# Untraceable Identity Management Framework for Mobile Access

Min-Chih Kao*, Yi-Shiung Yeh * , and Chuan-Chi Wang **

*Department of Computer Science and Information Engineering
National Chiao-Tung University
1001 Ta-Hsueh Road, Hsinchu, Taiwan 30050, ROC.
Tel: 886-3-5731813, Fax: 886-3-5724176
E-mail: (gau.csie91g, ysyeh)@csie.nctu.edu.tw
** Department of Computer Science and Information Engineering
Ching-Yun University
229 Chiao-Hsin Road, Jung-Li, Taiwan 320, ROC
E-mail: wcc@cyu.edu.tw

## Abstract

Although some Extensible Authentication Protocol (EAP) methods such as EAP-TTLS (Tunneled Transport Layer Security) can hide true identity to protect the privacy of the mobile user, they cannot identify the mobile user for accounting and authorization purposes. The EAP framework lacks a mechanism to manage the relationship between true identities and pseudo identities. This study proposes an identity management framework based on the short-lived certificate so that the proposed scheme can deal with both authentication and authorization with privacy. The proposed scheme has no need of a certificate revoke scheme in which the authentication process can only occur between the mobile user and an authenticator. This greatly reduces the authentication delay. Thus, the proposed scheme can achieve both privacy and efficiency.

***Key words:***

*Extensible authentication protocol (EAP), Short-lived certificate, Privacy*

## 1. Introduction

An administrative domain is an autonomous network infrastructure served by the same AAA (Authentication Authorization Accounting) server [6]. Due to the growth of wireless access technologies, users have more opportunities to roam across different networks and administrative domains. This implies that an authentication framework designed for multiple AAAs is needed. For this, the IETF (Internet Engineering Task Force) suggests a three-party (***the user, authenticator, and AAA***) EAP (Extensible Authentication Protocol) framework that can extend to multiple AAAs scenarios [1]. The EAP framework supports multiple authentication methods and allows the authenticator to simply pass the authentication negotiation exchanges of the user to the backend AAA. Some authentication methods, such as EAP-TLS (Transport Layer Security) [2]or EAP-TTLS (Tunneled Transport Layer Security)[7], allow a roaming user to use pseudo identities in untrusted environments. In these methods, the pseudo identity is sufficient to establish secure tunnels (TLS record layer) between the user and the home AAA to carry authentication negotiation messages without exposing sensitive material such as the user's true identities to the visited network. However, these methods are insufficient to identify the user for authorization and accounting purposes. This is because that the provider of the visited or host network needs a surrogate identity in order to bill the home network for the usage. Furthermore, the intermediate networks need the surrogate identity to determine usage privileges such as the number of simultaneous sessions for the user's traffic. Hence, when the user's real identity and location are concerns, the standard RFC 4372 introduces a specific billable identity called Chargeable-User-Identity (CUI), used to refer to the user on the home network. However, there are a number of problems with CUI [3, 15].

- The CUI is assigned by home networks and represents the user. The assignment must be temporary since the CUI may still be used to identify the user, if it is used for a long period.
- Only the home network knows how to bind a CUI to a real identity uniquely.
- The CUI must be transmitted in plaintext form, especially when authentication methods EAP-TTLS and EAP-PEAP (Protected Extensible Authentication Protocol) [21] are used.

This study proposes an identity management framework for solving these problems based on the short-lived certificate introduced in Wireless Public Key Infrastructure[16]. First, the framework uses the short-lived certificate for carrying a temporary chargeable identity such as the CUI to meet the

978-0-7695-3382-7/08 $25.00 © 2008 IEEE
DOI 10.1109/ISDA.2008.248

temporary requirement of RFC 4372 and prevent the risk of identity fraud. Second, the lifetime of the short-lived certificate can be short enough to negate the need for a certificate revocation scheme in the proposed framework [9, 16]. Third, the framework uses an authentication mechanism that does not need an on-line check between visited network and home network. Note that the authentication mechanism can be a fast authentication method for handovers between administrative domains. In fact, many schemes were proposed for this [5, 18, 19, 20, 22, 23, 24]. However, these schemes can not solve both privacy and accounting problems. Finally, a non-repudiation billing mechanism, which can be off-line, for multiple- domain scenarios is used.

The rest of this paper is organized as follows: in section 2, short-lived certificate frameworks, and some issues of EAP authentication methods are discussed. More detail on motivation, assumptions, and proposed schemes are described in section 3. Analysis of the proposed scheme and a comparison with existing solutions are given in section 4. Finally, the conclusion speaks to the matter of future work.

## 2. Requirements and Related Work

### A. The EAP authentication framework

EAP is a Point-to-Point protocol mainly used to provide multiple authentication methods for remote login where IP messaging is not available. The 802.1x [11] defines the EAPOL (EAP over LAN) to encapsulate EAP messages inside IEEE 802 LANs like Ethernet or 802.11 frames and to support a three-party (*the mobile user, authenticator, and AAA*) authentication model.

Intra-domain roaming occurs when a mobile user moves across two authenticators which are dominated by the same backend AAA. By contrast, inter-domain roaming means that a mobile user moves across two authenticators which belong to different backend AAAs. When privacy is concerned for both inter- and intra-domain roaming, the user can use an anonymous identity to perform the procedure of some authentication methods such as EAP-TLS or EAP-TTLS. How the methods work is depicted in Figure 1.

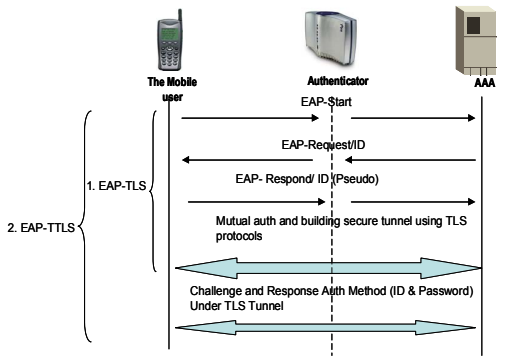


Figure 1 The TLS and TTLS protocols

However, as already pointed out, this protocol is not sufficient for authorization and accounting. The visited and intermediate networks need the user identity for distinguishing how to charge and serve the user but the true user identity cannot be revealed to these entities for security reasons. Hence the standard RFC 4372 introduces the CUI used to solve the problem. However, a number of problems remain, as mentioned in section I. The industry needs an identity management framework that satisfies the following requirements:

- Issues a temporary identity representing the user but the temporary identity does not reveal the true identity.
- The temporary identity is not used for a long period of time so it cannot be used to determine the true identify of the user.
- The temporary identity is protected to prevent the risk of identity fraud.
- The framework supports a non-repudiation billing mechanism.

In additional to the privacy problem, the authentication delay is also an issue when real-time services such as VoIP or multimedia are provided especially for inter-domain users. Backbone communication delay is difficult to control when AAA servers are located far away and the current EAP standard lacks a scalable identity management framework. Researchers engaged in a wave of research and produced many papers on this topic. We can roughly categorize these papers into two types:

### A.1 Pre-authentication

In order to reduce delay during roaming, IEEE 802.11i [12] allows the mobile user to authenticate with multiple authenticators simultaneously. This results in high signaling overhead and engaging the resources of authentication servers and the mobile user. Many schemes were proposed for this [5, 18, 19, 20, 22, 23, 24]. In [19], the authors use a predictive scheme such as Frequent Handoff Region (FHR) for predicting how a set of adjacent authenticators will be involved and minimizing the authentication message flow. Furthermore, the authors of [24] still proposed an inter-domain authentication scheme based on a symmetric key (called a Roaming key, RK) that can greatly reduce the authentication delay. They assume two domains having a direct roaming agreement share a set of RKs. Before the user can roam, the authenticators must get the RK from a secure place like the AAA server to authenticate the user. Although they suggest that the RKs can be stored in authenticators directly, this is not suitable for two domains, especially ones with different security-level such as WLAN-3G or WLAN-WiMAX (It may depend on whether the network management is thoroughgoing or not). This is because that the WLAN operator may not have a mature mechanism to manage their

authenticators (i.e. access points). Furthermore, the authors of [24] assumed that the WLAN operator may over bill the mobile user or claim usage fraudulently. Scalability issues may occur in the RK based scheme [22] as the number of involved parties and users grows. In addition, their scheme lacks for a suitable accounting trigger-signal. In an original AAA [6] framework, authenticators start an accounting process after receiving the accept-message (i.e. EAP-Success) from the home AAA. This implies that the accounting trigger-signal is the accept-message. However, the RK based authentication process only occurs between the mobile user and authenticators in order to eliminate the delay caused by backbone communication. The visited network informs the home network without any warrant generated by the mobile user. Hence, there may be accounting risk in the inter-domain authentication scheme of [22] when the home network provider and the visited network provider do not have a direct business agreement.

**A.2 Proactive Key Distribution**

In order to reduce the delay of re-authentication, proactive key distribution pre-distributes key materials to a set of neighbor authenticators in a neighbor graph (NG) developed in [26]. It works within a single domain, but is not appropriate for inter-domain use since that it skips the direct authentication between the mobile user and any new visited network. Thus, the new visited network cannot re-check the identity of the mobile user for authorization or accounting purposes.

From the above discussion, two requirements for a better identity management framework are added.

- The credential management mechanism must be scalable.
- The identity management framework cannot increase inter-domain authentication delay when real-time services are provided.

**B. X.509 certificates and WTLS certificates**

In [9], not only the X.509 certificate format is defined, but also an authentication framework based on the X.509 certificate is suggested. The X.509 certificate binds a user to a key pair (public/private keys) so that the communication parties can authenticate each other without sharing any secure information in advance. Under the X.509 framework, a user applies for a certificate from a Certificate Authority (CA) for authentication purposes. Usually, a certificate has a validity period ranging from 1 to 2 years. Such certificates are called long-lived certificates. Due to their long lifetime, the key pair may be compromised or lost. Therefore, certificate revocation schemes are necessary during the validity period of the long-lived certificates. Generally, a CA periodically issues a certificate revocation list (CRL) so a concerned party can download it or go on-line to check a participant's status [13, 14]. The CRL is a time-stamped record containing the serial number for all revoked certificates. CRLs become large over time. Such a certificate revocation scheme will greatly add cost and complexity to mobile applications.

By contrast to long-lived certificate, the Open Mobile Alliance (OMA) [9, 16] defined a Wireless Transport Layer Security (WTLS) certificate as a short-lived certificate for mobile devices such as mobile phones or PDAs. Their major purposes are:

- Avoid the burden of reliable CRL download and storage.
- Use light encoding methods to avoid additional computation requirements.

The difference between the WTLS and the X.509 certificate is depicted in Figure 2.

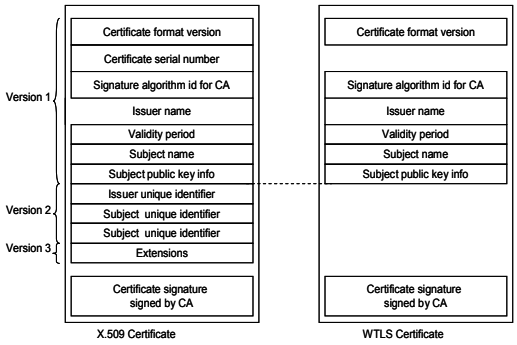


Figure 2 X.509 and WTLS Certificates

The scheme this paper proposes uses the X.509 certificate (used as a long-lived certificate), which contains the true identity, to authenticate a mobile user and then uses the WTLS certificate (used as a short-lived certificate), which contains the chargeable temporary identity, as a short-lived token for wireless networks access. Consider a scenario in which a mobile user uses a long-lived certificate to apply for a short-lived certificate from home or the office and then he/she uses the short-lived certificate for network access when visiting wireless network. Such a flexible scheme can indeed achieve both privacy and efficiency.

**C. Short-lived certificate framework**

In [10], the authors introduced a short-lived certificate framework that includes three servers: a Registration Directory Server, a Registration Authority Server, and a Certificate Server. A new user gets his/her short-lived certificate by means of the following steps:

1. The user gives his/her identifying information to the Registration Authority Server.
2. The Registration Authority Server verifies the authenticity of the user. If authenticated, the Registration Authority Server creates a record in

the Registration Directory Server. The record includes all credential information required in a certificate.

3. After this registration process, the Registration Authority Server issues a share secret such as a password and/or a smart card and sends it to the user by some other means.
4. The user then applies for a short-lived certificate from the Certificate Server using the credential provided by the Registration Authority Server.

They also claim that a certificate based access control mechanism has the following advantages:

- A certificate revocation scheme is not necessary.
- The user can use the shorter key length to improve performance.

However, their registration framework seems not to be suitable for Internet applications. Since the Registration Directory Server records all credentials not suit for distributing to a third party, it may be a bottleneck in their framework. The framework proposed by this paper uses the long-lived certificate to identify a user when the user wants to apply for a short-lived certificate. The benefit this provides is that the revocation scheme of the long-lived certificate can be distributed under X.509 framework [9, 13, 14] and all user credentials, except for a private key, are recorded in the long-lived certificate.

## 3. Identity Management Framework

An identity management framework is proposed in this paper that can meet the requirements mentioned above.

### A. System Assumptions

Assume a mobile user roams across two different networks (from the home network to a visited network). The mobile user is equipped with a long-lived certificate (with a public/private key pair) that is issued by a CA. The long-lived certificate is used to authenticate the mobile user under the X.509 framework suggested in certificate-relative standards such as X.509 [9]. When the mobile user is authenticated, he/she can get a short-lived certificate as a token from an Identity Management Server (IMS) for network access. The short-lived certificate contains the temporary identity issued by the IMS. The IMS must guarantee two things during the validity period of the short-lived certificate. First, the visited network operator can use the identity to bill the mobile user and for knowing how to serve the mobile user. Second, the identity cannot be used by others to identify the user. At the same time assume that the visit network operator uses short-lived certificates to avoid burden of downloading reliable CRL for devices like mobile phones or PDAs.

In addition to the above certificates, the root certificate of a CA is still needed to establish the trust relation between any two entities. This is due to the fact that digital signature verification includes two steps: the entity first validates the root certificate of the certificate issuing CA from a list of root certificates in local storage (called a CA trust list), and then verifies the signature value using the public key of the certificate issued by the CA. Hence, one must also assume that each entity maintains a CA trust list *in loco*.

### B. Identity Management Server

The IMS has two functions. First, it is responsible for issuing a short-lived certificate, which contains the temporary identity, to the mobile user who wants to roam across different domains with privacy. To acquire short-lived certificates, the mobile user submits, for authentication, a signature signed by his/her long-lived private key. The IMS verifies the signature by the following process:

1. Checks the root certificate of the long-lived certificate from its CA trust list.
2. Checks the status of the long-lived certificate from CRL.
3. Verifies the signature value by the public key contained in the long-lived certificate.

Once authenticated, the mobile user will obtain a short-lived certificate with a new key pair (public and private keys) and use as a token for mobile access. Note that the mobile user can connect to the IMS by a secure tunnel such as SSL/TLS. Figure 3 shows the proposed certification model.

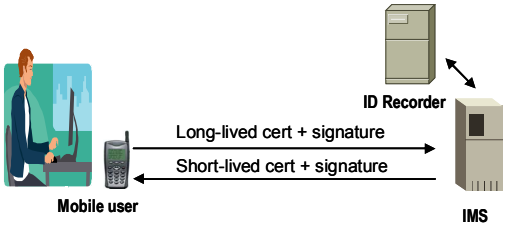


Figure 3 Applies for Short-lived Certificate

Second, the IMS must build a record, which is stored in an ID Recorder, to maintain the mapping between the true identity and the temporary identity for the periodical settlement purpose. In the design proposed in this paper, the visited network operator can claim the payment off-line due to the fact that the mobile user signs for the usage of the visited network. Thus an on-line check is not required. The details will be discussed in the next section.

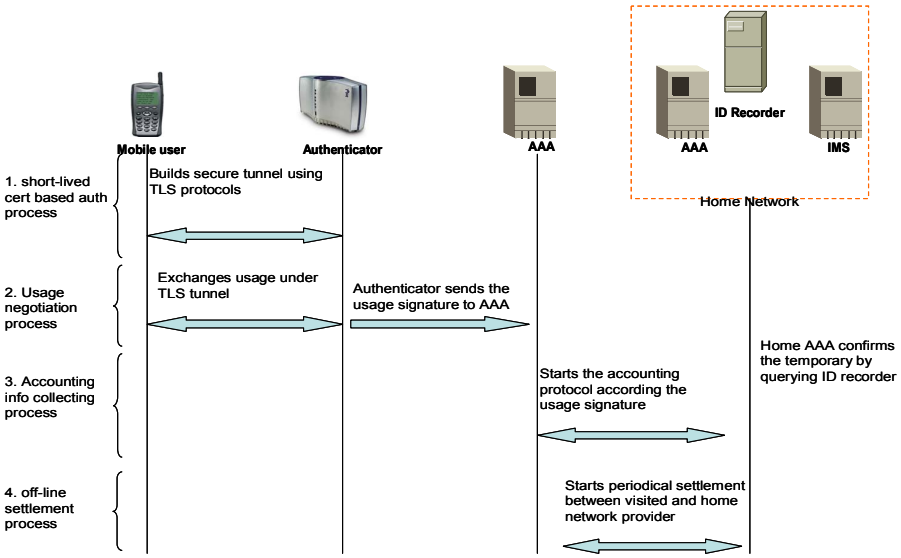


Figure 4 Fast Authentication Procedures

### C. Fast Authentication Method based on Short-lived Certificates

As previously stated, the proposed scheme can achieve both privacy and efficiency. This is because that the period of the short-lived certificate containing the temporary identity is short enough such that the mobile user cannot be identified and the authentication process occurs only between the mobile user and authenticator to eliminate the delay caused by backbone communication. The proposed scheme is depicted in Figure 4. Each phase is described below.

1. Short-lived certificate based authentication process: The mobile user and the authenticator authenticate each others using short-lived certificates and corresponding key pairs. Once authenticated, a secure tunnel is established using the session key derived during the authentication process.
2. Usage negotiation process: This could be done by means of an information pop-up window instructing the mobile user how to carry out usage negotiation. Another way is for the mobile user to send a pre-defined parameter indicating the amount of the usage (for example 5 dollars for each hour) to authenticator. The authenticator responds to the mobile user inquiry indicating the cost for the pre-defined parameter. If the mobile user agrees the usage, he/she generates the signature of the usage and the current time and then sends to the authenticator. At this point, the mobile user gains access service (or resumes session).
3. Accounting process: The visited AAA in turn communicates with the home AAA to info the transaction. Once receiving, the home AAA validates the usage signature using the public key which can be acquired from the ID Recorder.
4. Off-line settlement: The visited network operator claims the payment based on the usage signature. This can run periodically, for example, once a day.

### D. Inter-domain Roaming without Direct Agreement

In this section, the mobile user roams across two domains where two domains and the home domain have a trust relation described below.

Table 1 Trust relation between Home, First, and Second domains

| | Home | First | Second |
|---|---|---|---|
| Home | | V | X |
| First | V | | V |
| Second | X | V | |

V: have business agreement

X: have no business agreement

This means that the mobile user must create trust relation with the second domain when roaming. The following process can achieve this goal.

- The first and second domain share information stored in their CA trust list.
- The mobile user gets the root certificate from the first domain.
- When roaming to the second domain, the mobile user and the second domain can do the mutual authentication.

The model mentioned above can resolve the problem mentioned in [15] that traditional network providers such as cellular operators will lose some customers over time due to these newer access technologies such as WiMAX or WLAN are provided by newer providers. This is because the proposed model provides an easy way to integrate heterogeneous networks and deals with both accounting and authentication simultaneously.

## 4. Comparison and Performance Study

This section compares the previous inter-domain authentication schemes and evaluates the performance of the proposed scheme by implementing a test-bed described in the following section.

**A. Comparison**

Table 2 shows the results of comparing EAP-TLS [2] and a RK-based Authentication scheme [22] especially for inter-domain conditions. Each item is explained as follows.

1. Location privacy: A scheme which supports the temporary identity and can use a mobile user's temporary identity for authentication, authorization and accounting purposes. The temporary identity must satisfy the requirement "long enough to be useful for the external applications and not too long such that it can be used to identify the user" described in RFC 4372.
2. Direct agreement: The business agreement between a visited network and the home network.
3. Revocation scheme: The certificate revocation scheme.
4. Accounting trigger-signal: A suitable message can trigger the accounting process. This means that the authenticator starts session billing after receiving the message and the home AAA also recognizes the message.
5. Scalability issue: A scheme to acquire and manage the credentials of entities as the number of involved entities grows, resulting in a burden of storage and the complex procedures.

Table 2 Comparison of EAP-TLS, RK based Authentication Method and the Proposed Scheme

| items / Schemes | Location privacy | Accounting Trigger-signal | Direct agreement | Revocation scheme | Scalability issue |
|---|---|---|---|---|---|
| EAP-TLS | x | v | v | v | x |
| RK based Authentication | v | x | v | x | v |
| Proposed Scheme | v | v | x | x | x |

v : The scheme need or has the item

X: otherwise

**B. Authentication Delay**

For measuring the authentication delay for EAP-TLS, EAP-AKA (Authentication and Key Agreement) [4] and the proposed scheme in this paper, a test environment was built as depicted in Table 3 and Figure 5. The test-bed consisted of three AAA servers, a WLAN AP, and client software. Two of the AAA servers acted as proxy AAA servers and the other acted as the home AAA server. The experimental results are shown in Table 4. The test-bed uses some software such as freeradius, hostapd and wpa_supplicant that are derived from the freeRADIUS [25] and hostapd [8, 17] projects.

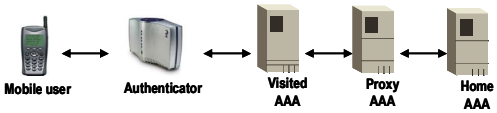


Figure 5 the Three-Party EAP Test-bed

Table 3 Test Environment

| | | CPU | Memory | OS | Software |
|---|---|---|---|---|---|
| Mobile user | Mobile Phone | ARM926EJ 220 MHZ | 30M byte | Linux | WPA_ supplicant |
| | PC | Pentium 1.5G MHZ | 1G byte | Win XP | WPA_ supplicant |
| Authenticator | | Pentium 700 MHZ | 512M byte | Linux | HostAP |
| AAA Server | | Pentium 1.5 MHZ | 512M byte | Linux | Free-RADIUS |

Table 4 the Performance of EAP-TTLS, EAP-TLS, EAP-AKA and the Proposed Scheme

| | EAP-AKA | EAP-TTLS | EAP-TLS | Proposed Scheme |
|---|---|---|---|---|
| Mobile phone | 201.12 ms | 156.74 ms | 264.30 ms | 180.49 ms |
| PC | X | 54.4 ms | 153.4 ms | 71.4 ms |

ms : milli-second

In the mobile phone of this test-bed, the program can only access the SIM card through the modem of the mobile phone, and the delay of setup the channel to the modem is large. Thus, the EAP-AKA has significant latency came from two parts: the channel-setup delay and the propagation delay from WLAN to a 3G-operator network.

**C. Analysis**

The analysis in terms of the requirements mentioned above is described below.

- The IMS issues the short-lived certificate for carrying a temporary chargeable identity to present the mobile user and meet the temporary requirement of RFC 4372.
- The proposed framework uses the short-lived certificate with a public key pair in the authentication process and billing process. This can avoid the risk of identity fraud and support the non-repudiation billing mechanism due to the fact that the digital signature is generated by the private key during the two processes.
- For building the trust relationship, the entities only need to store few root certificates. The proposed framework is a scalable model.
- The proposed framework does not increase the authentication delay. This has showed in Table 4.

## 5. Conclusions

The proposed framework encapsulates a temporary identity in a short-lived certificate so the scheme can deal with both authentication and authorization with privacy. Furthermore, the proposed scheme uses the short-lived certificate in a way that the

authentication process occurs only between the mobile user and authenticator avoiding the need for a certificate revoke scheme. This can greatly reduce the authentication latency. Thus, the proposed scheme can achieve both privacy and efficiency. Future work is to analyze risk and threat of the proposed scheme.

## Reference:


[1] B. Aboba, L. Blunk, L. Vollbrecht, J. Carlson, and H. Levokwetz, Extensible Authentication Protocol (EAP), IETF RFC 3748, June 2004.

[2] B. Aboba and D. Simon, PPP EAP TLS Authentication Protocol, IEFT, RFC 2716, October 1999.

[3] F. Adrangi, A. Lior, J. Korhonen and J. Loughney, Chargeable User Identity, IETF, RFC 4372, January 2006.

[4] J. Arkko and H. Haverinen, Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA), IETF Internet Draft, Nov. 2004.

[5] M. Bargh, R. Hulseboch, E. Eertink, A. Prasa, H. Wang and P. Schoo, "Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs," in Proc. ACM WMASH 2004 (October 2004).

[6] P. Calhoun, Diameter Base Protocol, IETF, RFC 3588, Setmber 2003.

[7] P. Funk and S. Blake-Wilson, EAP Tunneled TLS Authentication Protocol (EAP-TTLS), IETF Internet Draft, April 2004.

[8] hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator, http://hostap.epitest.fi/hostapd/

[9] R. Housley, W. Polk, W. Ford and D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL), IEFT, RFC 3280, April 2002.

[10]Y. Hsu and S. Seymour, "Intranet Security Framework Based on Short-Lived Certificates," in The 6th Workshop on Enabling Technologies on Infrastructure for Collaborative Enterprises (1997), pp. 228-234

[11]IEEE, Port-Based Network Access Control, IEEE STD 802.1x, June 2001.

[12]IEEE, Wireless Medium Access Contril (MAC) and Physical Layer (PHY) Specifications" Medium Access Control (MAC) for Enhanced Security Enhancement, IEEE STD 802.11i, July 2004.

[13]S. Koga and K. Sakurai, "A Distributed Online Certificate Status Protocol with a Single Public Key," in 7th International Workshop on Theory and Pratice in Public Key Cryptography (March 2004).

[14]M. Myers, X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol-OCSP, IEFT, RFC 2560, June 1999.

[15]M. Nakhjiri and M. Nakhjiri, AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility, Wiley, 2005.

[16]OMA, Wireless Application Protocol-Wireless Public Key Infrastructure, WAP-217-WPKI, April 2001.

[17]OpenSSL Project, http://www.openssl.org/

[18]S. Pack and Y. Choi, "Fast Inter-AP Handoff using Predictive Authentication Scheme in a Public WLAN," in Proc. Networks 2002 (Aug. 2002).

[19]S. Pack and Y. Choi, "Fast Handoff Scheme based on Mobility Prediction in Public Wireless LAN Systems," IEEE Proceedings Communications, vol. 151, no. 5 (October 2004), pp. 489-495.

[20]S. Pack, H. Jung, T. Kwon and Y. Choi, "SNC: A selective Neighbor Caching Scheme for Fast Handoff in IEEE 802.11 Wireless Networks," in ACM Mobile Computing and Communications Review, vol.9, no. 4 (October 2005), pp. 39-49.

[21]A. Palekar, D. Simon, J. Salowey, H. Zhou, G. Zorn and S. Josefsson, Protected EAP Protocol, IETF Internet Draft, October 2004.

[22]A. R. Prasad and H. Wang, "Roaming Key Based Fast Handover in WLANs," in WCNC 2005 (March 2005).

[23]A. R. Prasad, A. Zugenmaier and P. Schoo, "Next Generation Communications and Secure Seamless Handover," in Security and Privacy for Emerging Areas in Communication Networks (Sept. 2005), pp. 267-274.

[24]P. Prasithsangaree and P. Krishnamurthy, "A New Authentication Mechanism for Loosely Coupled 3G-WLAN Integrated Networks," in IEEE 59th Vehicular Technology Conference, VTC 2004-Spring, vol.5 (May 2004), pp. 2998-3003.

[25]FreeRADIUS Project, http://www.freeradius.org/

[26]M. Shin, A. Mishra and W. Arbaugh, "Improving the Latency of 802.11 Hand-offs using Neighbor Graphs," in Proc. ACM MobiSys 2004 (June 2004).