Advanced SSL/TLS-Based Authentication for Secure WLAN-3G Interworking

Georgios Kambourakis, Angelos Rouskas[*], Georgios Kormentzas and Stefanos Gritzalis

Department of Information and Communication Systems Engineering,
University of the Aegean, Samos 83200, Greece

[*]*Correspondence Author*

E-mail: arouskas@aegean.gr
Tel: +(30) 227 3082236, Fax: +(30) 227 3082009

Abstract – Motivated by the fact that SSL protocol has proved its effectiveness in wired IP backbones, recent research works examine the potential use of this protocol in various wireless technologies. Whereas Wi-Fi networks present security deficiencies, they manage to highly penetrate into the wireless market in a great degree due to their low cost, easy administration, great capacity, IP-oriented nature, etc. Considering Wi-Fi networking settings, administrated by different operators, as parts of a common core 3G infrastructure, the paper proposes the potential application of enhanced SSL-based authentication mechanisms in integrated emerging-3G and Wi-Fi networks. We discuss existing problems related to Authentication and Key Agreement (AKA) procedures and the Extensible Authentication Protocol (EAP)-AKA, as they appear in the latest 3G and integrated 3G/Wi-Fi specifications. We propose how EAP-TLS, combined with Public Key Infrastructure (PKI) elements, can be used to overcome these inefficiencies in a hybrid WLAN - 3G heterogeneous environment, in order to provide strong authentication and *end-to-end* security to the mobile user.

Keywords: AKA; EAP; TLS; PKI; UMTS; Wi-Fi; WLAN.

1. INTRODUCTION

It is anticipated that the number of users wishing wireless security-sensitive services (e.g., online banking, stock trading, shopping, etc.) will largely increase in the near future. Furthermore, potential wireless/mobile users will wish to use the most appropriate technology among a broad range of available heterogeneous wireless technologies (Mobile 2.5G or 3G telecommunications systems, such as GPRS and UMTS; Broadband Radio Access Networks, such as IEEE 802.11 or HIPERLAN; and wireless broadcasting technologies, such as DVB-T), depending on various criteria, such as the surrounding environment (e.g., home, car, office, etc.), technology available, cost, provided bandwidth, etc.

According to beyond-3G vision, an IP backbone will constitute the core network for all heterogeneous wireless technologies and secure communication provision will become one of the major goals of these systems. While Secure Sockets Layer/Transport Layer Security (SSL/TLS) is the predominant and most widely used security protocol on the wired Internet, to the best of our knowledge, no wireless data service today offers this protocol on a mobile device. Performance considerations in using SSL/TLS in resource-constrained environments, like the wireless one, drove mobile operators to choose a different and incompatible – mainly gateway-oriented - security protocol for their mobile clients [1]. However, recent works indicate that both a performance efficient implementation of SSL for handheld devices is feasible [2] and secure, flexible and reconfigurable Authentication and Key Agreement (AKA) procedures for beyond 3G wireless communication networks can be implemented [3].

The paper discusses the application of SSL/TLS-based authentication into integrated 3G and Wi-Fi networks to provide strong end-to-end security and authentication to the user. The proposed application enables a Wi-Fi user, who is also a subscriber to a 3G mobile network operator, to move across WLAN segments administrated by different WLAN operators. From a technical aspect, this application requires that all Wi-Fi networking settings are *loosely* or *tightly* incorporated [4] into a common core 3G infrastructure, while from a business point of view it is necessary that appropriate Roaming Agreements (RAs) are established among the various visited WLAN operators and the home 3G operator.

The rest of the paper is organised as follows: Considering 3GPP's proposals for interworking and handover between IEEE 802.11a/b/c/i and 3G networks, the next Section discusses how a Wi-Fi networking setting can be integrated in a 3G infrastructure. Section 3 deals with 3G and 3G/Wi-Fi combined security inefficiencies, which enforce the usage of more advanced security mechanisms such as SSL/TLS-based schemes. Section 4 presents how EAP-TLS can be part of an all-IP mobile environment, while Section 5 proposes and analyses an AKA mechanism based on EAP-TLS, which can be applied into Wi-Fi settings. The paper is concluded in Section 6.

2. INTEGRATION OF WI-FI NETWORKS INTO EMERGING 3G INFRASTRUCTURES

Emerging or beyond-3G architectures are envisaged to constitute of an IP-based core network, whereas the access network can be based on a variety of heterogeneous wireless technologies depending on the nature of the access cell. Focusing on picocell environments in such future architectures, where coverage is limited within the buildings, Wi-Fi networks are emerging as the most promising access technology. The anticipated provision of many *uncoordinated* Wi-Fi picocells will bring to foreground many open issues concerning authentication and security, mobility management, roaming and billing of mobile users moving among different Wi-Fi settings.

Our work deals with *authentication* issues in different Wi-Fi operators and proposes the application of beyond-3G SSL-based authentication mechanisms into Wi-Fi networks. We suppose that the Authentication, Authorization and Accounting (AAA) procedures of a mobile Wi-Fi user can be controlled in a "centralized" or "semi-centralized" way by his home core 3G network. According to this arrangement, the Wi-Fi networking settings are considered as multiple entry points of a common 3G infrastructure. A Wi-Fi user needs to know only his home 3G network operator, who is responsible to establish and maintain RAs with various ending WLAN operators. Depending on the RA between the two operators, the user may receive Internet access through his home 3G network (via the Wi-Fi network) or directly through the current Wi-Fi access network, after being authenticated by his home 3G network. Obviously, such a solution also assumes that the user has a dual mode mobile station supporting both WLAN and UMTS, or the WLAN device can be linked with a UE, which supports USIM capabilities (Bluetooth, USB, IrDa).

Current 3GPP specifications for UMTS R6 [5], describe an interworking architecture where the home network is responsible for access control, while 3GPP proxy AAA relays access control signalling to the home 3GPP AAA server (see Figure 1). USIM based authentication mechanism can be based on the existing UMTS AKA method. As this method should be independent of the underlying WLAN standard and should be supported by a standard authentication mechanism, 3GPP seems to choose the EAP-AKA protocol described in [5] & [6]. EAP is a general protocol for PPP authentication, which can support multiple authentication mechanisms. Consequently, EAP-AKA provides a way to exchange AKA authentication messages encapsulated within the EAP protocol.

In case the Serving Network (SN) is a WLAN, the mobile terminal is connected to an Access Point (AP). The user presents his Network Access Identifier (NAI), which is of the form IMSI@domain or Packet_TMSI@domain. The access request is forwarded to the AAA proxy that translates the AAA request into the equivalent 3G AAA protocol request. Note that this Proxy or Gateway might be pre-configured or dynamically searched. The procedure may cross several other authentication domains. Usually the EAP server is separate from the authenticator node, which resides closest to the user's machine (also called *Supplicant*) e.g. an AP or an 802.1X bridge. The supplicant communicates with the AAA server that provides EAP server functionality using an AAA protocol, such as RADIUS or DIAMETER.

This approach has the main advantage that mobility management, roaming, billing and location issues are under the supervision of the "master" UMTS network. Consequently, the users know only the UMTS operator, which is responsible to establish and maintain agreements with WLAN delegates. An enhanced system would also require support for "*vertical*" handover between WLAN and UMTS. This approach also minimizes the necessary changes to the existing 3G network core elements (e.g. HSS, GGSN).

From the user's security standpoint, USIM based authentication of a subscriber for WLAN services, offers two significant benefits: (a) easy integration of the WLAN's subscriber credentials, to 3G Home Subscriber Server (HSS), as those are of identical format to 2.5/3G, and (b) WLAN's security level equal to that offered by 2.5/3G, thereby resolving the drawbacks of current IEEE 802.11 protocols [7],[8].

However, as it is desirable to support mutual authentication and since EAP-AKA assumes the existence of a long-term symmetric key per subscriber, it is useful to have a mechanism for session key establishment. Introducing SSL/TLS, we can take advantage of the protected and flexible ciphersuite negotiation, mutual authentication and scalable key management capabilities, in order to provide strong authentication and end-to-end security to the user of this heterogeneous architecture.

3. EXISTING PROBLEMS IN 3G AKA AND EAP-AKA

In UMTS, the AKA mechanism is somewhat similar to the authentication in GSM. The authentication in both systems is based on a symmetric secret key K, which is stored in the user's USIM card and in the corresponding HE's Home Subscriber Server / Home Location Register (HSS/HLR). The procedure, as described in [9], is based on the Challenge/Response protocol. Note that AKA is used for authentication purposes at both the radio network and the IP multimedia subsystem (IM), introduced in UMTS release 5. Hence, the radio network uses IMSI, whereas the IM uses NAI.

Although several known weaknesses in AKA GSM seem to be now fixed in UMTS, there are still some "gaps" which affect the EAP-AKA mechanism too [10]:

- Passive or active attacks that can compromise authentication vectors either from the Serving GPRS support node (SGSN) or HSS/HLR which store a number of vectors for each user, or from the SGSN – HE/HLR link. The problem becomes more important in case the subscriber is roaming between two or more serving networks, where the home network (HSS/HLR) has always to send authentication vectors for use by the serving network.
- In some cases, the system allows the identification of a user by means of the permanent subscriber identity (IMSI) in clear text. The procedure is open to passive attacks, where the intruder is waiting for potential IMSI transmissions in clear text or active (man-in-the middle) attacks [10].

- The key sizes and the ciphering and deciphering algorithms are fixed. This makes the whole mechanism inflexible and less secure, whenever security vulnerabilities are discovered in an existing algorithm, like in the case of GSM's A5/1 algorithm [11].
- One security enhancement in UMTS is the inclusion of integrity protection service. However, integrity is only guaranteed for signalling data between RNC and MS. The user data do not have an associated integrity checksum, and are consequently vulnerable to replay attacks.
- In addition to securing mobile communications, the security mechanisms in mobile devices should be able to provide security services for multimedia applications and IP-based services. The challenge is even greater when mobile communication involves multiple domains in wireless, self-configuring, and heterogeneous environments.

Additionally, we can mention the following deficiencies related to EAP-AKA:

- The authentication procedure may require several request/response exchanges. When the user roams from one cell to another, he should gain or request authentication from the 3G AAA home server. This means that authentication efficiency should be significantly considered, since it is involved in the latency quality of the handover procedure.
- Identity privacy support can be optionally included in EAP-AKA to protect the privacy of the subscriber identity against passive eavesdropping. However, this mechanism cannot be used on the first connection with a given server and the IMSI must be sent in cleartext. In addition, active attacks can be triggered from individuals that impersonate the network using the AT_PERMANENT_ID_REQ attribute to obtain the subscriber's IMSI.
- EAP/AKA does not support ciphersuite negotiation or protocol version negotiation.
- Other protocol attacks are also possible, for instance man-in-the-middle and negotiation attacks, as described in [6].

4. Introducing EAP- TLS in Heterogeneous Mobile Environments

EAP-TLS [12] is based on SSL Version 3.0, and the SSL handshake is performed over EAP, whereas on the Internet the handshake is carried out over TCP. As EAP-TLS performs mutual

SSL authentication, each side is required to prove its identity to the other using its certificate and its private key.

Certainly to implement an AKA mechanism based on SSL/TLS, we need some sort of public key infrastructure (PKI), which is not necessarily part of the 3G-network core. Integration between 3G mobile systems and PKI has not been standardized yet, but recent 3GGP discussion documents [13] deal with that particular subject. Successful wireless PKI implementations and solutions from companies like Sonera Smarttrust, Lucent Technologies and Entrust, strengthen the assertion that PKI has become an acknowledged and promising component of standards. Projects like ASPeCT [14] and USECA [15], Third Generation Partnership Project (3GPP) discussion papers especially for UMTS R6, as well as other papers [16], foresee that evolution. The eNorge 2005 strategy calls for a shared PKI for Norway, while advanced standards such MexE, WAP and i-mode from NTT DoCoMo have moved forward to introduce public key methods.

More specifically, the introduction of EAP-TLS requires the following:

- There is some sort of Certification Authority (CA), which issues and revokes certificates. This can be public in the form of a common Trusted Third Party (TTP) or private.
- 3G+ USIM card is a crypto-card with good pseudo-random (or random) generation capabilities and in-built crypto accelerator chip.
- Every subscriber possesses a key pair (private + public), and his private key is stored in his USIM card. The keys are generated by either the mobile operator or TTP and associated with the user at registration time.
- USIM card is pre-loaded with all CAs public keys, which exist (or associate with) the particular operator.
- Every AAA server, which takes part in EAP-AKA procedure, possesses a similar key pair and the corresponding digital certificate.
- Every AAA server keeps track and stores possible CAs Cross reference certificates, which enable inter-operator trust relationships.
- There is one-at-least digital certificate database, which stores all the digital certificates (CR) and is being managed by the operator's CA or by a TTP.

Performance considerations have held from using SSL/TLS in resource-constrained environments, like the wireless one. Nevertheless, the necessity for more processing power and memory, has driven smart cards toward more advanced architectures, all the way to where we are beginning to see 32-bit RISC-based ARM processors in smart cards. These cards can effectively store and protect the subscriber's private key, generate good pseudo-random values and take over of symmetric key (un)+wrapping functions. Mobile's device processor can efficiently carry out the rest of the calculations needed by SSL/TLS protocol. A recent study has also shown the feasibility of SSL/TLS in handheld wireless devices [2], while relevant work showed that SSL's handshake protocol time can be improved up to 5.7X times [17].

SSL/TLS supports different protocols for creating pre-master keys (RSA, Diffie-Hellman, etc), several different cryptographic algorithms and two different MAC algorithms. In the context of an AKA procedure, these properties can provide the appropriate flexibility in an integrated 3G-WLAN environment, when the available means (from a perspective of diversity and computational power) at the attackers side are increasing rapidly.

5. An AKA Mechanism Based On EAP-TLS

Motivated by the aforementioned technological trends, we propose an alternative AKA procedure for integrated 3G/Wi-Fi networks based on EAP-TLS, instead of EAP-AKA,. Figure 2 depicts the exchange of EAP-TLS protocol messages, including the essential adaptations to make it "mobile-enabled" and focusing on public key operations in the supplicant side which is generally considered as computational weak.

The selection of the appropriate 3G AAA server is based on NAI. Since the client claims his identity in the EAP-Response Identity packet, the EAP server should verify that the claimed identity corresponds to the certificate presented by the peer. This means that the user ID must be included in the peer certificate. From the AAA server side, a mapping from the temporary identifier (P-TMSI) to the IMSI is required too. Likewise, supplicant must check against EAP's server certificate validity (Expiration time / Name / Signed by trusted CA etc). A detailed explanation of the pure EAP-TLS protocol is given in [12].

When comparing the two available options, EAP-AKA and EAP-TLS, we can mark down the following:

- The 3GPP network architecture to support integration remains the same with the addition of the underlying PKI. As shown in Figure 3, a CA can be connected with the 3G-core network, either through GGSN ("natural" option), SGSN, Proxy or Serving Call State Control Function (P-CSCF / S-CSCF) or with the addition of a new gateway element, which is connected to AAA server. This last option guarantees minimal changes to 3G-core network elements. In any case, new IP interfaces have to be created accordingly.
- The supplicant and the AAA server must support EAP-TLS, while the AP has to support EAP-TLS authentication. Currently, EAP-TLS protocol is becoming widely supported by the most accredited vendors in routers, APs and end user terminals, ensuring minimal changes and easy integration.
- Any AAA server (WLAN or 3G) that resides near the supplicant can provide for authentication, thus improving mobility. This is possible as the "Any-AAA server" can exchange (offline) cross-reference certificates with the home AAA server, or both can have a signed certificate from a common (root) CA. Accounting details could be "batch transferred", according to bilateral pre-arrangements.
- Supplicant certificate revocation can be handled by IMSI, thus avoiding CRLs and related procedures.
- The overall performance can be significant enhanced, using SSL/TLS option for session resumption. The purpose of sessionID included in supplicant's hello message, is to allow for improved efficiency in the case where a client repeatedly attempts to authenticate to an EAP server within a short period of time. Based on the sessionID chosen by the peer, and the time elapsed since the previous authentication, the EAP server will decide whether the proposed session should be resumed or not. Recent studies also showed that session reuse could be further improved, using an SSL/TLS session aware dispatcher, when the operator is planning to install a cluster of SSL/TLS authentication servers [18].
- SSL/TLS protocol has proved its effectiveness in the wired Internet, and, seconded by PKI, is best suited to support large heterogeneous infrastructures. The flexibility to

choose among several ciphersuites and built in MAC algorithms decrease the possibility of intrusions. For instance, using ephemeral Diffie-Hellman key_exchange can support forward secrecy. Furthermore, the scalability of public key mechanisms offers a competitive framework to overcome symmetric key based security inefficiencies. Last but not least, PKI add-on value services, like the use of Attribute Certificates (AC) are also possible [19].

- There is no need for HSS/HLR to generate and distribute authentication quintuplets, thus avoiding the risk to be stolen or spoiled. On the other hand, certificates control mutual authentication process.
- AKA-TLS has to be generally considered as an *end-to-end* authentication procedure in contrast to EAP-AKA, which provides a *hop-by-hop* fashioned security, as intermediate devices should implement IPsec, MAPsec or SSL to secure inter or intra network communications.

6. CONCLUSIONS

We considered the authentication problem faced by 3G mobile roaming subscribers who need to access wireless Internet services through Wi-Fi hot spots administrated by different operators. We proposed the application of EAP-TLS, in contrast to EAP-AKA based authentication mechanisms, into integrated 3G and Wi-Fi networks to provide strong end-to-end security and authentication to the user. Our proposed solution overcomes 3G and WLAN authentication inefficiencies, while users are also offered the possibility to enjoy add-on value services, which stem from PKI incorporation.

7. REFERENCES

[1] WAP forum WAP-217-WPKI, Wireless Application Protocol Public Key Infrastructure Definition; www.wapforum.org/what/technical.htm.

[2] Gupta V. & Gupta S., Experiments in Wireless Internet Security, *In the Proc. Of IEEE Wireless Communications and Networking Conf. (WCNC 2002)*, no. 1, pp. 859-863, March 2002.

[3] Kambourakis G., Rouskas A., & Gritzalis S., "Using SSL in Authentication and Key Agreement Procedures of Future Mobile Networks", *In the Proc. Of the 4th IEEE Int'l Conf. On Mobile and Wireless Comm. Networks (MWCN 2002)*, pp. 152-156, Sep. 2002.

[4] Salkintzis, A., Fors, C. & Pazhyannur, R., "WLAN-GPRS Integration for Next-Generation Mobile Data Networks", IEEE Wireless Communications Magazine, pp. 112-124, Oct 2002.

[5] 3GPP Technical Specification, WLAN Interworking Security, (TS 33.cde v0.1.0), July 2002.

[6] Arkko, J. and Haverinen, H., “EAP-AKA Authentication”, <draft-arkko-pppext-eap-aka-10.txt>, June 2003.

[7] M. Gast, "*802.11 Wireless Networks: The Definitive Guide*", O'Reilly, April 2002.

[8] D. Eaton, “Diving into the 802.11i Spec: A Tutorial”. Feb 2003, electronically available in http://www.commsdesign.com/design_corner/OEG20021126S0003.

[9] 3GPP Technical Specification, 3G Security Architecture, TS 33.102 v.5.1.0), December 2002.

[10] 3GPP Technical Specification, A guide to 3rd Generation Security, (TR 33.900 v.1.2.0), Jan 2000.

[11] Khare R., “W* Effect Considered Harmful”, IEEE Internet Computing, Vol. 3, no. 4, pp. 82-92, July/August 1999.

[12] IETF RFC 2716, “PPP EAP-TLS Authentication Protocol”, Oct. 1999.

[13] 3GPP TSG, “Architecture proposal to support subscriber certificates”, Discussion and Approval document, Tdoc S2-022854, Oct. 2002.

[14] ASPeCT Project, Securing the future of mobile communications, http://www.esat.kuleuven.ac.be/cosic/aspect, 1999.

[15] USECA Project, UMTS Security Architecture: Intermidiate report on a PKI architecture for UMTS, Public Report, July 1999.

[16] Kambourakis G., Rouskas A., Gritzalis S., "Introducing PKI to enhance Security in Future Mobile Networks", in the Proc. of the IFIPSEC'2003 18th IFIP Int’l Information Security Conf., pp.109-120, Athens, Greece May 2003.

[17] Nachiketh, P., Srivaths, R., Anand, R. & Ganesh, L., “Optimizing Public-Key Encryption for Wireless Clients”, *In the Proc. Of the IEEE Int’l Conf. On Communications (ICC 2002)*, no 1, pp. 1050 – 1056, April 2002.

[18] Apostolopoulos, G. et al., Securing Electronic Commerce: Reducing the SSL Overhead, IEEE Network Magazine, no 4, pp. 8-16, July/August 2000.

[19] 3GPP TSG, “Support of certificates in 3GPP security Architecture”, Discussion Document S3-010353 SA WG3 Security – S3#19, July 2001.

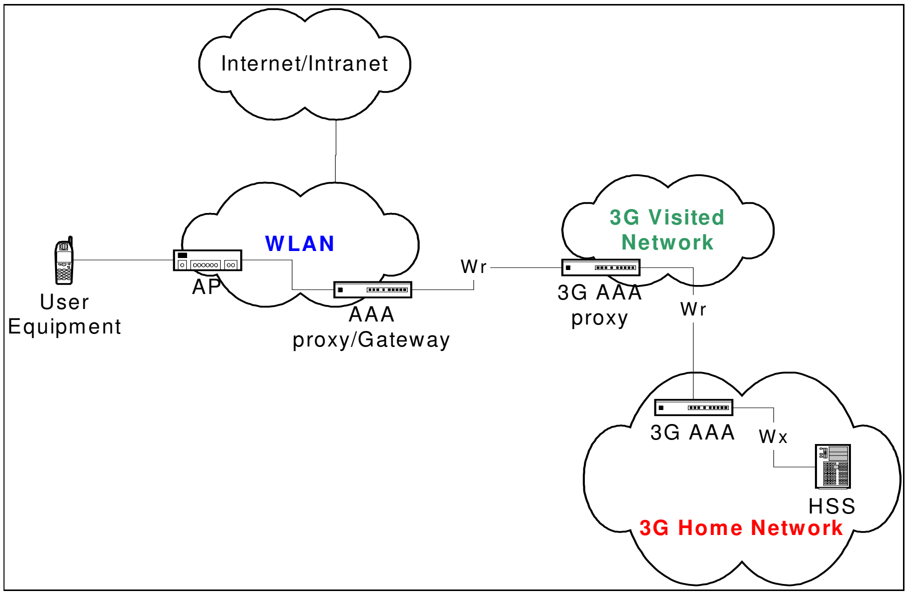


Figure 1. Wi-Fi integration in UMTS concept

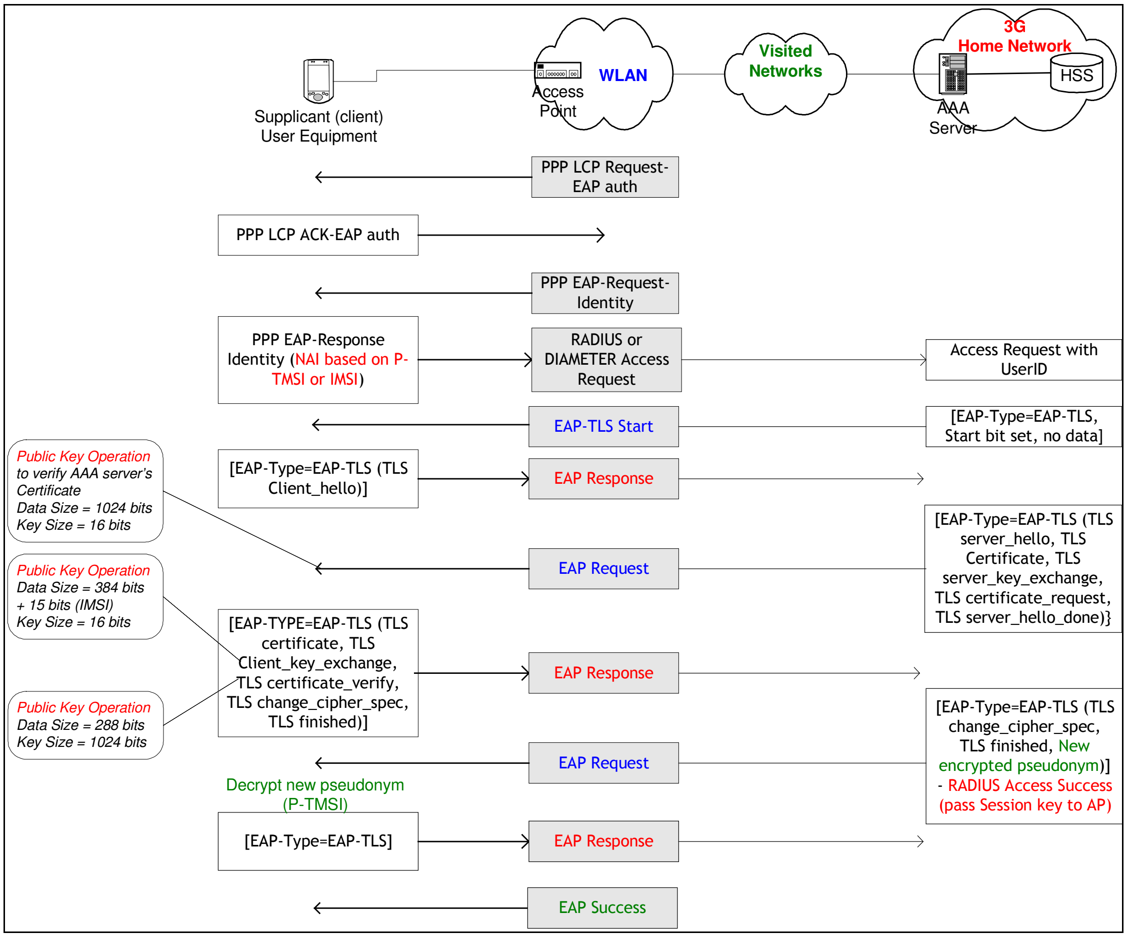
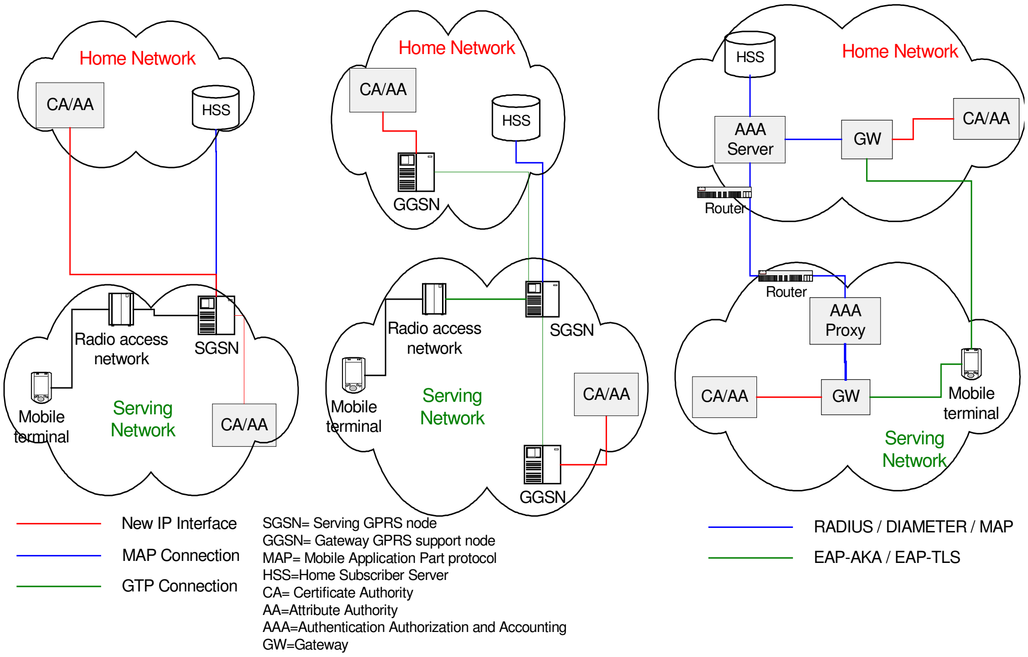


Figure 2. AKA Mechanism based on EAP-TLS for WLAN-3G interworking



SGSN= Serving GPRS node
GGSN= Gateway GPRS support node
MAP= Mobile Application Part protocol
HSS=Home Subscriber Server
CA= Certificate Authority
AA=Attribute Authority
AAA=Authentication Authorization and Accounting
GW=Gateway

Figure 3. UMTS Architecture to support PKI