Inter/Intra Core Network Security with PKI for 3G-and-Beyond Systems

Georgios Kambourakis, Angelos Rouskas, and Stefanos Gritzalis

Department of Information and Communications Systems Engineering
University of the Aegean, Samos 83200, Greece
{gkamb, arouskas, sgritz}@aegean.gr

Abstract. With a large number of different heterogeneous network technologies (e.g. UMTS, WLAN, HIPERLAN) and operators expected in the future mobile communications environment, that should frequently and seamlessly interwork with each other and a constantly increasing population of communication parties, capturing the full benefits of open channel key transfers and scaling public key methods requires Public Key Infrastructure (PKI). In this paper, we discuss and investigate different ways to take advantage of a proposed PKI system. Focusing on UMTS Release 6 IP multimedia subsystem, we analyze the ongoing 3GPP specifications and its limitations and examine how PKI can provide robust security solutions to both 3G-and-beyond inter/intra core network and the mobile user. Public key security mechanisms to protect operator's core networks seem to gain ground and protocols like IPsec and SSL, seconded by PKI, can support the continuous growth of diverse technologies and solve inter-operator many-to-many modeled trust relationships. From the user's side we present solutions, which far enhance authentication procedures and end-to-end communication model trust. We argue that PKI can become a promising candidate, which offers the competitive framework to overcome symmetric key based security inefficiencies and provide powerful solutions to protect both network core signalling and user's data from potential intruders.

Keywords: PKI; Mobile Networks; UMTS; Network Domain Security; SSL/TLS; Ipsec.

1 Introduction

An identified weakness in 2G systems security architecture is the absence of security in the core network. For instance, cipher keys are used to protect the traffic on the radio interface, but those keys are themselves transmitted unprotected between different networks. Originally and up to UMTS Release 99, this was not a problem, since 2G Signalling System Number 7 (SS7) networks were closed networks with very little interworking among different 2G operators and between 2G operators and the Internet.

Nevertheless, in a future wireless communication environment, like 3G and beyond, that will require frequent interworking of many different network technologies and providers there will also be a greater need for advanced security protection. Moreover, the introduction of IP, used not only for signalling traffic, but also for user

N. Mitrou et al. (Eds.): NETWORKING 2004, LNCS 3042, pp. 13–24, 2004.

traffic, as the network layer in the GPRS backbone network and later in the UMTS network domain (Figure 1), raises further reasons to worry about. Although this does not mean that inter/intra core network signalling would be carried over open connections, the involvement of many more "players" certainly brings a shift towards easier access to core network traffic.

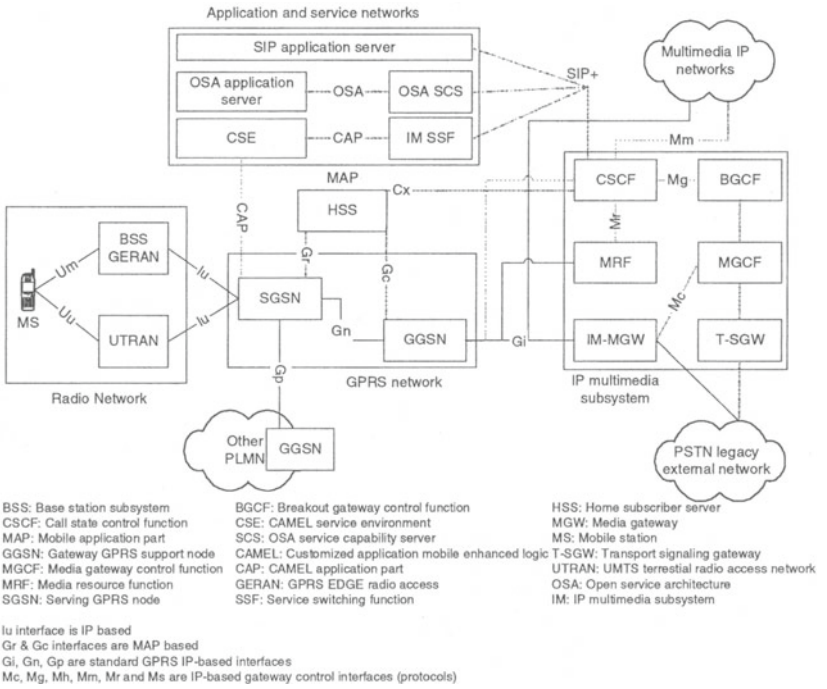

Fig. 1. UMTS Rel. 6 all-IP network architecture

Current mobile network standards perform user authentication, signalling and data encryption, as well as message integrity protection, by utilizing only symmetric key methods. However, as communication is envisaged to change from second generation (2G) person-to-person model to fourth generation (4G) machine-to-machine model, there is greater demand to provide more flexible, reconfigurable and scalable security mechanisms that can advance in a many-to-many trust relationship model.

PKI is gradually being introduced in the market, and its adaptation in future mobile networks will substitute long-term symmetric key relationships, with a flexible, reconfigurable and scalable public key based system. This will not only provide the appropriate level of inter/intra operator trust, but it will also offer solutions that far enhance user-to-network confidence and end-to-end security options.

The rest of this paper is organized as follows. In Section 2, we provide an overview of the current 3G-inter/intra security options and explain how PKI can adapt to existing architecture. Section 3 deals with PKI-proposed solutions that provide inter/intra operator trust, while Section 4 discusses user-to-network and end-to-end security. The paper is concluded in Section 5.

2 3G Core Network Security Specifications and PKI

2.1 Outline of 3G Inter/Intra UMTS Network Security

Global Mobile System (GSM) and Universal Mobile Telecommunication System (UMTS) networks, (Figure 1) use Mobile Application Part (MAP) protocol for the exchange of signaling messages between network Elements (NEs). User profile exchange, authentication, and mobility management are performed using MAP. MAP runs typically over the SS7 protocol stack. For instance, the signaling between the mobile, Serving GPRS node (SGSN) and Gateway GPRS support node (GGSN) to the Home Subscriber Server (HSS), and also the SMS message centre all consist of SS7 signaling.

3rd Generation Partnership Project (3GPP) has also defined a mechanism for protecting the MAP protocol at the application layer [1],[2]. MAP may also be protected at the network layer when IP is used as the transport protocol. However, when internetworking with networks using SS7-based transport is necessary, protection at the application layer shall be used. For this reason a new protocol header has been developed to protect MAP operations, much in the same way as the Encapsulating Security Payload (ESP) protocol protects IP packets. This new protocol is called MAPsec. In protection mode 2 of MAPsec, both confidentiality and integrity are protected, while in protection mode 1, only integrity is protected. When protection mode 0 is used there is no protection. While MAP runs over SS7, MAPsec and Internet Key Exchange (IKE) always run over IP. Therefore, it is assumed that nodes implementing MAPsec always have IP connectivity in addition to SS7 connectivity. In the 3GPP architecture MAPsec is typically running between two different network operators and the same Security Associations (SAs) are shared by a number of NEs. The necessary MAPsec-SAs between networks are negotiated between the respective Key Administration Centres (KACs) of the networks.

On the other hand, for native IP protocols, as in the GPRS backbone network, security shall be provided at the network layer. The security protocols to be used are the IETF defined IPsec suite [3]. The UMTS network domain control plane is sectioned into security domains, which typically coincide with operator borders. The borders between the security domains are protected by Security Gateways (SEGs) as shown in Figure 2.

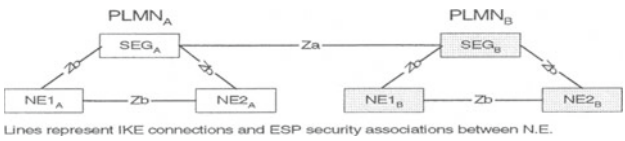

Fig. 2. Network Domain architecture for IP-based protocols

All network domain traffic shall pass though a SEG before entering or leaving the security domain. Consequently, IP Network Domain Security (NDS/IP) will only support tunnel mode IPsec SAs, ESP and main mode. SEGs shall offer capabilities for secure storage of long term keys used for IKE authentication, so NDS/IP will only

support Internet Security Association and Key Management Protocol (ISAKMP) SAs with pre-shared keys [4].

Only the inter-security domain SA IKE negotiations over the Za interface shall be mandatory, while the Zb interface is optional. Concluding, there is normally no NE-to-NE direct interface for NE belonging to different security domains.

2.2 PKI and Mobile Networks: A Viable Perspective

It was mentioned that in 3GPP's proposals and technical specifications the basic tool in protection of 3G-network domain traffic is IPsec protocol. The critical issue is key management: how to generate, exchange and distribute keys needed by algorithms that are used to provide confidentiality and integrity protection. Currently, agreements on keys and security associations are carried out on a bilateral basis between operators. However, as the number of network elements of each operator increases and the interworking between a high number of networks of different technologies will be frequent, a more scalable solution would be to replace those relationships with a PKI [5],[6]. This means that secure communications can be achieved without having to generate and distribute long-term secret keys.

PKI technology is gradually being introduced in the market. Projects like ASPeCT [7] and USECA [8], Third Generation Partnership Project (3GPP) discussion papers especially for UMTS R6 [9] as well as other papers [10] 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. Successful wireless PKI implementations and solutions from companies like Sonera Smarttrust, Lucent Technologies and Entrust, strengthens the assertion that PKI has become an acknowledged and promising component of standards.

Nevertheless, weighting up an asymmetric key system against a symmetric one, we note the following:

- The number of keys needed in a symmetric key system with n network elements communicating with each other is $O(n^2)$. On the other hand, in a public cryptosystem, the corresponding need for keys is $O(n)$. Therefore, when n increases, the costs in terms of key generation and distribution associated with the introduction of a new network element are quite different. In the symmetric model, we need to establish n new secret keys, while in the asymmetric case we only need 2 new keys (private + public) for any new network element.
- Pre-shared secrets are a rather inflexible way to provide authentication. A properly designed PKI, which supports digital certificates, will offer more dynamic, flexible and scalable mechanisms to issue certificates for new network elements and to revoke certificates that are no longer valid.
- One basic requirement and assumption in both GSM and UMTS, is that the Home Network has to trust the Serving Network, e.g. for the Authentication and Key Agreement (AKA) procedure. However, in future systems, where many different technologies, owned by different network operators, must frequently and seamlessly interwork, this is no longer the case. By introducing a Trusted Third Party (TTP) the requirement for bilateral trust is reduced.

- PKI can be used for authentication and symmetric key encapsulation and transport procedures, while derived symmetric session keys can be used to support confidentiality. Thus, we can by-pass the known public key cryptosystem disadvantages of key lengths and computational load.
- From the user scope, the implementation of public key algorithms in Mobile Stations (MSs) had been considered to be resource demanding. However, the increased processing requirements of IP capable terminals have driven towards high power computational platforms, which are now becoming ordinary in mobile devices.
- Furthermore, as IP-based networks are introduced to serve a large variety of applications, that may involve many and different network/service operators, complex and flexible communication relationships are necessary, which in turn demand a complex trust model. In many cases, the communication parties may not have prearranged security agreements. So, if unknown partners wish to perform mutual authentication and establish session keys, a public key based digital signature that is supported by a PKI will satisfy security needs. For example, a Session Initiation Protocol (SIP[1]) registration server, either proxy or redirect,[11] may not share any symmetric key with the User Equipment (UE). Instead, a digital signature may be an appropriate way to authenticate the proxy server.

2.3 Adaptation of PKI in Mobile Networks

Certainly, the support of asymmetric key services by a mobile network requires the adaptation of some PKI elements, which are not necessarily part of the current 3G-network core. Integration between 3G mobile systems and PKI has not been yet standardized, although, most recently 3GPP discussion papers deal with that particular subject [9],[12]. Figure 3 depicts the necessary PKI elements that should be included in the UMTS architecture. More specifically, we assume the following:

- There is some sort of Certification Authority (CA) per Public Land Mobile Network (PLMN) Operator, which issues and revokes certificates. Likewise, a presumable Attribute Authority (AA) can issue short-lived Attribute Certificates (ACs) [13] for the subscribers.
- There is at least one digital certificate database, which stores all the digital certificates and is being managed by the PLMN's CA.
- There is at least one revoked certificates database (CRL-database), which is being managed by the PLMN's CA and is accessible from all network elements that belong to the network core.
- Web servers or FTP servers can be used to store certificates and CRLs. Certificate revocation can be periodic or Online Certificate Status Protocol (OCSP) based. Revocation is generally a hard problem to run into. However, in that case, certificate revocation for core network elements can be handled manually as this proce-

[1] SIP is an application-layer, text-based, client-server control protocol that can establish, modify, or terminate user sessions. It has been chosen by 3GPP as the protocol for multimedia application in 3G mobile networks. See IP multimedia subsystem in Figure 1, where CSCF represent a SIP server. Upon registration every user is given a SIP URL of the format *sip:username@domainname.*

dure will happen infrequently. Moreover, subscriber's certificates revocation can be handled by International Mobile Subscriber Identity (IMSI).

- CAs which belong (or collaborate with) to different PLMN's issue (off-line) cross-reference certificates for inter-PLMN trust relationships. For instance in the case of two PLMNs with the corresponding certification authorities CA_a & CA_b, CA_a issues $Cert(CA_a)CA_a$[2] (the root certificate) and $Cert(CA_b)CA_a$. Respectively, CA_b issues $Cert(CA_b)CA_b$ and $Cert(CA_a)CA_b$.
- Cross-Reference certificates are cached in local Security Gateways SEGs (which probably implement firewall policies among other things) on the borders of IP security domains. Every PLMN can use one or more SEG, in order to balance inter network traffic.
- Every network element possesses a key pair (private, public), and the corresponding digital certificate (intra-operator trust). NE's private key and the public key of the local CA are stored locally in a secure manner.

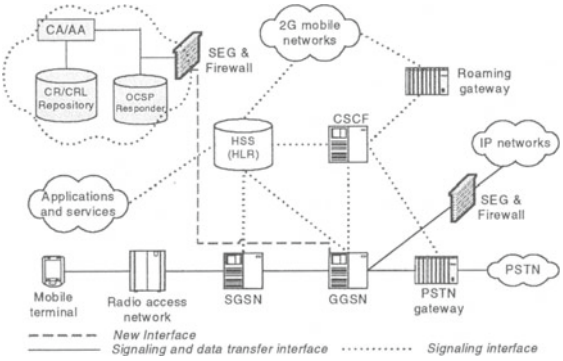

Fig. 3. General UMTS architecture Rel. 5 and PKI

If we are planning to extend PKI usage to the user, primarily for authentication, symmetric key encapsulation and support of certificates, we can assume the following:

- The User Services Identity Module (USIM) smart card should be a crypto-card with good pseudo-random (or random) generation capabilities and in-built crypto accelerator chip.
- Every subscriber possesses an asymmetric key pair and his private key is stored in his USIM card. The keys are associated with the user at registration time. IMSI handles revocation of subscriber's certificates, while attribute certificates are short-lived and will therefore not need to be included in any CRL.
- Furthermore, the USIM card is pre-loaded with all the CA's (root) public keys, which exist in the particular PLMN.

[2] $Cert(X)_Y$ = Public key certificate of X with format X.509v3 (or subset) issued by Y.

3 PKI-Based Intra/Inter Network Domain Security

3.1 IPsec, IKE, and SAs Establishment

With network domain security we mainly mean secure communications between network elements. Thus, by introducing a PKI to a future wireless network we can use powerful protocols to protect signaling and user traffic both between inter-network and intra network elements.

Two connections have to be protected as shown in Figure 2:

- Za or SEG-to-SEG (inter-operator security),
- Zb or SEG-to-NE and NE-to-NE (intra-operator security).

One candidate for this task is IPsec [14],[15] and IKE in particular. As we already mentioned, 3GPP currently uses pre-shared secrets for IKE phase I. This means that each NE has to be configured with a password that is associated with the remote system's IP address being authenticated. Note, however, that the keys to be used for encryption and authentication (SKEYID_*), after the completion of phase I, have been generated solely based on the peer's IP address [15]. So, in scenarios where the IP address is dynamic, the responder cannot maintain pre-shared secrets indexed by an IP address that may not be known at that time. Remote access solutions are an example where the initiator's IP address may be different for each connection (road-warrior cases and IKE's phase I main mode). Additionally, the main drawback in pre-shared secret key authentication is the lack of a secure and scalable mechanism for exchanging pre-shared secret keys. That is appropriate only in a rather small-scale environment with a restrained number of systems, in which the set of peers is known in advance. However, if a pre-shared secret key is compromised, there is no universal method to alert the peer and launch a replacement.

An alternative solution based on PKI, can overcome these shortcomings. In that case, IKE is used for key exchange over the Za, Zb interfaces, while the authentication could be based on digital signatures with certificates instead of pre-shared secrets. Consequently, the generation of the keys to be used for encryption and message authentication is based solely on the peer's nonce and Diffie-Hellman key value (SKEID = Pseudo_random_function (Nonce_i | Nonce_r, DH_Key). For system authentication, a certificate request can be included to obtain the public key of the peer if the initiator does not already have it. The peer must have the other's public key to validate the signature and authenticate the peer in the third exchange (IKE messages 5 & 6). Also, the use of certificates in such a scheme can provide for non-repudiation in key exchange e.g. when attribute certificates are used [15].

3.2 Introducing SSL/TLS

Another solution, which benefits by the incorporation of PKI, is the use of SSL/TLS to protect communications between security gateways and probably between NEs. Authentication for the corresponding NEs during the handshake procedure is mutual, and is performed by exchanging their certificates. SSL/TLS has many of the advantages of IPsec and the successful introduction of the protocol in the wired Internet has proved its usability and effectiveness. Likewise, SSL/TLS can be part of an all-IP

mobile environment, as it runs above TCP/IP and below higher-level protocols such as HTTP or FTP and consequently the TCP header is not encrypted.

For instance, using Performance Enhancing Proxies[3] (PEPs) in 3G in parallel with IPsec, end-to-end security can be compromised, as the PEP module must decode the encrypted IP protocol headers [16]. So either the packets bypass the PEP module and are directed to mobile hosts, in that case the connection will not benefit from any performance enhancement, or the user should trust the PEP in the middle (it is part of the IPsec's security association). In general however, the end system cannot trust PEPs.

3.3 UMTS IP Multimedia (IM) Subsystem

The case of application-level registration in UMTS Release 6, discussed below, proves even more the necessity for flexible and scalable public key security mechanisms. In an all-IP network, MS conducts two types of registration [11],[17].

Bearer-level registration (and authentication), where the MS registers with the GPRS network following the standard UMTS routing area update or attach procedures [18]. During that procedure the MS obtains an IP address and discovers (sending a DNS query) the Proxy CSCF (P-CSCF). The user may be at his home or at foreign network. The P-CSCF provides basic multimedia session support as well as functioning as a firewall to the IP multimedia (IM) subsystem.

Application-level registration (and authentication), where a Serving CSCF (S-CSCF) is assigned to MS. MS sends a REGISTER message to the P-CSCF, and this is relayed to an Interrogating CSCF (I-CSCF) in the home network (the home network can be found by the P-CSCF using the IMSI or SIP URL of the user). Thus I-CSCF acts as a gateway for serving networks. The I-CSCF in the home network communicates with HSS and retrieves the user's data from HSS's IM database (HSS is an HLR with new capabilities added to support IM subsystem. For example HSS may generate, store and manage security data and policies used in the IM subsystem). Then it selects an S-CSCF to deal with the requested service, as the latter has access to the resources needed to create services, such as video servers and media gateways.

We notice that a variety of network elements take part in application-level registration, especially when P-CSCF resides in a visited network. Moreover, the data being transferred are important to both the user and the network. Among others (e.g. CSCF-MS security parameters sent from the HSS to the I-CSCF), SIP messages may contain information a user or server wishes to keep private. For example, the headers can reveal information about the communication parties, or other confidential information. The SIP message body may also contain user information (media type, addresses, codec and ports, etc.) that should not be exposed.

Security should aim to keep network and user data private and prevent SIP sessions from being set up or modified by others masquerading the identity of the real user. As the confidentiality and integrity protection of SIP signaling is provided in a *hop-by-hop* fashion and SIP does not provide specific security features for that, protection relies on network level (IPsec) or transport-level (SSL) security. Note that hop-by-hop mechanisms are needed because intermediate elements may perform SIP processing by reading and/or writing some parts of SIP messages.

---

[3] PEPs improve the performance of wireless TCP connections between the core network and mobile hosts. Usually PEPs are implemented in the Radio Network Controller (RNC).

It is worth discussing the aforementioned Za and Zb interfaces in the case of SIP. 3GPP uses IPsec to secure communication between SIP entities that have preconfigured and thus have quite static security associations and policies. On the other hand, consider a roaming user who wishes to connect to a P-CSCF that resides in an Internet Telephony Service Provider (ITSP). No guarantee that secure transport will be used on the entire end-to-end path can be provided to the user.

To the best of our knowledge, the most recent version of the SIP specification [19] defines a way to indicate that a resource (e.g. a server or a user) should be reached securely using SSL. In that case a new type of URI (for example *sips:test@secure.com*) designates the use of SSL. This is well suited to architectures in which hop-by-hop security is required between hosts with a more dynamic and flexible security association using public key mechanisms. The incorporation of PKI can solve such problems, providing a scalable model, when interworking among different operators and diverse technologies (e.g. UMTS and IEEE 802.11) is required.

4 PKI and Mobile User Enhancements

From the user's side, a PKI can support the appropriate reconfigurable infrastructure, which offers great flexibility and scalability in an all-IP wireless environment. In this fashion, authentication and end-to-end security solutions can be provided to far enhance user's trust in a continuously evolving environment.

It is still a common misbelieve, that mobile devices are not ready for 'expensive', in terms of memory and processing power, public key computations. However, that is partially true, since contemporary mobile devices are featuring advanced architectures with processors up to 400 MHz, memory capacities of 64MB RAM and 32MB ROM, support for applications and strong operating systems. Besides that, these trends has also 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 based on such modern chips from companies like Atmel and Infineon are just appearing in the market, and they can effectively store and protect the subscriber's private key, generate good pseudo-random values and take over of symmetric key (un)wrapping functions. The mobile's device processor can efficiently take over the rest of the calculations, needed by protocols like IPsec and SSL.

4.1 Providing Public Key Based Mutual Authentication

In an IP-enabled mobile device with the aforesaid characteristics, IPsec, can effectively secure signalling and user traffic, therefore, providing a secure end-to-end channel. Once again, IKE with authentication based on digital certificates will be used instead of pre-shared secrets. Road-warrior cases can also be effectively authenticated using this scheme.

For example, consider the following scenario. A business employee has IPsec-based Virtual Private Network (VPN) client software installed on his laptop, which is connected to his wireless network provider, via his mobile phone. Also assume that the employee is roaming to a foreign (serving) network. Upon connection, the employee is being authenticated by IKE sending its digital certificate and receiving

SGSN's certificate and cross-reference certificate. When IPsec's SAs have been created, VPN client filters the traffic, watching for IP packets destined to the employee's head office. It allows any traffic not going to the head office to pass unprotected. When however the client spots a packet that is addressed to the head office intercepts it. It then uses IPsec services to transmit the packet securely and to assure that all traffic back from the head office to him is also secure.

The first thing that the VPN client does is to establish a bi-directional IPsec Security Association (SA) with the head office server. IKE (ISAKMP) [20] defines the framework how the VPN client and server set up security associations. It does however require the use of digital signatures within the authentication section. This means that the VPN client and server must have IPsec public key certificates to be able to establish a security association.

Taking into account the aforesaid technological trends, SSL can provide for user authentication and end-to-end security [21],[22]. Until now performance considerations in using SSL in a resource-constrained environment drove wireless designers to choose a different, incompatible and insecure gateway oriented security protocol for their mobile clients, like in the case of WAP. The ASPeCT project has demonstrated that public-key authentication is possible and GSM and UMTS applications can coexist on a single smart card. A recent study has also shown the feasibility of SSL in handheld wireless devices [22] while relevant work showed that SSL's handshake protocol time could be improved up to 5.7X times [23].

4.2 Support of Subscriber's Certificates

Another "added value" PKI service could be the support of subscribers' certificates [12]. Figure 4 depicts a presumable network architecture where a subscriber can obtain (attribute) certificates [13] regardless of the network (home or serving) he is connected to. Other alternative architectures are also possible for implementation; e.g. direct connection of CA/AA with GGSN or SGSN or even CSCF, although the proposed solution has minimum effects on existing 3G core network nodes.

The AAA server in the subscribers home network, provide the actual authentication for the subscriber. Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA) [24] is an appropriate, directly applicable in UMTS, access-independent, user authentication method to support this architecture, as it provides a way to exchange AKA authentication messages encapsulated within the EAP protocol. Note that 3GPP has chosen EAP-AKA to support authentication of a subscriber who access WLAN subsystems. Of course SSL and/or IKE connections can be used to support such architecture. In either case, MS has to support new authentication mechanisms e.g. EAP-AKA or SSL.

In the first case, MS has to discover the appropriate (visited or home) Certificate Gateway (CG) and send a certificate request to it using EAP-AKA. CG acts as a certificate-provisioning gateway for the MS. EAP messages will be routed to an AAA server in the subscriber home network probably through a local AAA proxy. CG will wait for a reply from AAA server indicating successful or abortive authentication and other possibly required subscriber data, retrieved from HSS. If certificate issuing for this subscriber is endorsed, CA or AA generates and signs the certificate, updates its database and returns the certificate back to CG.

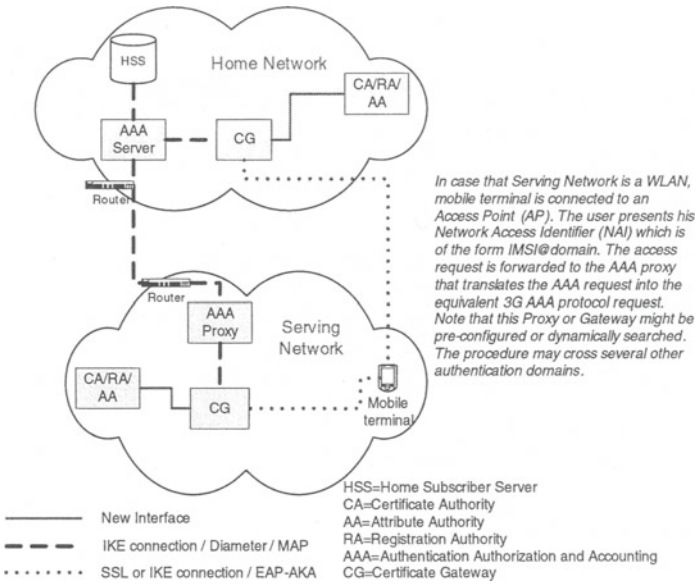

Fig. 4. Network Architecture to support subscriber's certificates

5 Conclusions

The constantly increasing population of users expect from mobile operators to provide features that will protect their data while in transit, safeguard their billing and customer information, and offer availability and quality comparable to that of the wired services. Thus, more flexible, dynamic and scalable security mechanisms are necessary in order to support on-demand services and all-IP end-to-end solutions in a many-to-many trust model integrated with the Internet environment. In this paper, we proposed several alternative procedures based on PKI infrastructure and public key enabled protocols introduced in the mobile network architecture. The ultimate challenge is the invigoration of future inter/intra mobile core network security, enhancing authentication procedures and end-to-end communication model trust. We showed that PKI can be a competitive player, offering the appropriate framework to overcome symmetric key based security inefficiencies and providing powerful solutions to protect both 3G-and-beyond network core signaling and user's data.

References

1. 3GPP Tech. Spec. , "MAP Application Layer Security", (TS 33.200 v. 5.1.0), Dec. 2002.
2. Arko, J. and Blom, R., "The MAP Security Domain of Interpretation for Internet Security Association and Key Management Protocol", <draft-arkko-map-doi-07.txt>, May 2002.

3. Kent, S. & Atkinson, R., "Security Architecture for the Internet Protocol", IETF RFC 2401, Nov. 1998.
4. 3GPP Tech. Spec., "IP Network Layer Security", (TS 33.210 v.5.3.0), Mar 2003.
5. 3GPP TSG, "Using PKI to provide network domain security", Discussion Document S3-010622 SA WG3 Security – S3#21, Nov. 2001.
6. 3GPP TSG, "Security Services using Public Key Cryptography", Discussion Document S3z000025 SA WG3 Security – S3#15bis, Nov. 2000.
7. ASPeCT Proj, Securing the Future of Mobile Comm., www.esat.kuleuven.ac.be/cosic/aspect.
8. USECA Project, UMTS Security Architecture: Intermediate report on PKI architecture for UMTS, Public Report, July 1999.
9. 3GPP TSG, "Architecture proposal to support subscriber certificates", Discussion and Approval document, Tdoc S2-022854, Oct. 2002.
10. 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.
11. 3GPP Tech. Spec., "Access security for IP-based services", (TS 33.203 v.5.2.0), June 2002.
12. 3GPP TSG, "Support of certificates in 3GPP security Architecture", Discussion Document S3-010353 SA WG3 Security – S3#19, July 2001.
13. Oppliger, R., Pernul, G. & Strauss, C., "Using Attribute Certificates to Implement Role Based Authorization and Access Control Models", In the Proc. of 4. Fachtagung Sicherheit in Informationsystemen (SIS 2000), pp. 169 – 184, Oct. 2000.
14. Frankel, S., *Demystifying IPsec Puzzle*, Artech House, 2001.
15. Tiller, J., *A Technical Guide to IPsec Virtual Private Networks*, Auerbach CRC Press, 2000.
16. Assaf, N. et. al., "Interworking between IP Security and Performance Enhancing Proxies for Mobile Networks", IEEE Comm. Mag., pp.138-144, May 2002.
17. Lin, Y., & Pang, A., "An All-IP Approach for UMTS Third-Generation Mobile Networks", IEEE Network, pp. 8-19, Sept./Oct. 2002.
18. 3GPP Tech. Spec., "Security Architecture", (TS 33.102 v.5.1.0), December 2002.
19. Rosenberg, J. et al., "SIP: Session Initiation Protocol", IETF RFC 3261, June 2002.
20. Maughan, D., et al, "Internet Security Association and Key Management Protocol (ISAKMP)", IETF RFC 2408, Nov. 1998.
21. Kambourakis G., Rouskas A., & Gritzalis S., "Using SSL/TLS 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), Stockholm, pp. 152-156, Sep 2002.
22. Gupta V. & Gupta S., "Experiments in Wireless Internet Security", In the Proc. of IEEE Wireless Comm. & Networking Conf. (WCNC 2002),no. 1,pp. 859-863,March 2002.
23. 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.
24. Arkko, J. and Haverinen, H., "EAP-AKA Authentication", <draft-arkko-pppext-eap-aka-10.txt>, June 2003.