Evaluation of digital certificates acquisition in large-scale 802.11-3GPP hybrid environments

Nikolaos Doukas*, Eleni Klaoudatou**, Georgios Kambourakis, Angelos Rouskas and Stefanos Gritzalis

Department of Information and Communication Systems Engineering
University of the Aegean, Karlovassi, GR-83200 Samos, Greece
Tel: +30-22730-82010 Fax: +30-22730-82000
Email:{*icsdm02002, **icsdm03019}@icsd.aegean.gr; {gkamb,arouskas,sgritz}@aegean.gr

Abstract— **This paper evaluates the performance of a hybrid WLAN-3GPP network architecture for delivering subscribers' certificates. Two main categories of simulation scenarios are implemented and evaluated based on the underlying access network technology used; 802.11b and UMTS. Each of the scenarios is categorized further in numerous sub-cases. Results showed that AC acquisition when deployed in large scale between several heterogeneous networks is feasible within acceptable time limits.**

Index Terms—**Attribute Certificates; Heterogeneous Wireless Environments WLAN-3G; PKI; Security.**

I. Introduction

The Third Generation (3G) of mobile communication systems is moving towards to fulfill the vision of what is called 'all-IP'. As a result, connectivity solutions have been focused on the integration of heterogeneous networks to provide a unified access to the Third Generation Partnership Project (3GPP) systems. Moving towards this direction, 3GPP has recently provided a cellular-WLAN interworking architecture as an add-on to 3GPP system specifications [1,2,3].

More particularly, this specification defines the procedures for the AAA services that need to be supported through the 3GPP System in order to allow the WLAN User Equipments (UEs) to access WLAN infrastructures, and provide WLAN UEs with IP bearer capability to access Packet Switched (PS) based services provided by the 3GPP providers. The user's 3GPP home network is always responsible for access control, while the system provides Authentication, Authorization and Accounting (AAA) proxy that relays access control signaling to the AAA server of the 3GPP subscriber's home network.

On the other hand, the provision of new services for the mobile users, introduces new security issues 3GPP providers should deal with. For instance, in the near future, mobile users will carry out sensitive transactions (e.g. m-banking and m-commerce services) using the mobile network. As a result, effective certification and authorization of the mobile users becomes a critical issue. Attribute Certificates (ACs) [4] seem to be more suitable, when compared to Public Key Certificates (PKCs), for carrying user's authorization information and for temporary or time-limited transactions due to their ephemeral nature (short-life) that suppresses revocation. The main difference between PKCs and ACs is that the first bind an entity with a public key whereas the second bind an entity with an attribute. ACs can be used to specify various attributes like role, group membership, security clearance or any other authorization related information associated with the AC holder. An AC may be used with various security services, including access control, data origin authentication, and non-repudiation. ACs are included into both the ANSI X.957 standard and the X.509 recommendation of ITU-T and ISO/IEC as well as in IETF RFC 3281 [4].

Role-Based Access Control (RBAC) [5,6] seems to be the most promising method for access control and a better alternative to mandatory access control (MAC) and discretionary access control (DAC) schemes. It is also supported by the fourth edition of X.509 recommendation. RBAC associates permissions to roles. First of all the roles are specified and then those roles are associated with permissions based on the authorization policy. Each user may have numerous roles.

The support of the RBAC model in the X.509 recommendation is based on the use of two types of ACs, the Role-specification ACs and the Role-assignments ACs. Role-specification ACs specify the rights for each role (the AC holder is the role and the Attribute field contains the privileges granted for this role). Role-assignment ACs specify the roles for each user (the AC holder is the user and the Attributes field contains his roles). In this context, this paper evaluates the performance of a WLAN-3GPP network architecture for delivering, primarily, subscribers' ACs in large scale hybrid environments. Performance evaluation, in terms of service times, is based on simulation results. Two main scenarios are implemented based on the access network technology used. In the first scenario, a WLAN-based access network is assumed for the user to connect to, whereas in the second scenario a UMTS-based access network is providing access to the user. Each one of the aforementioned scenarios is categorized further in several sub-cases.

The rest of the paper is organized as follows. Section II gives an overview of the proposed hybrid WLAN-3GPP network architecture capable of delivering subscribers' certificates, while Section III presents the simulation scenarios and assumptions and the derived performance results. The last section concludes the paper and introduces some future work.

II. The Proposed Architecture

3GPP does not assume any specific type of WLAN system, but for the purpose of this paper we presume that the WLAN is of the IEEE 802.11 type. The proposed architecture, which extends undergoing work by 3GPP, enables a Wi-Fi user, who is also a subscriber to a 3GPP mobile network operator, to move across WLAN segments administrated by different WLAN operators and to acquire on-demand ACs. Consequently, the user needs to know only his home 3G network operator, who is responsible to establish and maintain Roaming Agreements (RAs) with various intermediate visited 3GPP and ending WLAN operators.

Figure 1 depicts the proposed architecture, which is fully compatible with 3GPP WLAN-3G interworking specifications [1,2,3]. The anticipated architecture includes a new gateway element which acts as a Certificate provisioning Gateway (CGW) for the user. The proposed schema also requires the specification of new IP interfaces and protocol messages between the CGW and the corresponding 3GPP network elements (e.g. between CGW and CA/AA). It is to be noted that this hybrid WLAN-3GPP architecture has been originally introduced and discussed broadly in [7,8]. The present work focuses only on evaluation issues considering large-scale deployment.

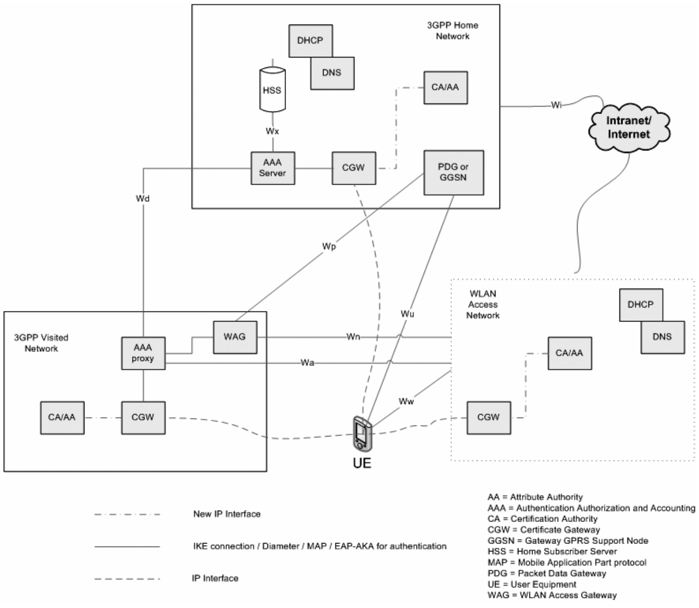
3GPP Home Network
DHCP
DNS
HSS
CA/AA
Wx
AAA Server
CGW
PDG or GGSN
Wi
Intranet/ Internet
Wd
Wp
Wu
WLAN Access Network
DHCP
DNS
3GPP Visited Network
AAA proxy
WAG
Wn
Wa
CA/AA
Ww
CA/AA
CGW
CGW
UE
New IP Interface
IKE connection / Diameter / MAP / EAP-AKA for authentication
IP Interface
AA = Attribute Authority
AAA = Authentication Authorization and Accounting
CA = Certification Authority
CGW = Certificate Gateway
GGSN = Gateway GPRS Support Node
HSS = Home Subscriber Server
MAP = Mobile Application Part protocol
PDG = Packet Data Gateway
UE = User Equipment
WAG = WLAN Access Gateway

Fig. 1. The proposed architecture

Moreover, we introduce the necessary Public Key Infrastructure (PKI) elements for digital certification provision, with the assumption that all 3GPP core network communications are already secured by the appropriate protocols. For example, IPsec Authentication Header (AH) protocol in transport mode can be used to protect intra-network communications along with IPsec Encapsulating Security Payload (ESP) protocol in tunnel mode for the protection of inter-network communications, as it is specified in [9]. Note, that PKI services can be offered by the 3GPP or WLAN operator itself or by another third party in the form of a Certification Service Provider (CSP).

Very recent 3GPP specifications documents for UMTS Release 6 [10,11] explore the possibility of deploying PKI and supporting subscribers' certificates by mobile operators. However, 3GPP approach enables certificate issuing only from the Home 3GPP network. In addition, the whole mechanism is based on symmetric key derivation after the user has been authenticated against a bootstrapping server, rather on long term private keys. Finally, the issued certificates can be used to obtain certain services only by the home operator-controlled Network Application Function (NAF).

Normally, before the user can obtain an AC he has to be successfully authenticated by the network. As already stated in the previous section, 3GPP specifications for UMTS Release 6 [1,2,3,12] set the responsibility for access control on the user's 3GPP home network. Following this approach, the AAA proxy relays access control signaling to the user's home 3GPP AAA server (see Figure 1). Consequently, user's authentication is based on EAP-AKA protocol described in [3,13]. EAP is a general protocol for PPP authentication, which can support multiple authentication mechanisms. EAP-AKA provides the way to exchange AKA authentication messages encapsulated within the EAP protocol.

III. Performance Evaluation

A. *Simulation Parameters and set-up*

Performance evaluation of the discussed architecture for large-scale environments was based on simulations where two distinct scenarios were defined and implemented accordingly. In our first scenario, the user's access network is an 802.11b WLAN. The user may obtain access whenever he wishes to and the signal strength allows it, through the network that covers the area where he is located (e.g. through the local Hot Spot). In the second scenario, we examine the case where the access network is a UMTS based network. In both scenarios the user obtains access through a serving network which communicates directly or through other networks with his home network and is responsible to forward his requests.

We can categorize each scenario even further, assuming more than one serving networks are interposed between the user and its home network. Further down, we evaluate the proposed architecture for the following cases:

A. For the first scenario, where the access network is a WLAN, four serving networks are intervening between the user and his home 3GPP network.

B. For the second scenario, where the access network is a UMTS, two serving networks are intervening between the user and his home 3GPP network.

We also specify the following metrics that were considered to be most indicative for the performance evaluation procedure. These metrics are expressed in terms of service times needed for several functions (phases) to be completed and are presented in Table I. We have also defined two additional metrics in order to furnish an overall view of the simulation results. That is, the Application Response Time (ART) which represents the time needed for the whole transaction to complete (execution and delivery of all the messages) and the Ping Time (PT) which is a direct indication of the network connection quality. In the following paragraphs, we present a small description for each of the two scenarios implemented, followed by the simulation results derived and our comments.

TABLE I
METRICS USED FOR PERFORMANCE EVALUATION

	Description
CRTT	Client Request Transmission Time: Elapsed time elapsed from the clients' request transmission until he has received an ACK from the CGW (indication of request reception & validity)
CRRT	Client Request Return Time: Elapsed time from CGW-ACK reception until the client has received the AC
CROT	Client Request Overall Time: Elapsed time from clients' request transmission until he has received the AC and responded with an ACK
GWFT	CGW request Forward Time: Elapsed time since the CGW forwards the request until he has received a CA/AA-ACK (indication of request reception by the CA/AA)
GWOT	CGW Overall Time: Elapsed time since the CGW forwards the request until he receives the AC
AART	Attribute Authority certificate Return Time: Elapsed time since the CA forwards the AC until he receives a CGW-ACK (indication of successful delivery of the AC)

B. ***Scenario I***: *The user connects through a WLAN*

In this scenario, depicted in Figure 2, the user is assumed to be connected to a WLAN-based serving network, via an Access Point (AP). The serving network communicates with the user's home network which is responsible to issue the ACs for the user. More specifically, the UE on behalf of the user sends a request message to the serving network's CGW asking for an AC to be issued from his home 3GPP network. We also assume that until request completion the user remains attached to the same WLAN network. The user's request is forwarded from the local CGW to the home network's CGW and then to the appropriate CA/AA which is responsible to issue the corresponding AC.

The simulation is based on the IEEE 802.11b standard which supports data rates of 1, 2, 5.5, and up to 11 Mbps. The actual data rate varies, depending on many parameters such as the transmission technology, channel frequency, distance from the AP, pathloss and interference, number of devices connected to the AP, etc. We conducted several pre-tests prior to the main simulation, and concluded that the main factors that affect the response time of certificate acquisition, and thus the architecture's overall performance, are the utilization degree of the wired network and the wireless communication quality and speed. Another factor that significantly affects performance is the number of the serving networks interpolated between the user and its home network. According to these factors, the simulation scenarios are based on the following assumptions: first of all, we define three cases based on the utilization percentage of the wired network, that is:

1) An "UnderUtilized" network which is utilized in an average load of 40%.
2) A "Utilized" network which is utilized in an average load of 70%.
3) An "OverUtilized" network which is utilized in an average load of 90%.

For each of the aforementioned cases the simulation scenario is conducted by varying the data rate of the UE, so that all of the four supported data rates (1, 2, 5.5, 11 Mbps) can be evaluated, resulting in twelve different sub-cases for scenario I. Moreover, as far as the number of serving networks affects the overall performance, we considered several different architecture variations focusing on large scale environments. In this paper we present only the situation where four distinct serving networks are impeded between the user and its home network, as shown in Figure 2.

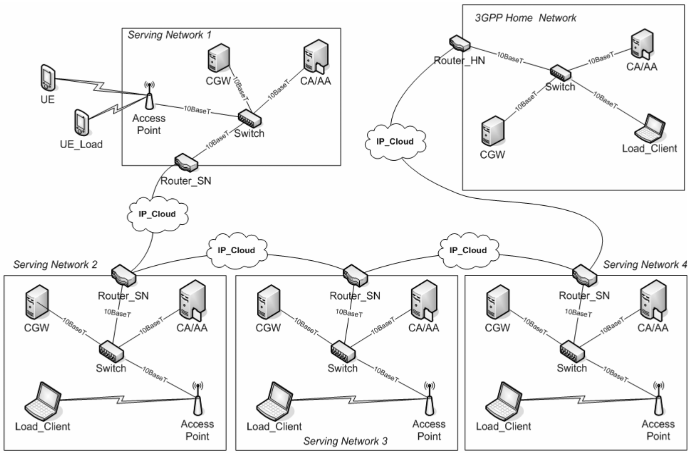

Fig. 2. User connects through a WLAN (where four distinct serving networks are impeded between the user and its home network).

C. *Simulation Set-up for Scenario I*

The AP is connected to the local switch using a 10BaseT connection. The interconnection of the serving networks and the user's home network is achieved via a pair of routers that are connected through a PPP DS3 link. In order to simulate the delay caused by the interconnection of the several networks, we consider a standard ping delay of 80 ms between each network. Both the home and serving networks consist of the following components:

- A CGW, which communicates with the UE, the CA/AA machine and the CGW of the other networks.
- A CA/AA (Certification Authority/Attribute Authority) Server, which accepts the requests from the CGW and is responsible for the creation and issuing of ACs.
- A router, responsible for interconnection and packet routing among the corresponding networks (i.e. the

serving networks in our simulation scenarios).

Moreover, in the WLAN segment, we consider an AP that bridges communication between the wireless and the wired links. Summarizing, the user sends a signed with his private key request to the CGW of the first serving network (the network that is connected to). The request is then forwarded through the CGWs of the four serving networks to the CGW of the user's home network and finally to the CA/AA machine. If everything is in place (e.g. signature validation succeeds) CA/AA shall issue the certificate and sent it back to the user. Figure 3 depicts in detail the message flows between all the involved entities, as well as the times used for performance evaluation. An in depth detail description on request generation and validation procedures can be found in [7,8]. Furthermore, in order to simulate the processing load introduced to the CGW and CA/AA servers by other requests in a real deployment scenario, a client workstation is employed in every network in the chain (see Figure 2) that sends successive AC requests to the CGWs. In addition, we employed a second wireless workstation connected through the same AP, in order to generate IP traffic flows (with transfer rate of 2 Mbps) to the router of the serving network for the whole period the simulation was running.

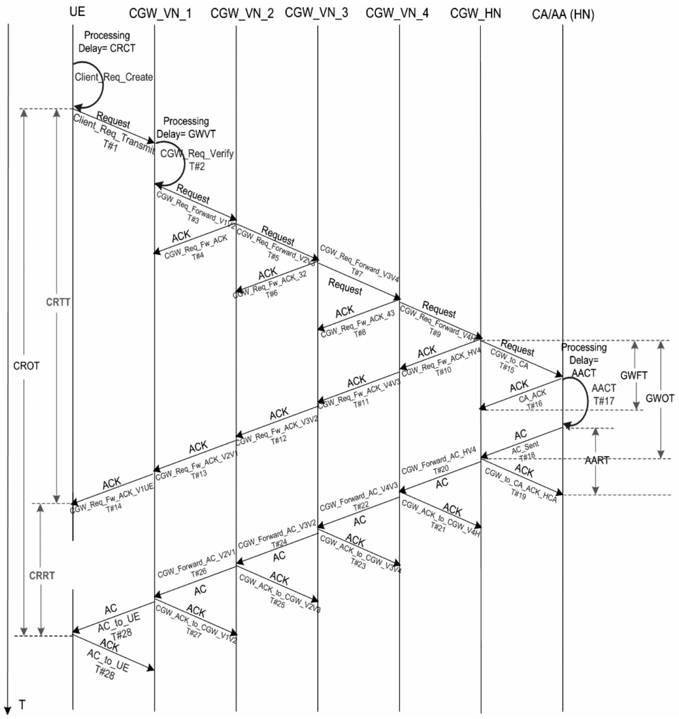

Fig. 3. Message flows between all entities for scenario I

D. *Results for Scenario I*

Table II contains the results recorded during the simulation, containing twelve cases in total, as well as the PT between the UE and the router of the home network. In addition, Figures 4,5,6 demonstrate the probability density function diagrams of the application's response time for the 3 cases of network utilization, that is, UnderUtilized, Utilized and OverUtilized. The depicted diagrams imply that there is a small differentiation of the Application Response Time (ART) per data rate, whereas the best performance is achieved for the higher data rate. We also notice that the ART is considerably affected by the utilization percentage. Finally, we emphasize on the fact that the performance times seem to be strongly dependent on the round trip times between the participating networks.

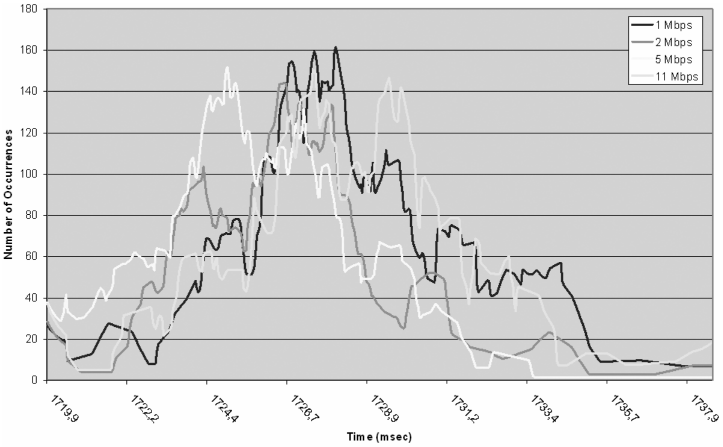

Fig. 4. Probability density function diagram of the ART for "UnderUtilized" network utilization (Scenario I)

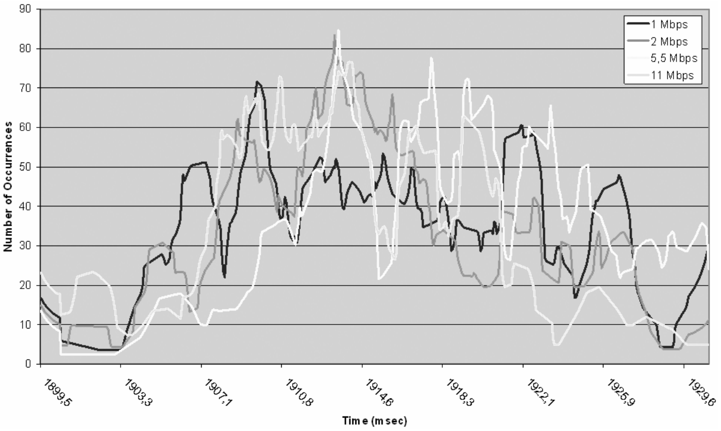

Fig. 5. Probability density function diagram of the ART for "Utilized" network utilization (Scenario I)

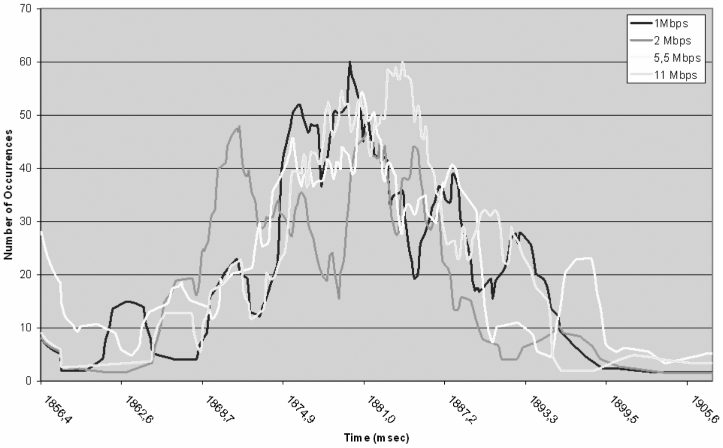

Fig. 6. Probability density function diagram of the ART for "OverUtilized" network utilization (Scenario I)

E. *Scenario II*: *The user connects through a UMTS*

Concerning this scenario, depicted in Figure 7, the user is connected to a UMTS-based 3GPP network, through the UMTS Radio Access Network (UTRAN) access network. One of the most important UMTS features is the ability to support high data rates of up to 2 Mbps for data services. However, the peak data rate of 2 Mbps can only be achieved under special conditions. Therefore, in our evaluation we consider three different cases of data rates, those of 64, 144, and 384 kbps, which are commonly achieved.

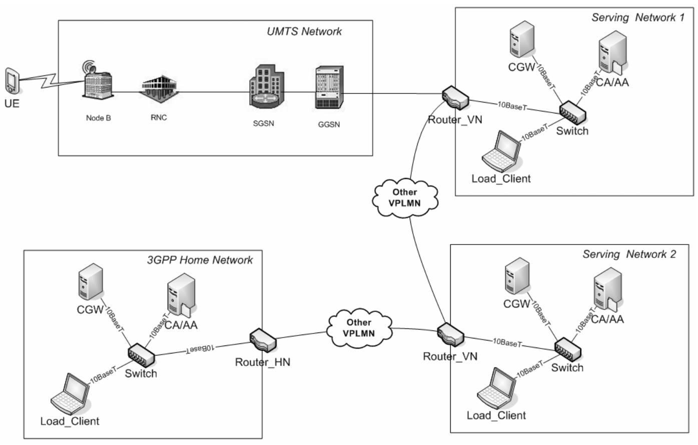

Fig. 7. User connects through a UMTS (where two distinct serving networks are impeded between the user and its home network)

Likewise to scenario I, we conducted several simulation pre-tests coming to the conclusion that the main factors which affect the ART of AC acquisition are the utilization of the wired network as well as the wireless communication quality and speed (data rates). Another factor that affects performance is, obviously, the number of the serving networks interpolated between the user and its home network. According to these factors, the simulation scenarios are based on the following assumptions. We first define two cases based on the utilization percentage of the wired network:

1) A "Utilized" network which operates in an average load of 40% utilization.
2) An "OverUtilized" network which operates in an average load of 80% utilization.

For each of the aforementioned cases of network utilization, the simulation scenario is executed by varying the UE's data rate, (64, 144 & 384 kbps), thus resulting in six different sub-cases for this scenario. In relation to the number of intervened networks, we consider the situation where two serving networks are posed between the user and his home network. Both serving networks consist of two servers, a CGW and a CA/AA server that are connected to a local switch (10BaseT connections). For the communication of this local network with the UMTS Core network, a router is used that is connected via a PPP DS3 link with the GGSN. The interconnection of the serving networks and the home network is also achieved via a pair of routers that are connected through a PPP DS3 link. In order to simulate the delay caused by the interconnection of the several networks, we consider a standard ping delay of 80 ms between each network.

According to this scenario, the user is roaming in the coverage area of a UMTS serving network. The UE is connected to the UMTS-based network through the UTRAN access network. It is implied, that the Packet Data Protocol (PDP) context activation procedure should be performed before the user is able to use the packet service. The UTRAN network is consisted of the Node B and the Radio Network Controller (RNC) which are connected through an ATM OC3 link. The UMTS Core Network is consisted of the SGSN and the GGSN which are connected though a PPP DS3 link. The SGSN is also connected with the RNC with an ATM OC3 link.

In this context, the user sends a request, signed with his private key, to the CGW of the serving network that is connected to. The request arrives at the GGSN, through the local CGW, and then is forwarded to the CGW of the first serving network. Hereupon, the request is forwarded through the CGW of the second serving network to the CGW of the home network and then to the CA/AA machine, in order to have the AC issued. Detailed description of the messages exchanged between the participating entities, as well as the times measured is depicted in Figure 8. In order to simulate the load introduced to the CGW and CA/AA servers by other certificate requests in a real deployment scenario, an additional client workstation has been used in every network generating successive ACs requests.

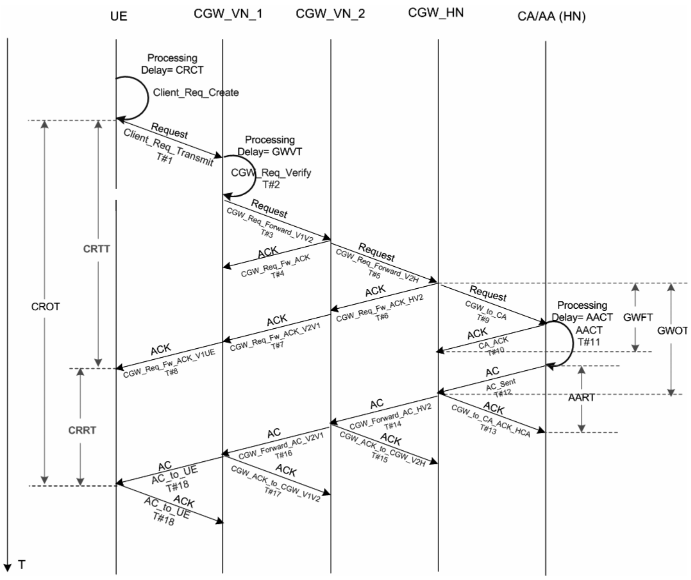

Fig. 8. Message flows between all entities for scenario II

F. *Results for Scenario II*

The simulation results logged are summarized in Table III. This table contains the PT calculated between the UE and the router of the home network as well as all the results generated by the simulation of this scenario (six cases in total). Furthermore, Figure 9 demonstrates the probability density function diagram of the ART for the two cases of network utilization, that is, Utilized and OverUtilized. As we easily notice, there is a considerable differentiation in the Application Response Time (ART) per data rate. As it is expected, the best performance is achieved when the data rate of 384 kbps is used along with UnderUtilized scheme. The second best performance is achieved for the higher data rate but for the highest network utilization, whereas the lowest measured performance corresponds to the case of the lowest data rate of 64 kbps and OverUtilized scheme. It is also clear, that the differentiation becomes comparatively smaller considering the cases of a high utilization percentage and a high data rate with the case of a low utilization percentage and a lower data rate (384 kbps OverUtilized with 144 kbps Utilized and 144 kbps OverUtilized with 64 kbps Utilized). Finally, performance times seem to be strongly dependent on the round trip times between the participating networks.

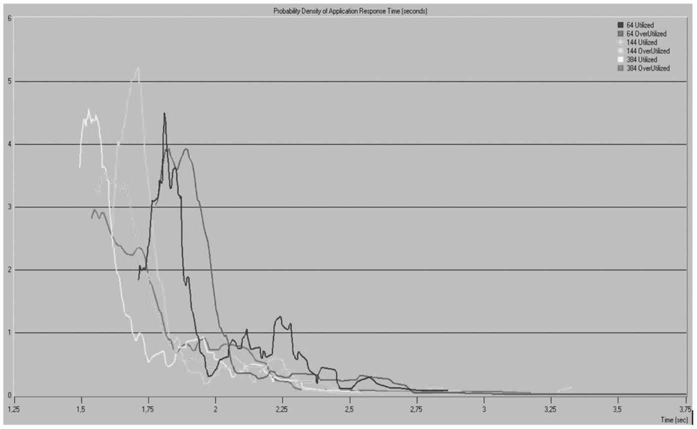

Fig. 9. Probability density function diagram of the ART for the two cases of network utilization (Scenario II)

IV. CONCLUSIONS AND FUTURE WORK

Public Key Infrastructure, to support digital certificate provision, is about to be incorporated to 3G-and-beyond mobile networks. In this paper, we simulated digital certificate acquisition, focusing on performance evaluation issues and targeting to large scale deployment scenarios. The proposed architecture, originally introduced in [7,8], enables on-the-fly, on-demand certificate generation and deliverance and achieves maximum compatibility with current 3GPP interworking specifications. Through the implementation of two subsequent simulation scenarios, based on the access network technology used, we demonstrated that ACs issuing is satisfactory in terms of service time for both mobile operators and users. More importantly, the derived times prove that our solution can be readily scaled to support digital certificate provision through large heterogeneous network deployments thus fulfilling the vision of the forthcoming 4G networks. However, the proposed architecture and certification procedure has to be further evaluated in terms of security strength and robustness. Another important topic, in common with roaming agreements, is the trust issues between the CA/AAs operated by or collaborating with 3GPP or WLAN providers and end service providers.

REFERENCES

[1] 3GPP Technical Specification, *3GPP System to WLAN Interworking; System description*, TS 23.234 v.6.1.0, June 2004.

[2] 3GPP Technical Specification, *3GPP System to WLAN Interworking; UE to Network protocols*, TS 24.234 v.1.5.0, July 2004.

[3] 3GPP Technical Specification, *3GPP System to WLAN Interworking Security,* TS 33.234 v.6.1.0, June 2004.

[4] S. Farrell, R. Housley, An Internet Attribute Certificate Profile for Authorization, IETF RFC 3281, April 2002.

[5] R. Oppliger, G. Pernul, C. Strauss, “Using Attribute Certificates to Implement Role-based Authorization and Access Control Models”, SIS 2000, Zurich, Switcherland, pp. 169-184, 2000.

[6] D.F. Ferraiolo, J.A. Cugini and R.D. Kuhn, Role-Based Access Control (RBAC): Features and Motivations (http://hissa.ncsl.nist.gov/rbac/newpaper/rbac.html, 1995.

[7] Kambourakis G., “3G network security with PKI services”, PhD thesis dissertation, University of the Aegean, 2004.

[8] Kambourakis G., Rouskas A., Gritzalis S., "Delivering Attribute Certificates over GPRS", in the Proceedings of the 19th ACM Symposium on Applied Computing (SAC) – Mobile Computing and Applications Track, pp. 1166-1170, May 2004, Nicosia, Cyprus, ACM Press.

[9] 3GPP Technical Specification, *IP Network Layer Security*, TS 33.210 v.6.5.0, June 2004.

[10] 3GPP Technical Specification, *Generic Authentication Architecture (GAA); Support for subscriber certificates*, TS 33.221 v.6.0.0, March 2004.

[11] 3GPP Technical Specification, *Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description*, TS ab.cde v.0.3.0, Sept. 2003.

[12] G. Koien and T. Haslestad, “Security Aspects of 3G-WLAN interworking”, *IEEE Communications Magazine,* vol 41, no. 11, pp. 82-88, Nov. 2003.

[13] 3GPP Technical Specification, *MAP Application Layer Security;*, TS 33.200 v.5.1.0, Dec 2002.

TABLE II
SIMULATION RESULTS FOR SCENARIO I (**802.11**)

	DATA RATE (MBPS)	CRTT (ms)	CRRT (ms)	CROT (ms)	GWFT (ms)	GWOT (ms)	AART (ms)	ART (ms)	ART St. Deviation	Ping Time (ms)
UnderUtilized	1	1054.94	92.08	1147.02	7.20	74.78	7.58	1735.70	0.0035	324
	2	1050.55	92.74	1143.29	7.21	74.99	7.60	1732.06	0.0042	325
	5.5	1003.00	92.50	1095.50	7.22	75.16	7.61	1729.08	0.0035	323
	11	1047.23	92.60	1139.83	7.06	75.27	7.56	1728.58	0.0036	323
Utilized	1	1173.57	110.90	1284.47	19.00	87.00	19.32	1931.30	0.0071	328
	2	1167.10	102.78	1269.87	18.78	86.00	19.63	1916.62	0.0068	327
	5.5	1162.97	104.79	1267.75	18.78	86.74	19.42	1914.00	0.0064	327
	11	1163.63	104.32	1267.95	18.61	87.24	19.91	1914.06	0.0066	327
OverUtilized	1	1167.83	94.74	1262.57	7.15	74.70	7.64	1891.19	0.0097	336
	2	1136.81	96.84	1233.65	7.32	74.85	7.61	1886.93	0.0109	332
	5.5	1159.23	95.68	1254.91	7.09	74.87	7.69	1882.93	0.0106	332
	11	1159.08	95.03	1254.10	7.14	74.49	7.65	1882.16	0.0093	331

TABLE III
SIMULATION RESULTS FOR SCENARIO II (**UMTS**)

	DATA RATE (KBPS)	CRTT (ms)	CRRT (ms)	CROT (ms)	GWFT (ms)	GWOT (ms)	AART (ms)	ART (ms)	ART St. Deviation	Ping Time (ms)
Utilized	64	1486.59	256.28	1742.86	4.68	68.92	5.03	1992.49	0.256	755
	144	1382.38	201.30	1583.67	4.61	69.07	4.97	1834.93	0.404	755
	384	1381.61	119.40	1501.01	4.60	69.04	5.00	1750.46	0.302	755
OverUtilized	64	1521.52	259.48	1781.00	14.69	79.08	15.44	2049.16	0.424	727
	144	1439.66	143.40	1583.06	14.45	78.60	14.62	1854.74	0.322	727
	384	1489.64	165.29	1654.92	14.24	78.61	14.97	1921.96	0.639	727