Performance Evaluation of Certificate Based Authentication in Integrated Emerging 3G and Wi-Fi Networks

Georgios Kambourakis[1], Angelos Rouskas[1], and Dimitris Gritzalis[2]

[1]Department of Information and Communication Systems Engineering,
University of the Aegean, Samos 83200, Greece
{gkamb, arouskas}@aegean.gr
[2]Department of Informatics,
Athens University of Economics and Business,
76 Patission St., Athens GR-10434, Greece
dgrit@aueb.gr

Abstract. Certificate based authentication of parties provides a powerful means for verifying claimed identities, avoiding the necessity of distributing shared secrets beforehand. 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 and evaluates the potential application of enhanced TLS-based authentication mechanisms in integrated emerging-3G and Wi-Fi networks. We propose to use EAP-TLS protocol seconded by Public Key Infrastructure entities, to provide users with robust authentication mechanisms in hybrid WLAN-3G heterogeneous environment. Our alternative solution is discussed against EAP-AKA procedures as they appear in the latest 3G and integrated 3G/Wi-Fi specifications. Finally, the proposed mechanism is evaluated through a properly designed experimental test bed setup. *Keywords*: AKA; EAP; TLS; PKI; UMTS; WLAN.

1 Introduction

According to beyond-3G (B3G) vision, an IP backbone will constitute the core network for all heterogeneous wireless technologies and secure communication provision like confidentiality, access control and entity authentication, will become one of the major goals of these systems. Thus, certificate based authentication is attractive to support roaming in future mobile communications. Furthermore, the concept of digital signatures, that requires the usage of certificates, allows the introduction of complex many-to-many business models.

Recent works indicate that both a performance efficient implementation of TLS protocol for handheld devices is feasible [1] and secure, flexible and reconfigurable Authentication and Key Agreement (AKA) procedures for beyond 3G wireless communication networks can be implemented [2].

S.K. Katsikas et al. (Eds.): EuroPKI 2004, LNCS 3093, pp. 287-296, 2004.

The paper discusses the application of 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 Wi-Fi hot spots administrated by different WLAN operators. From a technical aspect, this application requires that all Wi-Fi networking settings are *loosely* or *tightly* incorporated [3] 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: Taking into consideration Third Generation Partnership Project (3GPP)'s proposals and specifications 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. Sections 3, 4 and 5 analyze and evaluate an AKA mechanism based on EAP-TLS, which can be applied into Wi-Fi settings and the paper is concluded in Section 6.

2 Wi-Fi Networks and 3G Infrastructures Integration

Emerging or B3G 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. The anticipated provision of many *uncoordinated* Wi-Fi picocells where coverage is limited e.g. within buildings, 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 B3G TLS 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. A WLAN 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 Universal Mobile Telecommunications System (UMTS) Release 6[4], describe an interworking architecture (Figure 1) where the home network is responsible for access control, while 3GPP proxy AAA relays access control signalling to the Home 3GPP AAA server. UMTS-SIM (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 [4, 5]. EAP is a general protocol for PPP authentication, which can sup-

port multiple authentication mechanisms. Consequently, EAP-AKA provides a way to exchange AKA authentication messages encapsulated within the EAP protocol.

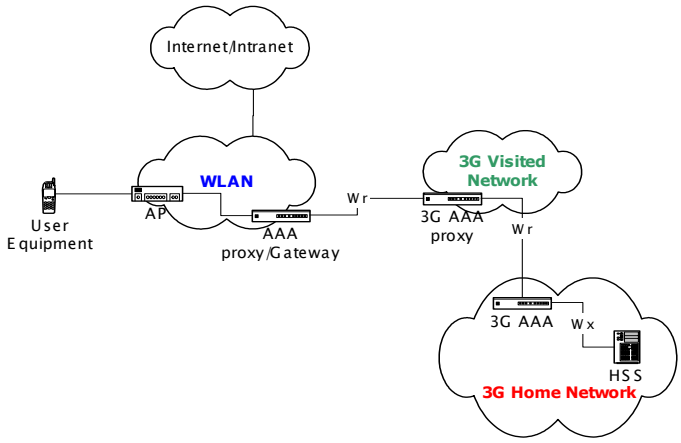

Fig. 1. Wi-Fi integration in UMTS concept

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. 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 [6, 7].

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 TLS, we can take advantage of the protected and flexible ciphersuite negotiation, mutual certificate based authentication and scalable key management capabilities, in order to provide strong authentication and end-to-end security to the user of this heterogeneous architecture.

Moreover, although several known weaknesses in GSM AKA seem to be now fixed in UMTS, there are still some inefficiencies which affect the EAP-AKA authentication mechanism too. For a detailed breakdown of 3G-AKA and EAP-AKA shortcomings refer to [2, 9, 10, 11] & [5] respectively.

3 EAP-TLS and PKI 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 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], 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 on PKI and 3G integration requirements can be found in [2, 13, 16, 17, 18].

Performance considerations have held from using 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 TLS protocol. A recent study has also shown the feasibility of TLS in handheld wireless devices [1], while relevant work showed that SSL's handshake protocol time can be improved up to 5.7X times [19].

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.

4 An AKA Mechanism Based on EAP-TLS

Motivated by the aforementioned technological trends, we propose an alternative AKA procedure based on EAP-TLS, instead of EAP-AKA, for integrated 3G/Wi-Fi

networks. Figure 2, depicts the exchange of 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 appropriate 3G AAA server is chosen based on the NAI. Note, that since the client claimed 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 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). For a detailed pure EAP-TLS protocol explanation, refer to [12].

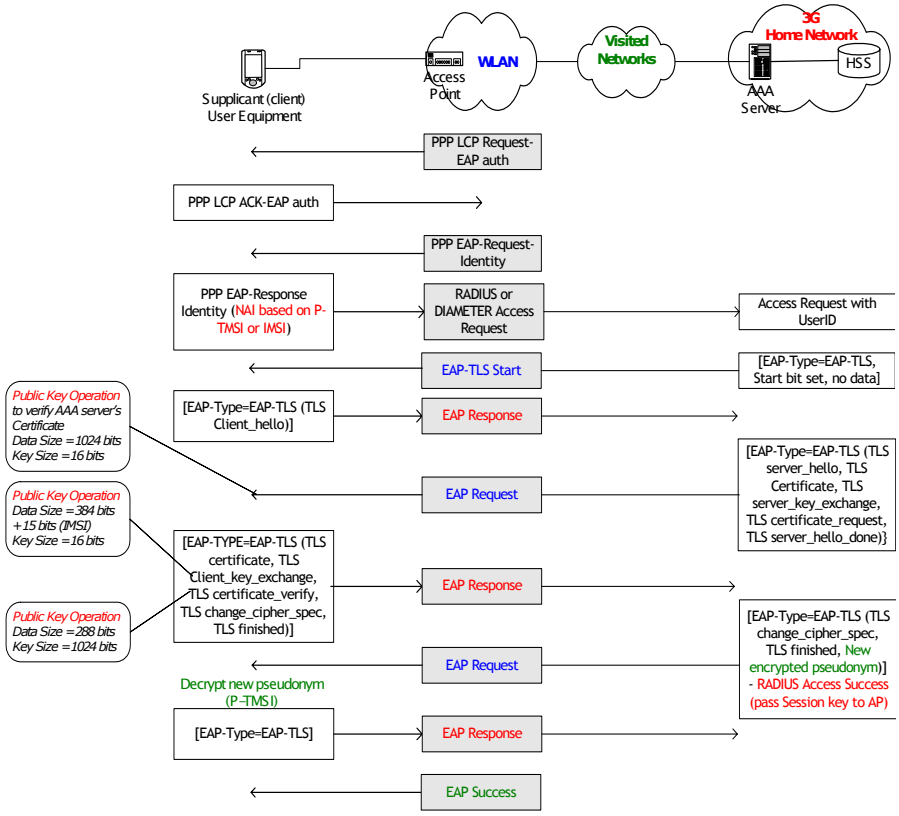

Fig. 2. AKA Mechanism based on EAP-TLS

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

- 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.

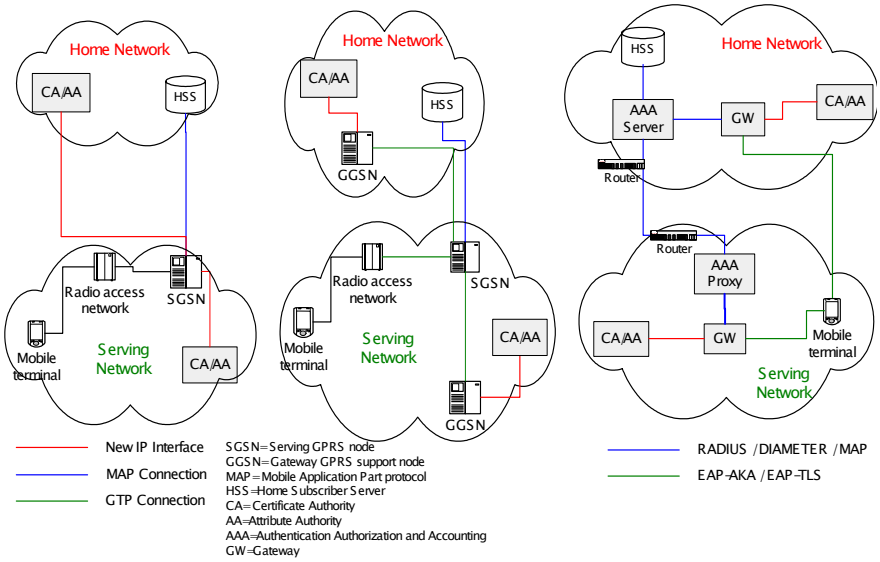

Fig. 3. 3G Architectures to support PKI

- 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 TLS option for session resumption. The purpose of sessionID included in supplicant hello, 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 or should be resumed or not. Recent studies also showed that session reuse could be further improved, using a TLS session aware dispatcher, when the operator is planning to install a cluster of TLS authentication servers [20].

- 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 [21].
- There is no need for HSS 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.

5 EAP-TLS Service Time Evaluation

5.1 Test Bed Setup

In order to evaluate the performance of EAP-TLS AKA mechanism in terms of service times, we constructed experimental hardware architecture. The development and test model topology is illustrated in Figure 4. The presumed mobile device is a low-end laptop machine that uses Windows XP Home edition operating system. The supplicant incorporates a Pentium II 400MHz CPU and has 80 MB of RAM available. At the other end, the RADIUS server machine has a Pentium 4 1.4 MHz processor and 128 MB RAM, running Linux Slackware 9.1 operating system. To implement RADIUS server functionality we used the well known open-source package Freeradious in version 0.9.3.

The client is connected to the network using an 802.11g wireless PCMCIA card and an 802.11g AP. The RADIUS server and the AP reside to different networks, acting as the Visited (foreign) and Home networks for the client. The average ping time between the two networks, measured with a ping tool was about 120 msec. Another laptop machine which is connected to the same network with the RADIUS server, generates a large number of EAP-TLS requests to virtually load the server. The times between successive EAP-TLS authentication requests follow the negative exponential distribution. Finally, the necessary for our experiments certificates, was constructed using the well known Apache style license OpenSSL toolkit in version 0.9.7c.

The handshake and authentication procedures are mutual, meaning that both the supplicant and the RADIUS server exchange their certificates, which are kept locally along with the corresponding trusted CAs public keys list. We used a depth-two certificate chain schema in order to weigh up a serving or visited network authentication schema. Both parties check certificates validity, against time expiration and issuing CA (trust anchor). Neither party check certificates validity against any revocation list.

Only the RADIUS server is bound to do so by checking against supplicant's P-TMSI (mapping it to the correct IMSI).

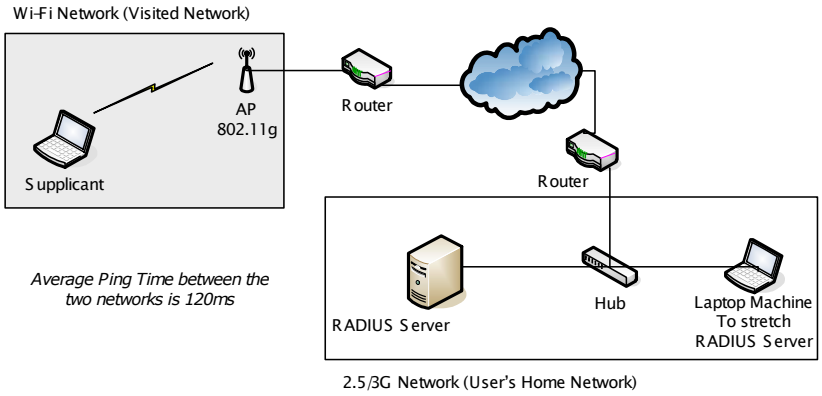

Fig. 4. Test bed Topology

5.2 Measurements Results

We run our experiments with various values of the request arrival rate λ (transactions per second) for the process which adds virtual load to the server. We gathered 1000 measurements from an equal number of transactions initiated by the supplicant, using the popular network analyzer Ethereal in version 0.10.0 and RADIUS server log files. The average initialization time for the supplicant was 0.062 sec. We present the corresponding average total EAP-TLS authentication service time values in seconds for different scenarios we tested, in Table 1 and Figure 5.

Table 1. Average Total EAP-TLS Service Times in Seconds

Virtual Load (λ)	AP in the same room with supplicant	Supplicant outside the building
1	4.468	4.575
4	4.524	4.604
5	4.694	4.625
8	4.737	4.695
10	4.897	4.753
20	4.917	4.959
25	5.036	5.045
50	5.761	5.912
Average Time	4.879	4.896

An average time below 5 sec, as it appears in Table 1, is certainly an acceptable authentication time duration for the users of a mobile B3G device, since a real 2.5G standard AKA mechanism, assuming that someone activates his device in a roaming, network, takes about 4 – 7 sec to complete. Nevertheless, EAP-TLS authentication

time is expected to grow according to the Home and Serving networks 'distance'. The greater the distance measured in ping times is, the greater the EAP-TLS authentication time is expected to be. This is mainly due to TLS protocol round-trips. Moreover, during the TLS handshake the server must wait for a client message and vise versa. Thus, it is often computationally cheaper and network faster (considering round-trip times) to generate a number of TLS messages and transmit then all at once [22].

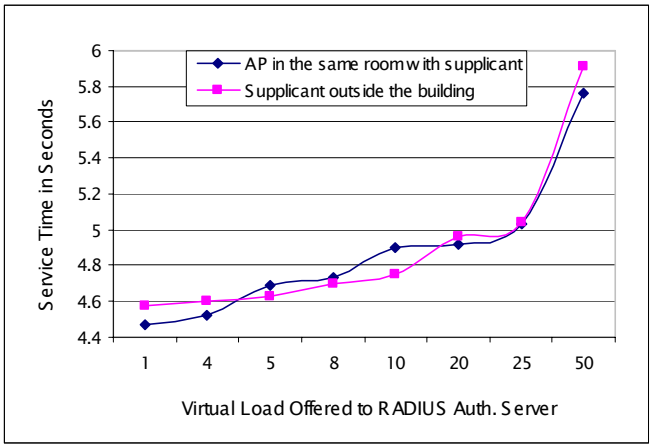

Fig. 5. EAP-TLS Service Times

It is also obvious, that the distance between the AP and the supplicant has a negligible affect on EAP-TLS authentication time. We discovered that this is true as long as the signal quality remain above 55 – 60%. Furthermore, the size of the certificates and its depth, not only decelerates the certificate verification process in each party, but also at the same time adds several extra bytes to the relevant handshake messages. Finally, an extra delay is expected if the RADIUS server is located remotely to user's Home network HSS. In that case, the RADIUS server has to communicate with the subsequent HSS in order to fetch user's credentials and successfully authenticate the user.

6 Conclusions

With the ongoing development in the area of mobile communication technologies we are approaching the 'all-IP' 4G vision step by step. In this paper 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 argued on the application of EAP-TLS in contrast to EAP-AKA based authentication mechanisms into integrated 3G and Wi-Fi networks. Through experimentation we discovered that EAP-TLS authentication is attainable in terms of service times. 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. Topics to be further investigated include evaluation scenarios with Pocket PC machines, certificate-depths above two and RADIUS – HSS communication.

Acknowledgments
We would like to thank Mr. Lizos Konstantinos for providing us with the network measurements.

7 References

1. 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.
2. 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.
3. Salkintzis, A., Fors, C. & Pazhyannur, R., "WLAN-GPRS Integration for Next-Generation Mobile Data Networks", IEEE Wireless Communications Magazine, pp. 112-124, Oct 2002.
4. 3GPP Technical Specification, WLAN Interworking Security, (TS 33.cde v0.1.0), July 2002.
5. Arkko, J. and Haverinen, H., "EAP-AKA Authentication", <draft-arkko-pppext-eap-aka - 11.txt>, Oct. 2003.
6. M. Gast, "*802.11 Wireless Networks: The Definitive Guide*", O'Reilly, April 2002.
7. D. Eaton, "Diving into the 802.11i Spec: A Tutorial". Feb 2003, electronically available in http://www.commsdesign.com/design_corner/OEG20021126S0003.
8. 3GPP Technical Specs, A guide to 3rd Generation Security, (TR 33.900 v.1.2.0), Jan. 2000.
9. Aamodt, T., Friiso, T., Koien, G., "Security in UMTS–Integrity", Telenor R&D, Feb. 2001.
10. Niemi, V. & Nyberg. K., *UMTS Security*, Wiley, 2003.
11. 3GPP Technical Specs, 3G Security Architecture, TS 33.102 v.5.1.0), December 2002.
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, www.esat.kuleuven.ac.be /cosic/aspect, 1999.
15. USECA Project, UMTS Security Architecture: Intermediate 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. 3GPP TSG, "Using PKI to provide network domain security", Discussion Document (S3-010622 SA WG3 Security – S3#15bis), Nov. 2000.
18. 3GPP Technical Specs, Bootstrapping of application security using AKA and Support of Subscriber Certificates; System Description, (TS ab.cde v.3.0), Sep. 2003.
19. 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.
20. Apostolopoulos, G. et al., Securing Electronic Commerce: Reducing the SSL Overhead, IEEE Network Magazine, no 4, pp. 8-16, July/August 2000.
21. 3GPP TSG, "Support of certificates in 3GPP security Architecture", Discussion Document S3-010353 SA WG3 Security – S3#19, July 2001.
22. Rescorla, E., SSL and TLS Designing and Building Secure Systems, Addison-Wesley, 2001