymity [38].

Off late, several other schemes were proposed by various researchers [24][17] [14][39][8][13][16][15][12][27][21][23][35]. However, none of these schemes are in line with EAP-AKA. For a mobile operator that already has a big subscriber base, changing over to a completely new authentication and key agreement protocol is a big challenge. Therefore, an ideal scheme for enhanced identity privacy in Non-3GPP access to the EPS would be the one that can be easily configured into the existing authentication and key agreement protocol (i.e., EAP-AKA). At the same time, an ideal scheme should also be restricted only to the operator. Intermediary network elements that may even belong to third party operators should not be expected to participate equally.

5 Our Proposed Security Extension

In this section, we explain our security extension for EAP-AKA that overcomes the existing identity privacy vulnerabilities mentioned in Section 3 and relaxes

the need to trust an intermediary network element with the IMSI during Non-3GPP access to the EPS. The knowledge of the IMSI of a subscriber is restricted to the UE and the HSS, and in no situation is revealed to any third party; thus conforming to the requirement stated by Herzberg et al. [19]. This extension is implemented only at Subscriber Identity Module (SIM) of the UE, and the HSS; and does not envisage any change at the intermediate network elements like the Non-3GPP AN and the AAA servers. The SIM and the HSS can be upgraded to support this extension, thereby easing migration challenges in the face of current wide scale deployment. As only the UE and HSS needs to be aware of this extension, the migration can also be taken up in a phased manner, or can be offered as a value added service for ensuring anonymity. This work is in continuation of the authors' earlier proposal for UMTS [9] and LTE [11]. The following sub-sections explain the working of this security extension. A summary of all the functions used in the security extension (working details of which are explained later in this section) is presented in Table 1.

Table 1. Functions used in the extension.

Function	Details
f_i	Generates a $DMSI$ from a given RIC.
f_{Embed}	Embeds a 32 bit RIC into a 128 bit $RAND$.
$f_{Extract}$	Extracts the 32 bit RIC from a 128 bit $ERAND$.
f_n	Encrypts RIC_{Padded} to find $ERIC$.
f_d	Decrypts $ERIC$ to find RIC_{Padded}.
f_{PRNG}	Generates a 128 bit pseudo random number.

5.1 DMSI: Pseudonym for IMSI

Our scheme replaces the transmission of the IMSI with a pseudonym - Dynamic Mobile Subscriber Identity (DMSI). A fresh DMSI is generated as and when the need for transmission of IMSI as per the original protocol arises. Being untraceable to the IMSI, the transmission of short-lived DMSI does not compromise the permanent identity of the user, thereby ensuring anonymity. As the IMSI never gets transmitted, the same also remains unknown to all intermediary network components and thereby remains restricted to UE and HSS.

5.2 Generating DMSI

The DMSI is generated from the most recent value of RAND (Equation 1) received at UE during a successful EAP-AKA procedure, and owes its existence

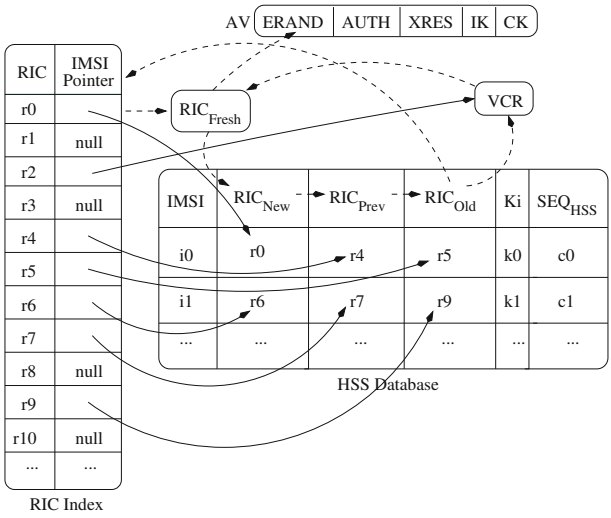

Fig. 4. RIC Index with modified HSS database

to a random number, called the Random number for Identity Confidentiality (RIC) that remain embedded in the RAND (we call this Embedded RAND or ERAND). The HSS maintains a pool of RICs, some of which may be in-use (i.e., assigned to certain UEs) while the others not-in-use at any point in time (Fig. 4). During each run of the EAP-AKA protocol, a not-in-use RIC is randomly selected from the pool of RICs, and is securely transmitted, embedded into the RAND, to the UE. The UE extracts the RIC from the most recently received RAND to generate the next DMSI, which is then used as a pseudonym for the IMSI of the UE. Thus, DMSI is a function of RIC as is shown later in Equation 8:

$$DMSI = f(RIC) \tag{2}$$

The extension ensures that the selected RIC is sufficiently random, and has no correlation with a previously selected RIC. A mapping between the selected RIC and the IMSI of the UE is maintained at the HSS (explained later in this section); this allows the HSS to uniquely identify the UE with the corresponding RIC, and thereby the DMSI.

5.3 Management of RIC

The size of RIC is decided by the operator, and this decides on the size of the RIC pool at HSS. A RIC of size b bits provide a pool of n unique RIC values:

$$n = 2^b \tag{3}$$

As for example, a 32 bit RIC size will ensure a pool of 2^{32}, i.e., approximately 4.29 billion unique RIC values which should be sufficient for the HSS to support

a reasonable number of subscribers. The RIC pool is maintained at the HSS database as the RIC-Index (Fig. 4). This is a sorted list of the possible $n = 2^b$ RIC values. Each entry in the RIC-Index has an associated pointer the RIC-Pointer. If the particular RIC value is assigned to a UE, i.e., the RIC is in-use, this pointer will point to the corresponding IMSI in the HSS database. If the RIC is not assigned to any UE, i.e., not-in-use, the RIC-Pointer will be null.

A fresh value of RIC, randomly chosen from the pool of not-in-use RICs from the RIC-Index, is allotted to the UE during the run of EAP-AKA. This is stored as RIC_{Fresh} at the HSS database, and is cryptographically embedded into the RAND part of AV using the long term secret key Ki shared between the HSS and the UE resulting in a new random number called the Embedded RAND (ERAND):

$$ERAND = f_{Embed}Ki(RIC_{Fresh}, RAND) \tag{4}$$

The AV thus get modified as follows:

$$AV = (ERAND; AUTH; XRES; IK; CK) \tag{5}$$

This ERAND is now used by the 3GPP-AAA server, instead of the RAND as in the original protocol, to challenge the UE. Since the size of RAND and ERAND is same, this change will be transparent to the 3GPP-AAA server. Example algorithms to embed a 32 bit RIC into a 128 bit RAND and to extract the embedded RIC form the ERAND is proposed in [10]. Only the UE, having the knowledge of the long term shared key Ki, will be able to extract RIC from ERAND.

$$RIC = f_{Extract}Ki(ERAND) \tag{6}$$

Few, say m, RICs associated with an IMSI the fresh RIC (say RIC_{Fresh}) and $m - 1$ previously generated RICs are stored at the HSS database against that IMSI in the fields RIC_{New}, RIC_{Prev}, RIC_{Old}, etc. When a new RIC is allotted, it is stored in RIC_{New}, the previous value at RIC_{New} moved to RIC_{Prev}, the previous value of RIC_{Prev} to RIC_{Old}, and so on, the oldest of the previous m RICs being released back to the RIC-Index as not-in-use i.e., the RIC that is released will have the IMSI-Pointer reset to null against it in the RIC-Index. This ensures robustness of the protocol against the loss of an ERAND during transit to the UE. The storage of m RICs ensures that a mapping between the RIC that is currently stored at the UE and the corresponding IMSI is always maintained at the HSS. As for any other critical information such as the subscriber's security credentials, billing details, etc., it is the responsibility of the operator to ensure a robust backup mechanism against database crash.

The choice of m is left to the operator. For illustration, if we consider the RIC size to be 32 bits, and $m = 4$, i.e., 2^2 RICs are stored against each IMSI, it would still allow one to provide for 2^{30}, which is approximately 1.073 billion subscribers; this number is more than 5 times the approximately 200 million subscriber base of the largest cellular operator in India as of January, 2014 [30].

Thus, if s is the maximum number of subscribers that the operator wants the proposed extension to handle, then

$$s = n/m \tag{7}$$

n being the total number of possible RICs in the entire pool and m the number of RICs maintained against each IMSI in the HSS's database. The HSS maintains a field SEQ_{HSS} against every IMSI to verify the freshness of a DMSI it receives from an UE and to prevent replay attacks.

5.4 Handling Collision at RIC-Index

Whenever a RIC needs to be embedded into a RAND at the HSS, a new RIC (RIC_{Fresh}) is selected from the pool of not-in-use RICs. In order to select RIC_{Fresh}, a b bit random number (say RN) is generated using a standard Pseudo Random Number Generator. This RN is then searched for in the RIC-Index. If the IMSI-Pointer against RN in the RIC-Index is found to be null, RN is selected as RIC_{Fresh} and the null value is replaced with the address of the record in the HSS's database where the IMSI is stored. However, a collision may occur in this process if the IMSI-Pointer against RN in the RIC-Index is not null, i.e., if that particular RIC value is in-use. For collision resolution, a b bit variable called Variable for Collision Resolution (VCR) is maintained at HSS (Fig. 4). The VCR always contains a not-in-use RIC. Thus, when RN results in a collision, the value at VCR can be used instead. At the very outset, during initialization of the HSS's database, a b bit random number (say RN_0) is stored in the VCR and the IMSI-Pointer against it in the RIC-Index is set to the address of VCR. Whenever there is a collision, the b bit value stored in the VCR is selected as RIC_{Fresh}, its value searched in RIC-Index and the IMSI-Pointer against it set to the address at HSSs database where the IMSI is stored. Once the value of VCR is used for RIC_{Fresh}, the former will have to be replaced with a new not-in-use RIC value. The oldest of the m RIC values in the HSS database against the IMSI in question is then not released to the pool on not-in-use RICs, but is stored at VCR, and the IMSI-Pointer against its value in RIC-Index set to the address of the VCR. This ensures that VCR always contains a not-in-use RIC value to take care of the collisions.

5.5 Resolving Identity to IMSI in AV Request

Under normal operation of EAP-AKA, the UE uses a temporary identity in NAI format [2] to present its identity to the network. The realm part of the temporary identity (NAI format) allows the intermediate AAA proxy servers to guide the request to the appropriate 3GPP-AAA server. When a request for an AV reaches the 3GPP-AAA server along with the temporary identity of the subscriber, the 3GPP-AAA Server resolves the temporary identity to its corresponding IMSI using the procedure discussed in Section 2.3. The AV request is then forwarded to the HSS along with the resolved IMSI. However, in situations enumerated in

Section 3 where the IMSI needs to be transmitted by the UE, the DMSI in NAI format is now transmitted instead:

$$DMSI = MCC \| MNC \| RIC \| ERIC \tag{8}$$

MCC stands for the Mobile Country Code, MNC stands for the Mobile Network Code, and ERIC is created by encrypting a padded RIC (say RIC_{padded}) with the Advanced Encryption Standard (AES) algorithm, taking the long term secret key Ki as parameter. Thus, the ERIC, whose use is explained later, is:

$$ERIC = f_n Ki(RIC_{padded}) \tag{9}$$

where,

$$RIC_{padded} = RIC \| SEQ_{UE} \| R \tag{10}$$

SEQ_{UE} is the value of a 32 bit counter maintained at UE with its value incremented whenever a new DMSI is created for identity presentation, and R is a $128 - (32 + b)$ bit random number. SEQ_{UE} ensures the freshness of DMSI and prevents replay attack at HSS, and inclusion of R pads the RIC_{padded} to 128 bits, a requirement for AES cipher. R also introduces sufficient amount of randomness to harden cryptanalysis of the cipher text.

As before, the realm part allows the intermediate AAA proxy servers to guide the request to the appropriate 3GPP-AAA server, which forwards the DMSI to the HSS along with a request for AV, as it would have done for a received IMSI. Thus, the onus of resolving the DMSI is passed on to the HSS. On receiving the AV request, the HSS resolves the DMSI, which it does by locating RIC part of the received DMSI. It then uses the RIC-Index to find the corresponding RIC-Pointer (Fig. 4), and thereby the IMSI and the long term key Ki. The next step is to decrypt the ERIC part using AES and Ki:

$$RIC_{padded} = f_d Ki(ERIC) \tag{11}$$

The RIC contained in RIC_{padded} is then compared with the RIC part of the DMSI, a success ensures that the DMSI was created by UE having key Ki, and not by a malicious agent. The sole purpose of including ERIC in DMSI is to ensure this protection. A SEQ_{UE} value in RIC_{padded} greater than SEQ_{HSS} ensures the freshness of the request. If any of these checks fail, the request is rejected, else the SEQ_{UE} is copied into SEQ_{HSS} for future reference and a fresh AV is generated as in Equation 5 to respond to the AV request. Fig. 5 and Fig. 6 depicts the message flow under this proposed extension for trusted and untrusted non-3GPP access to EPS.

6 Formal Analysis of Security Requirements

We performed a formal analysis of the proposed scheme through an enhanced BAN logic [6] called AUTLOG [32]. A similar analysis is performed by 3GPP in [1]. The security goals for this analysis are listed in the following subsection.

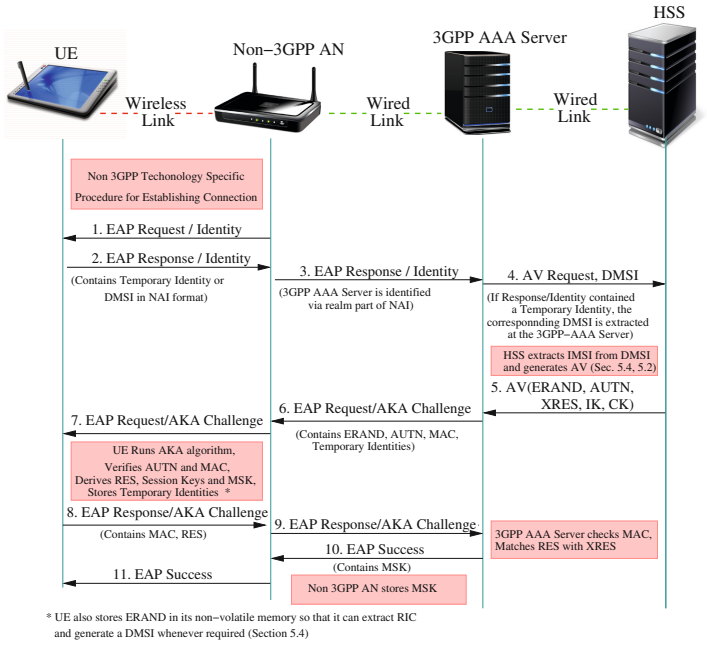

Fig. 5. Message flow during authentication under proposed extension in trusted non-3GPP access to the EPC

6.1 Security Goals

$IMSI$ should be a shared secret between the UE and the HSS. The same should not be disclosed by the UE to any third party including the AN.

$$\textbf{G1: } UE \text{ believes } UE \overset{IMSI}{\longleftrightarrow} HSS$$

$$\textbf{G2: } UE \text{ believes } \neg(AN \text{ sees } IMSI)$$

When ever temporary identities (i.e., re-authentication identities and pseudonyms) fail to protect the permanent identity (due to reasons discussed in Section 3), a backup mechanism is followed according to our proposed extension, so that identity privacy may still be ensured to the subscriber. According to this mechanism (Section 5), a $DMSI$ created with the RIC that is extracted from the most recent $RAND$ received at the UE is transmitted in lieu of the $IMSI$. During every successful run of the EAP-AKA protocol, if the UE receives a fresh RIC, it can easily protect its permanent identity following this mechanism.

$$\textbf{G3: } UE \text{ believes } UE \text{ has } RIC$$

$$\textbf{G4: } UE \text{ believes } fresh(RIC)$$

It should not be possible for anyone except the HSS (that has access to the RIC-Index) to map a $DMSI$ with its corresponding $IMSI$.

$$\textbf{G5: } UE \textit{ believes } \neg(DMSI \equiv IMSI)$$

The formal analysis of our extension established the achievement of the above security goals.

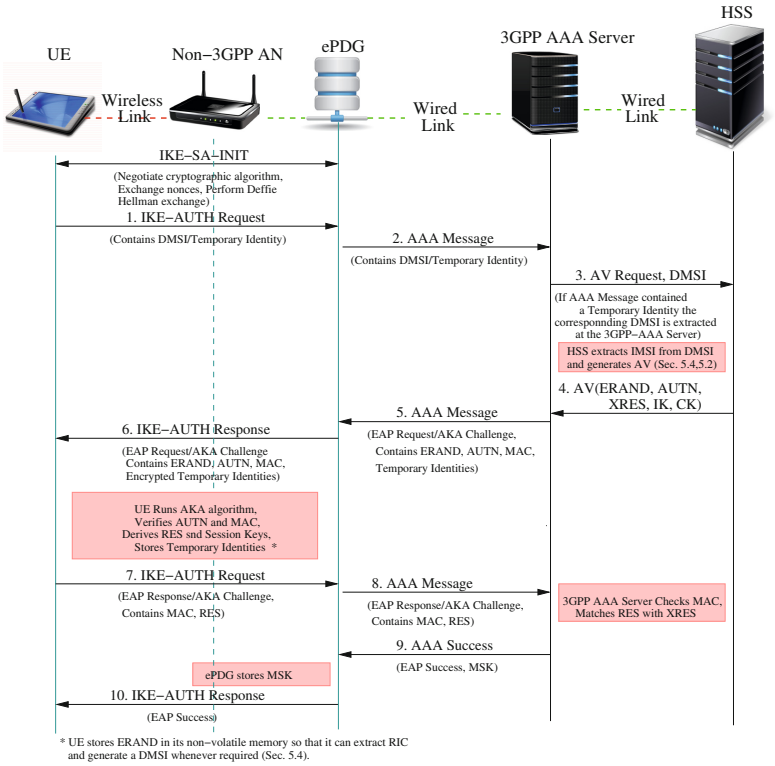

Fig. 6. Message flow during authentication under proposed extension in untrusted non-3GPP access to the EPC

7 Conclusion

A factor that complicates and restricts non-3GPP access to the EPS is the trust requirement on intermediary networks (like non-3GPP AN and ePDG) to take care of subscriber's identity privacy. In this paper, we have proposed an extension to the EAP-AKA protocol to resolve the user anonymity related issues in non-3GPP access to EPS. The main contribution of this paper is to enable total confidentiality of the permanent identity - the IMSI - of the subscriber from eavesdroppers as well as from intermediary network components; this would

allow access to 3GPP based networks from diverse non-3GPP based access networks without detailed requirements of trust amongst them. As an additional feature, the proposed changes are transparent to the intermediary network components and can be implemented over the existing subscriber base with limited changes in the HSS and the UE, i.e. only at the operator's level. Being a symmetric key based approach, as followed in EPS-AKA, it takes care of the constraint of the limited computational power of UE; unlike the schemes using public key cryptography. We have also carried out a formal security analysis of our proposal using AUTLOG, and have shown that the extension proposed here conforms to the necessary security requirements.

References

1. 3GPP: Formal Analysis of the 3G Authentication Protocol. TR 33.902, 3rd Generation Partnership Project (3GPP) (2001), http://www.3gpp.org/ftp/Specs/html-info/33902.htm
2. 3GPP: Numbering, addressing and identification. TS 23.003, 3rd Generation Partnership Project (3GPP) (2011), http://www.3gpp.org/ftp/Specs/html-info/23003.htm
3. 3GPP: 3G Security; Security architecture. TS 33.102, 3rd Generation Partnership Project (3GPP) (2012), http://www.3gpp.org/ftp/Specs/html-info/33102.htm
4. 3GPP: 3GPP System Architecture Evolution (SAE);Security aspects of non-3GPP accesses. TS 33.402, 3rd Generation Partnership Project (3GPP) (2012), http://www.3gpp.org/ftp/Specs/html-info/33402.htm
5. 3GPP: Architecture enhancements for non-3GPP accesses. TS 23.402, 3rd Generation Partnership Project (3GPP) (2012), http://www.3gpp.org/ftp/Specs/html-info/23402.htm
6. Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 426(1871), 233–271 (1989)
7. Chang, C., Lee, C., Chiu, Y.: Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Computer Communications 32(4), 611–618 (2009)
8. Chen, C., He, D., Chan, S., Bu, J., Gao, Y., Fan, R.: Lightweight and provably secure user authentication with anonymity for the global mobility network. International Journal of Communication Systems 24(3), 347–362 (2011)
9. Choudhury, H., Roychoudhury, B., Saikia, D.K.: End-to-end user identity confidentiality for umts networks. In: 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 2, pp. 46–50. IEEE (2010)
10. Choudhury, H., Roychoudhury, B., Saikia, D.: Umts user identity confidentiality: An end-to-end solution. In: 2011 Eighth International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1–6. IEEE (2011)
11. Choudhury, H., Roychoudhury, B., Saikia, D.: Enhancing user identity privacy in lte. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 949–957. IEEE (2012)
12. Feng, T., Zhou, W., Li, X.: Anonymous identity authentication scheme in wireless roaming communication. In: 2012 8th International Conference on Computing Technology and Information Management (ICCM), vol. 1, pp. 124–129. IEEE (2012)

13. He, D., Bu, J., Chan, S., Chen, C., Yin, M.: Privacy-preserving universal authentication protocol for wireless communications. IEEE Transactions on Wireless Communications 10(2), 431–436 (2011)
14. He, D., Chan, S., Chen, C., Bu, J., Fan, R.: Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. Wireless Personal Communications 61(2), 465–476 (2011)
15. He, D., Chen, C., Chan, S., Bu, J.: Analysis and improvement of a secure and efficient handover authentication for wireless networks. IEEE Communications Letters 16(8), 1270–1273 (2012)
16. He, D., Chen, C., Chan, S., Bu, J.: Secure and efficient handover authentication based on bilinear pairing functions. IEEE Transactions on Wireless Communications 11(1), 48–53 (2012)
17. He, D., Ma, M., Zhang, Y., Chen, C., Bu, J.: A strong user authentication scheme with smart cards for wireless communications. Computer Communications 34(3), 367–374 (2011)
18. He, Q., Wu, D., Khosla, P.: The quest for personal control over mobile location privacy. IEEE Communications Magazine 42(5), 130–136 (2004)
19. Herzberg, A., Krawczyk, H., Tsudik, G.: On travelling incognito. In: First Workshop on Mobile Computing Systems and Applications, WMCSA 1994, pp. 205–211. IEEE (1994)
20. Horn, G., Preneel, B.: Authentication and payment in future mobile systems. In: Quisquater, J.-J., Deswarte, Y., Meadows, C., Gollmann, D. (eds.) ESORICS 1998. LNCS, vol. 1485, pp. 277–293. Springer, Heidelberg (1998)
21. Jiang, Q., Ma, J., Li, G., Yang, L.: An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. In: Wireless Personal Communications, pp. 1–15 (2012)
22. Kaufman, C., Hoffman, P., Nir, Y., Eronen, P.: Internet key exchange protocol version 2 (ikev2). The Internet Engineering Task Force Request for Comments (IETF RFC) 5996 (2010)
23. Kuo, W.C., Wei, H.J., Cheng, J.C.: An efficient and secure anonymous mobility network authentication scheme. Journal of Information Security and Applications (2014)
24. Lee, C., Chen, C., Ou, H., Chen, L.: Extension of an efficient 3gpp authentication and key agreement protocol. Wireless Personal Communications, 1–12 (2011)
25. Lee, C., Hwang, M., Liao, I.: Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Transactions on Industrial Electronics 53(5), 1683–1687 (2006)
26. Lin, H., Harn, L.: Authentication protocols for personal communication systems. ACM SIGCOMM Computer Communication Review 25(4), 256–261 (1995)
27. Liu, H., Liang, M.: Privacy-preserving registration protocol for mobile network. International Journal of Communication Systems (2012)
28. Park, J., Go, J., Kim, K.: Wireless authentication protocol preserving user anonymity. In: Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS 2001), vol. 26, pp. 159–164. Citeseer (2001)
29. Samfat, D., Molva, R., Asokan, N.: Untraceability in mobile networks. In: Proceedings of the 1st Annual International Conference on Mobile Computing and Networking, pp. 26–36. ACM (1995)
30. Trai: Highlights on telecom subscription data as on 07 july 2014. Press release, Telecom Regulatory Authority of India (2014)

31. Varadharajan, V., Mu, Y.: Preserving privacy in mobile communications: a hybrid method. In: 1997 IEEE International Conference on Personal Wireless Communications, pp. 532–536. IEEE (1997)
32. Wedel, G., Kessler, V.: Formal semantics for authentication logics. In: Martella, G., Kurth, H., Montolivo, E., Bertino, E. (eds.) ESORICS 1996. LNCS, vol. 1146, pp. 219–241. Springer, Heidelberg (1996)
33. Wong, D.: Security analysis of two anonymous authentication protocols for distributed wireless networks. In: Third IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom 2005 Workshops, pp. 284–288. IEEE (2005)
34. Wu, C., Lee, W., Tsaur, W.: A secure authentication scheme with anonymity for wireless communications. IEEE Communications Letters 12(10), 722–723 (2008)
35. Xie, Q., Hu, B., Tan, X., Bao, M., Yu, X.: Robust anonymous two-factor authentication scheme for roaming service in global mobility network. Wireless Personal Communications 74(2), 601–614 (2014)
36. Yang, G., Wong, D., Deng, X.: Anonymous and authenticated key exchange for roaming networks. IEEE Transactions on Wireless Communications 6(9), 3461–3472 (2007)
37. Youn, T., Park, Y., Lim, J.: Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks. IEEE Communications Letters 13(7), 471–473 (2009)
38. Zeng, P., Cao, Z., Choo, K., Wang, S.: On the anonymity of some authentication schemes for wireless communications. IEEE Communications Letters 13(3), 170–171 (2009)
39. Zhou, T., Xu, J.: Provable secure authentication protocol with anonymity for roaming service in global mobility networks. Computer Networks 55(1), 205–213 (2011)
40. Zhu, J., Ma, J.: A new authentication scheme with anonymity for wireless environments. IEEE Transactions on Consumer Electronics 50(1), 231–235 (2004)