Passport/Visa: Authentication and Authorisation Tokens for Ubiquitous Wireless Communications

Abdullah Almuhaideb, Phu Dung Le, and Bala Srinivasan

Faculty of Information Technology, Monash University, Melbourne, Australia
{Abdullah.Almuhaideb,Phu.Dung.Le,Srini}@monash.edu.au

Abstract. Ubiquitous connectivity faces interoperation issues between wireless network providers when authenticating visiting users. This challenge lies in the fact that a foreign network provider does not initially have the authentication credentials of the mobile users. The existing approaches are based on roaming agreement to exchange authentication information between the home network and a foreign network. This paper proposes Passport/Visa approach that consists of two tokens: Passport (authentication token) and Visa (authorisation token), to provide a flexible authentication method for foreign networks to authenticate mobile users. Our approach can be used when there is no roaming agreement between foreign networks and the mobile user's home network. The security analysis indicates that our protocol is resistant to well-known attacks, ant it efficiently ensures the security for both mobile users and network providers. The performance analysis also demonstrated that the proposed protocol will greatly enhance computation, and communication cost.

Keywords: authentication, ubiquitous mobile access, security protocols, roaming agreement, wireless roaming.

1 Introduction

The enhancement of mobile devices and wireless systems provide new opportunities for the next generation of mobile services, such as m-commerce, m-learning and m-government. This fact makes it desirable for m-internet users to be connected everywhere. It is estimated that half the world population pay to use mobile services [1]. When mobile users (MU) move from their home network (HN) domain to a foreign network (FN) domain, efficient cross-domain authentication and access control are necessary for multiple domains roaming [2-3]. There are security concerns from both the MUs and FNs perspectives, as they cannot establish a connection without being authenticated to each other. The traditional solution is to have a roaming agreement between the HN and a FN for verification. However if there is no roaming agreement, MUs cannot be authenticated and served by the FNs.

Problem Statement. A key challenge in such a ubiquitous heterogeneous network environment is authenticating unknown users by FN providers and preventing unauthorised access. This should take place when roaming to administrative domain without a pre-established roaming agreement with a MU's HN domain [4].

P. Sénac, M. Ott, and A. Seneviratne (Eds.): MobiQuitous 2010, LNICST 73, pp. 224–236, 2012.

Our Approach and Contributions. This paper proposes a novel Passport/Visa authentication tokens as a practical solution to provide the MU with a flexible authentication and service access mechanism in a ubiquitous mobile access environment. One of the main features of the proposed scheme is the lack of having to authenticate a MU, via a trusted identity provider (IdP), every time the MU requests a service from the FN. In other words, it can eliminate re-authentication with the HN after the first successful authentication. Also, our scheme provides an efficient MU energy consumption, as the operation required by MU only involves symmetric cryptography. These features support both limited-resource (low-power) mobile devices and the low-bandwidth mobile communications. Security and performance analysis conducted to evaluate our proposed protocol.

Paper Organization. The rest of this paper is structured as follows. It starts with an overview of the ubiquitous mobile access model and the Passport/Visa approach, where Passport acquisition, Visa acquisition, mobile service provision, Passport and Visa revocation are illustrated (Section 2). This will be followed by a review and comparison of functionality of existing approaches to the problem (Section 3). We then demonstrate the security analysis (Section 4) and present the evaluation of performance in comparison to existing approaches (Section 5). Finally, our conclusion of this paper will be presented (Section 6).

2 The Proposed Solution

2.1 Ubiquitous Mobile Access Authentication Model

To achieve authentication for ubiquitous wireless access environments, there should be more flexible ways to establish trust without relying on roaming agreements. In The proposed model [5], the MUs are able to negotiate directly with potential FNs regarding quality of service, pricing and other billing related features in order to establish service agreement and get the authorization token. IdPs are required to verify the MU's identity and credentials, and IdP can provide this as a service to MUs. Identifying a MU is important for accounting and charging purposes by FN. MU is pre-registered with IdP to get identification token. The IdP role can be played by a trusted entity such as HN. To simplify the example, in this paper the HN will be considered as the IdP in this context. Also, FN providers are able to communicate directly with potential MUs and make trust decision whether or not to provide network service. For the FN provider to trust a MU, HN is used to verify the claimed identity of the MU. Also, Certificate Authority (CA) is engaged to establish a trust with both HN and FN. With the mutual trust, FN provider ensures that the service will get paid and MU ensures that the FN provider is a legitimate and trusted provider.

2.2 Passport/Visa Approach

This approach designed based on the above described model. It can be used when there is no roaming agreement between FNs and the MU's HN. It consists of two tokens: Passport and Visa. The "Passport" is an authentication token issued by the HN to the MU in order to identify and verify MU identity. The Passport in itself does not

grant any access, but provides a unique binding between an identifier and the subject. The "Visa" is an authorisation token that granted to a MU via a FN. The Visa token can be used as an access control to ban individual users. In this paper, an improved version of our previous [6] Passport/Visa protocols is introduced. The followings are a set of protocols were developed to achieve the approach objective. Notations are clarified in the following table.

Table 1. Notations used in the protocols

Symbol	Description	Symbol	Description
MU	Mobile user	**HN**	Home network service provider.
id_A	Identity of an entity A	**FN**	Foreign network service provider.
CA	Certivicate Autheroity	**SC**	Smart card issued by HN for MU.
$\mathbf{Visa}_{\mathbf{B}}^{\mathbf{A}}$	A visa that issued by A to B.	$\mathbf{Passport}_{\mathbf{B}}^{\mathbf{A}}$	A passport that issued by A to B.
$\mathbf{Visa}_{\mathbf{No}}$	The visa number	$\mathbf{Pass}_{\mathbf{No}}$	The passport number
$PK_A(x)$	Encrypting a message X using the public key of A	$Sig_A(x)$	Signing a message X using the private key of A
$h(x)$	One-way has function	K_{A-B}	Symmetric Key shared between A and B
$Cert_A$	Certificate issued for A by the CA.	$valid_{A-B}$	Entity A has been validated by B.
T_A	Timestamp generated by an entity A	r_A	A random number generated by entity A
$expiry$	Passport or visa expiry date.	$VisaReq_{FN}$	Visa Request
$RevOke$	Revoke request	$SerReq$	Service Request
$data$	Consists of all other information such as type of Passport/Visa, type of MU, MU name, MU date of birth, date of issue, place of issue, issuer ID, and issuer name.In the Visa it may include number of access, duration of access, service type, service name, and times of access.		

2.2.1 Passport Acquisition Protocol

This protocol describes the MU registration process with HN (Passport issuer); by completing this protocol MU will receive a Passport. For any network service request from a FN, MU is required to have a Passport that registered with the HN. The registration with the HN takes place offline, and it occurs once. When completed, the HN issues a smart card (SC) to the MU. The SC information is encrypted with the MU's biometric (such as finger print). Every SC consists of three components:

$$SC =< K_{MU-HN}, Passport_{MU}^{HN}, Pass_{No} >$$

Every SC has a unique ID, which is combined with MU's biometric to generate a symmetric master Key. Key master is offline distributed, and stored on the Passport and the MU's SC. The HN's generate the Passport which is signed and encrypted with both the HN's Sig_{HN} and PK_{HN}, then stored in the SC. The HN's $Cert_{HN}$ is included for verification by FN and establishing trust with the HN using CA. The signature can be verified to ensure the integrity of the Passport. The Passport is given as:

$$Passport_{MU}^{HN} = \{Sig_{HN}(Pass_{No}, expiry, id_{HN}, PK_{HN}(id_{MU}, K_{MU-HN}, data)), Cert_{HN}\}$$

2.2.2 Visa and Service Acquisition Protocol

The MU will receive the required Visa from the FN after completing the identification and verification process with the HN successfully. When the MU has his/her Passport

(authentication token) in hand, the authentication process can be started with the FN in order to obtain the required Visa. The protocol is demonstrated as follows (Fig. 1):

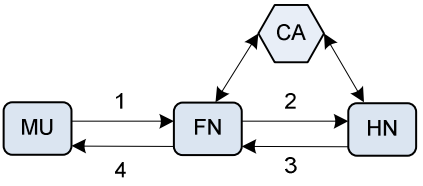

Fig. 1. Visa and service acquisition.

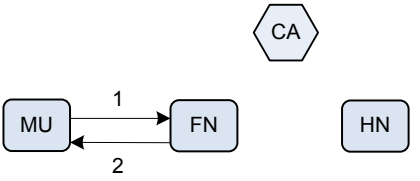

Fig. 2. Mobile service provision.

Step 1: MU → FN: $VisaReq_{MU-FN}, Passport_{MU}^{HN}, \{id_{FN}, r_{MU}, T_{MU}\}_{SK_{MU-HN}}, T_{MU}, r"_{MU"}$

$$SK_{MU-HN} = h(K_{MU-HN}, id_{MU}, id_{FN}) \quad (1)$$

This protocol starts once the MU sends his/her Visa request, Passport, and $\{id_{FN}, r_{MU}, T_{MU}\}$ where they are encrypted by the session key SK_{MU-HN}. This key is generated using the formula (1) to establish a mutual authentication between the MU and the HN. Every time MU request service from different FN a new session key is generated, three factors are involved: K_{MU-HN}, id_{MU}, and id_{FN} are hashed using *h(x)*. The id_{FN} is used to enable the HN to verify it with the one in the FN certificate to make sure that it has not been modified by an attacker. The r_{MU} is used to authenticate the FN. Another MU's random number $r"_{MU"}$ is sent to the FN to be used as a factor in generating the initial key IK_{MU-FN} based on the formula (2).

Step 2: FN → HN: $Passport_{MU}^{HN}, \{id_{FN}, r_{MU}, T_{MU}\}_{SK_{MU-HN}}, Cert_{FN}, T_{FN}, r_{FN}$

Before processing the authentication with the HN, the FN checks T_{MU} and $Cert_{HN}$ whether it is valid or not, and if so, it forwards the Passport, $\{id_{FN}, r_{MU}, T_{MU}\}_{SK_{MU-HN}}$ with its $Cert_{FN}, T_{FN}, r_{FN}$ to the HN as illustrated in Step 2. The $Cert_{FN}$ is sent to the HN for verification and establishing trust using the CA. The r_{FN} used to authenticate the HN. Both T_{MU} and T_{FN} are used to stop reply attacks.

Step 3: HN → FN: $PK_{FN}(Sig_{HN}(Pass_{No}, valid_{MU-HN}, r_{MU}, r_{FN})),$

$$\{id_{FN}, valid_{FN-HN}, r_{FN}, r_{MU}, T_{HN}\}_{SK_{MU-HN}}$$

After receiving the message from the FN, the HN ensures if T_{MU} and T_{FN} are valid. If one of them is not, the HN replies with un-fresh session and terminates the request. Otherwise, the HN checks the validity of the $Cert_{FN}$ with the CA. If it was valid, the HN decrypts the Passport with its private key and then verifies the signature using the HN's public key. After the HN checks that the MU's Passport is genuine and valid, it gets the shared key (K_{MU-HN}) and its relevant information such as the date of expiry. The HN then generates the session key (SK_{MU-HN}) to decrypt the second part of the message $\{id_{FN}, r_{MU}, T_{MU}\}$. The HN compares the id_{FN} in this message with the one in the certificate to ensure the FN has not been changed. The HN then encrypts $\{id_{FN}, valid_{FN}, r_{FN}, r_{MU}, T_{HN}\}$ with the session key Sk_{MU-HN}.

Also, as the HN authenticate the MU, the HN then computes their digital signatures using its private key, then encrypt them ($Pass_{No}, valid_{MU}, r_{MU}, r_{FN}$) using the FN's public key. The HN then put both the FN and the MU authentication part in one message and sends it to the FN.

Step 4: FN → MU: $Visa_{MU}^{FN}, \{id_{FN}, valid_{FN-HN}, r_{FN}, r_{MU}, T_{HN}\}_{SK_{MU-HN}}$,

$$\{k_{MU-FN}, Visa_{No}\}_{Ik_{MU-FN}}, r"_{FN"}, \{Service\}_{SK_{MU-FN}}$$

Once the FN received the message from the HN, it decrypts its part using its private key and verifies it using the HN's public key. If the FN received the validity of the Passport and checks its random number, the Visa will be generated as follows:

$$Visa_{MU}^{FN} = PK_{FN}(Sig_{FN}\ (Pass_{No}, Visa_{No}, expiry, data, K_{MU-FN}))$$

The signature of the FN Sig_{FN} in the Visa is used to stop a forged Visa. The Visa is encrypted with the FN's public key, which means that only the FN can decrypt it. The FN stores the Visa information for future verifications. The field "valid" is set to FALSE once a Visa is revoked; otherwise it is set to TRUE.

The following is an example:

$$\{Pass_{No};\ Visa_{No};\ expiry;\ \text{valid}\}$$

Then the FN generates the initial key using formula (2). The initial key will be used once to distribute the master key K_{MU-FN} and $Visa_{No}$. Also, the FN forwards a new random number $r"_{FN"}$ to be used by the MU to generate the session key. The session key will be used to achieve mutual authentication between MU and FN and to deliver the services. This session key SK_{MU-FN} is generated using formula (3).

$$IK_{MU-FN} = h(Pass_{No}, id_{FN}, r_{MU}, r_{FN}, r"_{MU"}, r"_{FN"}) \quad (2)$$

$$SK_{MU-FN} = h(K_{MU-FN}, Visa_{No}, Pass_{No}) \quad (3)$$

After the MU receives the authorisation message from the HN through the FN $\{id_{FN}, valid_{FN}, r_{FN}, r_{MU}, T_{HN}\}_{SK_{MU-HN}}$, the MU decrypts it using the SK_{MU-HN}. The HN's T_{HN}, r_{MU}, and id_{FN} correctness will be checked. If they were incorrect, the Visa will be rejected, and if they were verified, the Visa will be kept for future service requests. The MU computes the Ik_{MU-FN} to get the shared master key K_{MU-FN} and $Visa_{No}$. Finally, The MU computes the SK_{MU-FN} to get the requested services.

2.2.3 Mobile Service Provision Protocol

This protocol (Fig. 2) illustrates how a MU can be granted further network services from a FN in secure manner. When the MU obtains a valid Visa, the MU will be eligible to request further network services from the FN based on the Visa condition.

Step1: MU → FN: $SerReq, Visa_{MU}^{FN}, \{r_{MU"}, Visa_{No}\}_{SK_{MU-FN}}$

To request an access to the FN services, the MU sends $SerReq$, the Visa, and both $r_{MU"}$ and $Visa_{No}$ encrypted by the first session key SK_{MU-FN} (formula 3).

Step2: FN → MU: $\{r_{FN"}, Pass_{No}\}_{SK'_{MU-FN}}, \{Service\}_{SK"_{MU-FN}}$

After the FN receives the service request, it decrypts the Visa with its private key to check its validity by its public key. If the Visa is considered as valid, the FN has to compute the SK_{MU-FN} to verify the $Visa_{No}$, and to get the new $r_{MU"}$. The $r_{MU"}$ will be used to generate the second session key SK'_{MU-FN} as follows (formula 4):

$$SK'_{MU-FN} = h(SK_{MU-FN}, K_{MU-FN}, r_{MU"}) \quad (4)$$

The third session key will be used by the FN to encrypt its $r_{FN"}$ and $Pass_{No}$. Finally, the third session key will be generated $SK"_{MU-FN}$ using formula (5).

$$SK"_{MU-FN} = h(SK'_{MU-FN}, SK_{MU-FN}, r_{FN"}) \quad (5)$$

By having the third session key in hand both parties know that mutual authentication has been realized, and the service can be started. However, for the next access the MU is required to generate a new set of session keys.

2.2.4 Passport and Visa Revocation Protocol

This protocol will be used to stop requesting services with a stolen Passport or Visa. If a Passport or Visa is considered to be revoked (e.g., the mobile user's shared keys K_{MU-HN} or K_{MU-FN} expires, or the MU notices the FN revoking a Visa or the HN to revoke a Passport). The Passport revocation can be illustrated as:

$$\text{MU} \rightarrow \text{HN: } Passport_{MU}^{HN}, \{Pass_{No}, RevOke\}_{K_{MU-HN}}$$

The protocol starts when the MU sends the RevOke message to the corresponding HN. The HN decrypts the Passport with its private key and verifies the signature with its public key. The HN get the shared key from the Passport and decrypt the second part of the message. The HN checks if Pass_{No} is already stored. If not, it means that there is no Passport issued with this Passport number. If it was stored, it stores the revoked Passport information and updates the status of the Passport as RevOke. The Visa revocation can be illustrated as:

$$\text{MU} \rightarrow \text{FN}: \ Visa_{MU}^{FN}, \{Pass_{No}, Visa_{No}, RevOke\}_{SK_{MU-FN}}$$

When FN receives a RevOke message from MU, the FN decrypts the Visa with its private key and verifies the signature with its public key. The FN gets the shared key from the Passport and generates the session key to decrypt the second part of the message. Then the FN decrypts the message with the session key SK_{MU-FN} (illustrated in (3)). The FN updates the status of the Visa as RevOke. Once a MU requests network services, the FN checks if the Visa was revoked. If it is revoked the service request will be rejected.

3 Related Works and Functionality Comparison

In this section we review a number of related works in the area of ubiquitous mobile access authentication. The review was based on following three key requirements. A flexible ubiquitous mobile access authentication solution should satisfy the following requirements: (A) Wireless Technology Independence: the proposed authentication solution should not be designed for a specific underlying wireless technology. It

should be aimed to be designed at the network layer, or higher, of the OSI to avoid the differences in the link and physical layer. (B) Roaming Agreement-less: in the current solutions roaming agreement is used by cellular network to extend its services using other networks. However, it is not likely to set up formal roaming agreements with every possible provider by MU's HN [2, 7]. Therefore, the solution should not depend on roaming agreement between FN providers and the HN. (C) Home Network Independent: The solution should support direct negotiation to establish service agreement between the MU and any FNs, where the FN has full control over the authorisation process. As HN plays the role of an IdP, MUs can get the benefits of the HN partners and more. They could get more network service in areas not covered by the HN's partners with full freedom of choice. The below table summarise the comparison and indicates that our proposed approach can satisfy these requirements while the other related approaches cannot (Table.2).

Table 2. Functionality comparison between the existing approaches and our approach

Approach / Function	*A*	*B*	*C*
Proof-Token [4]	Yes	No	No
SSO architecture [8]	No (WLAN)	No	Yes
Mobile Bazaar [9]	No(Ad Hoc)	Yes	Yes
Homeless mechanism based on tickets [2]	Yes	No (Broker)	No
Sirbu et al.'s scheme (Kerberos-PK)[10]	Yes	No (Broker)	No
Lee et al. 's scheme (Ticket base) [11]	Yes	No (Broker)	No
Our Passport/Visa Approach	Yes	Yes	Yes

Tuladhar et al. [4] have proposed proof tokens authentication architecture and protocol. In their approach, they tried to solve two problems. The first problem is that the limited roaming agreement of the HN with FNs, and they proposed to allow MUs to access the partners of previously visited networks by that MU. The second problem is authentication delays, which they identified as a major cause for high latency. They propose the collaboration between adjacent networks. However, this approach still relies on roaming agreement for authentication, and does not support a direct negotiation and service agreement between the MU and FN.

Matsunaga et al. [8] have proposed a single sign-on (SSO) authentication architecture that confederates WLAN service providers through trusted IdPs. They argue that the dynamic selection of authentication method, and IdP will play a key role in confederating public wireless LAN service providers under different trust levels and with alternative authentication schemes. However, there are three limitations to this approach. The first limitation in this approach is the dependence on roaming agreement between network providers and IdPs, which may limit the MU roaming freedom. The second limitation is the dependency on a single wireless technology. Lastly, it is limited to web-based authentication using cookies [12].

Chakravorty et al. [9] proposed a mobile bazaar (MoB) , an open market architecture for collaborative wide-area wireless services by using reputation management. Their approach is based on short-term transient access network resource reselling by the network's subscribers to other users using an ad hoc network type solution. The limitation of this approach is the dependency on FN's users availability in trading and accessing the network.

The following four works are based on ticket model. Patel and Crowcroft [2] proposed a homeless mechanism based on the notion of tickets. Lei, Quintero and Pierre [13] presented a reusable tickets for accessing mobile services. In [10], Sirbu et al. proposed an extended Kerberos with PKC to improve the scalability and security. While, in [11], Lee et al. proposed a secure scheme for providing anonymous communications in wireless systems using ticket based authentication and payment protocol. The major disadvantage of this model is that a FN does not have a control over granting the authorisation token, as the tickets are approved by the ticket server (TS). The TS acts as a broker, where it requires FNs to have pre-established roaming agreements. The broker concept reduces the issue of one-to-one roaming agreement by having one-to-many service agreement. However, the broker approach will not work in case of there is no service level agreement between the TS and the potential FN. This solution does not support the open market environment as MUs depend on TS to access network providers. While in our solution, IdP does not require pre-established roaming agreement to authenticate their MU, and CA is used to establish trust between both FN and IdP.

4 Security Analysis

The SVO logic [14] has been use to prove the correctness of our protocol. The detailed proof is not included because of the pages limit. In this section, we analyse the security of the proposed protocol with respect to following security requirements:

Proposition 1. *The proposed scheme can prevent Passport/Visa forge.*

Proof. Since the Passport and the Visa contain the signature of the issuer, they cannot be generated by attackers in the name of the HN or FN. So it is impossible to fabricate or fake a Passport or a Visa as the issuer will check the integrity by verifying the signature.

Proposition 2. *The proposed scheme can provide mutual authentication.*

Proof. In the mobile service provision phase, the MU sends a message that consists of two parts: a Visa, and the encrypted new random number $r_{MU"}$.The FN decrypts the Visa with its public key and gets the shared key. Also as the FN signed the Visa, it can check the validation of the Visa. The FN uses the previous session key with $Pass_{No}$ and $Visa_{No}$ to generate the first session key which will be used to decrypt the second part of the message and get a new random number. The shared master key with the first session key, and $r_{MU"}$ will be used to generate the second session key. By decrypting the FN message, the MU can get the FN's random number. Now, both parties are able to generate the third session key and mutual authenticate each other.

Proposition 3. *Our protocol can resist replay and man-in-the-middle attacks.*

Proof. An attacker may sniff a valid Visa, however, the K_{MU-FN}, $Pass_{No}$, and $Visa_{No}$cannot be obtained as they are encrypted in the Visa. The only party that can get the K_{MU-FN}, $Pass_{No}$ and $Visa_{No}$ from the Visa is the FN. In addition, timestamps are used in each communication between the three entities: MU, FN and HM to ensure the message has not been replayed.

Proposition 4. *The proposed scheme is safe against impersonation attacks.*

Proof. In our protocol, the stored information in SC (e.g. Passport) is encrypted with the MU fingerprint. Thus, when the SC has been stolen, it is infeasible for attackers to impersonate the MU to have an access.

Proposition 5. *The proposed scheme can withstand spoofing.*

Proof. Since a FN cannot get any information regarding to the MU unless the HN authenticates the FN, it is impossible for a malicious entity to masquerade as a legitimate FN to get the MU information. In other word, the MU can ensure that s/he is indeed communicating with a real service provider and not with a bogus entity.

Proposition 6. *The proposed scheme can provide key freshness.*

Proof. Only the MU and the FN know the shared master key K_{MU-FN}. In addition, it is not used to encrypt any message. Instead, a new session key is generated in every service request. This key is established by contributing the random numbers provided by both the MU and the FN. So the key freshness is guaranteed.

Proposition 7. *The proposed scheme can provide privacy and user anonymity.*

Proof. The MU's personal details are kept secretly with the HN. Therefore, when a MU wants to roam into a FN, s/he only needs to send his/her Passport without reveal any information related to his/her ID. Moreover, the HN only returns the $Pass_{NO}$ to the FN if the verification is true. This means that the FN has no idea about the ID of the owner of this Passport.

5 Performance Analysis

In this section, we will evaluate the proposed protocol in terms of computation, and communication cost, by comparing those of the existing schemes in [10] and [11]. Also, scalability analysis will be discussed to demonstrate the key management efficiency.

5.1 Computation Cost

In this subsection, the results of performance comparison of our scheme, the scheme of Lee et al. and the scheme of Sirbu et al. are shown in Figure 3 and Table 3. In the performance comparison, T_{sym} and T_{Asym} are used to denote the computational time of symmetric and asymmetric key cryptography, respectively.

In this performance analysis of the authorisation and service provision phase, the scheme of Sirbu et al. took $16T_{\text{sym}}+4T_{\text{Asym}}$, while Lee et al. and our schemes took $4T_{\text{sym}}+6T_{\text{Asym}}$ and $6T_{\text{sym}}+8T_{\text{Asym}}$, respectively. Obviously, the scheme of Sirbu et al. gains better performance as it requires less asymmetric encryptions/decryptions in this phase. Additionally, in the access service phase, it required $6T_{\text{sym}}+2T_{\text{Asym}}$ in our scheme, while the other two schemes require re-authentication and repeat the first phase. Our time calculations is based on [15], they indicated a symmetric encryption/decryption requires 0.87ms, and an asymmetric cryptography is approximately equal to 100 symmetric operations. Therefore, an asymmetric

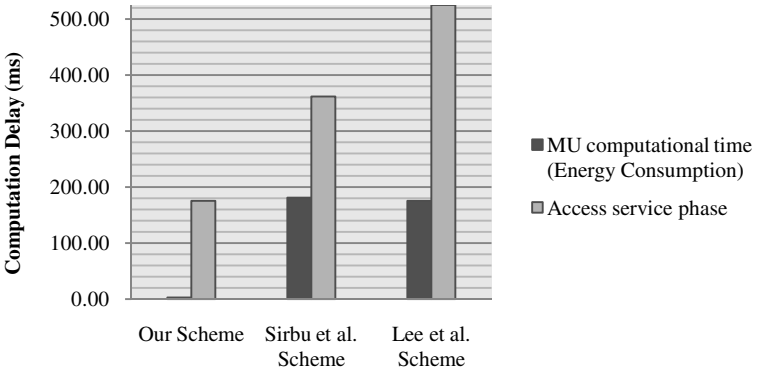

Fig. 3. Computation comparison among different protocols

encryption/decryption computation takes approximately 87ms. The computational costs of the one-way hash function (0.05ms) can be ignored since it is quite lighter, compared to asymmetric and symmetric operations.

Based on the above estimated times, the computational time for the access service phase were 179.22ms, 361.92ms, and 525.48ms in our scheme, Sirbu *et al*., and Lee *et al*. schemes, respectively. Thus, our scheme is reduced to 49% and 34%, of access service phase computational cost of Sirbu *et al*., and Lee *et al*. schemes, respectively. Therefore, the proposed scheme is highly efficient in the terms of service provision computational overheads, as shown in Figure 3. The other two schemes take more than the double of our access service phase computational time, as they requires MU to do both authorisation and access service phases (re-authentication) every time for service provision. For example, the scheme of Sirbu *et al*. is based on Kerberos which relies on timestamps for freshness indicator, therefore the time stamped ticket can only be valid for a single session [13].

Also, our scheme took around 2.61 ms ($3T_{sym}$ in both phases), while the scheme of Sirbu *et al*. required 180.96 ms ($8T_{sym}+2T_{Asym}$) and the scheme of Lee *et al*. took 175.74 ms ($2T_{sym} + 2T_{Asym}$). The MUs computational cost of our scheme is reduced to 2% of other schemes. In other words, our scheme outperforms the other two approaches in terms of the MUs computational cost, which affect the energy consumption of their limited power device. The proposed scheme is highly efficient in the terms of MUs computational overheads and energy consumption, shown in Figure 3, because of the elimination of asymmetric cryptosystems.

In terms of authorisation and service provision phase, our scheme is slower than the other two schemes by 2 s to 3 s. Since our scheme took 701.2 ms, while the scheme of Sirbu *et al*. required 361ms and the scheme of Lee *et al*. took 525.48ms. Most of our computation time is spent in the authorisation phase. However, compared with other two schemes, our scheme took less computation time in the access service phase, which will be performed more frequently than authorisation phase. For example, in our scheme MU performed authorisation phase (Visa acquisition) just once, then MU can access services any time based on the Visa expiration date. Table 3 summarizes the

performance comparisons of our scheme with the schemes of Sirbu *et al*., and Lee *et al*. In summary, our scheme took more computation time in the authorisation phase, but achieves better performance in the access service phase and MU energy consumption.

5.2 Communication Cost

The communication cost in our scheme can be reduced to 33% of the schemes of Sirbu *et al*., and Lee *et al*. after the first authorisation phase. Since the proposed scheme can eliminate re-authentication with the HN compare to other schemes. In other words, FNs authenticate MUs with their HN just once in the authorisation phase (takes 4 round messages) to get the Visa, then they can access their services (takes 2 round message) multiple time, based on the Visa type, without the need for HN re-authentication. Most of the communication cost is in the authorisation phase; therefore eliminating the re-authentication will highly improve the performance.

Table 3. Efficiency comparisons between our scheme and other related schemes

Efficiency feature/Approach	***Our Scheme***	*Sirbu et al.'s scheme (Kerberos-PK)[10]*	*Lee et al. 's scheme (Ticket base)[11]*
Computation cost:			
Authorisation & service provision phase	$6T_{sym}+8T_{Asym}$ ≈701.2ms	$16T_{sym}+4T_{Asym}$ ≈361.92ms	$4T_{sym}+6T_{Asym}$ ≈525.48ms
Access service phase	$6T_{sym}+2T_{Asym}$≈179ms	≈$416T_{sym}$=361.92ms	≈$604T_{sym}$=525.48ms
MU computational time (Energy Consumption)	$3T_{sym}$=2.61ms	≈$208T_{sym}$=180.96ms	≈$202T_{sym}$=175.74ms
Communication cost:			
Eliminate HN re-authentication	Yes	No	No
Number of messages	4 then 2	5	6

In term of the total number of messages required in the full protocol, our scheme has better communication cost with 4 round messages, while the schemes of Lee *et al*. and Sirbu *et al*. required 5 and 6 round messages, respectively. Table 3 indicates that our proposed protocol can reduce computation and communication cost for the limited resource mobile device compares the other two schemes.

5.3 Scalability Analysis

The proposed scheme is scalable, as the increase of MUs subscription will not affect the HN and the FN storage space. Since both HN and FN do not store MUs shared master-key, which eliminate the maintenance of this key with every MU. Also, the large storage of these keys is eliminated. Moreover, this technique improves the scheme security as the compromise of the key storage in HN or FN will reveal all the symmetric keys to the attacker and will have to be revoked. This problem exist in the traditional Kerberos in the event of a KDC compromise [10]. Instead the master-keys are stored in both the Passport and the Visa to achieve an efficient key management. The Passport and Visa stored only in the MU's SC which provides tamper resistance.

6 Conclusion

This paper argued for the need of a flexible way to authenticate mobile users in ubiquitous wireless access environment. Thus, as a flexible and practical solution, we introduced the Passport/Visa approach as a roaming agreement-less based to enable MUs to authenticate themselves to FN providers via direct negotiation. Moreover, the FNs have full control over the authorisation process. In contrast to the existing approaches, we believe that our approach is more flexible and eliminates the need for roaming agreements. The security and performance analysis indicates that our protocol is secure and efficient to authenticate MUs and network service providers.

References

1. GSM Association: 20 Facts for 20 Years of Mobile Communications (2007), http://www.gsmtwenty.com/20facts.pdf (Date accessed: October 31, 2010)
2. Patel, B., Crowcroft, J.: Ticket based service access for the mobile user. In: MobiCom 1997: Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 223–233. ACM, NY (1997)
3. Wang, H., Zhang, Y., Cao, J., Varadharajan, V.: Achieving secure and flexible m-services through tickets. IEEE Transactions on Systems, Man, and Cybernetics 33, 697–708 (2003)
4. Tuladhar, S., Caicedo, C., Joshi, J.: Inter-Domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks. In: Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008), pp. 249–255. IEEE Computer Society, Washington, DC (2008)
5. Almuhaideb, A., Alhabeeb, M., Le, P.D., Srinivasan, B.: Flexible Authentication Technique for Ubiquitous Wireless Communication using Passport and Visa Tokens. Journal of Telecommunications 1, 1–10 (2010)
6. Almuhaideb, A., Alharbi, T., Alhabeeb, M., Le, P.D., Srinivasan, B.: Toward a Ubiquitous Mobile Access Model: A roaming agreement-less approach. In: SNPD 2010: the 11th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, June 9-11. IEEE Computer Society, London (2010)
7. Shrestha, A., Choi, D., Kwon, G., Han, S.: Kerberos based authentication for inter-domain roaming in wireless heterogeneous network. Computers & Mathematics with Applications (2010)
8. Matsunaga, Y., Merino, A., Suzuki, T., Katz, R.: Secure authentication system for public WLAN roaming. In: Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, pp. 113–121. ACM, New York (2003)
9. Chakravorty, R., Agarwal, S., Banerjee, S., Pratt, I.: MoB: a mobile bazaar for wide-area wireless services. In: MobiCom 2005: Proceedings of the 11th Annual International Conference on Mobile Computing and Networking, pp. 228–242. ACM, New York (2005)
10. Sirbu, M.A., Chuang, J.C.I.: Distributed authentication in Kerberos using public keycryptography. In: Proceedings Symposium on Network and Distributed System Security, pp. 134–141 (1997)

11. Lee, B., Kim, T., Kang, S.: Ticket based authentication and payment protocol for mobile telecommunications systems, pp. 218–221 (2001)
12. Shin, M., Ma, J., Arbaugh, W.: The Design of Efficient Internetwork Authentication for Ubiquitous Wireless Communications. Network 3, 1 (2004)
13. Lei, Y., Quintero, A., Pierre, S.: Mobile services access and payment through reusable tickets. Computer Communications (2008)
14. Syverson, P., Cervesato, I.: The logic of authentication protocols. In: Focardi, R., Gorrieri, R. (eds.) FOSAD 2000. LNCS, vol. 2171, pp. 63–137. Springer, Heidelberg (2001)
15. Chen, Y., Chuang, S., Yeh, L., Huang, J.: A practical authentication protocol with anonymity for wireless access networks. Wireless Communications and Mobile Computing (2010)