PRIPAY: A Privacy Preserving Architecture for Secure Micropayments

Christoforos Ntantogian, Dimitris Gkikakis, Christos Xenakis
Department of Digital Systems
University of Piraeus
Piraeus, Greece
{dadoyan, dimgkik, xenakis}@unipi.gr

***Abstract*—This paper proposes a privacy preserving architecture, called PRIPAY, which enables micropayments and financial transactions through mobile/wireless operators (2G, 3G, WLANs, 4G, etc.) in a secure and efficient manner. It enables the operator to generate and assign a different pseudonym to each requesting mobile user, equipped with a mobile station (MS), every time it wishes to access a remote Merchant or Service Provider, achieving anonymity and unlinkability. PRIPAY hides the real identity of MS from remote Merchants or Service Providers; but, at the same time it allows the operator to track the MS's activities achieving traceability. It utilizes the established trust relationships between mobile users and networks operators, and employs public key cryptography to ensure authenticity, integrity and confidentiality of the assigned pseudonyms. Apart from privacy, PRIPAY constitutes an efficient micropayment solution that enables the operator to aggregate and charge all the user's micropayments during a charging time period (i.e., monthly) within its mobile telephone bill. It is compatible with the employed technologies and minimizes the required typing and configuration effort by mobile users on the reduced-sized smartphones' screens, facilitating m-commerce.**

Keywords-micropayments; privacy; mobile operators; trusted third party.

I. INTRODUCTION

Due to the proliferation of mobile devices, web access by people on the move using their smart phones or tablets is likely to exceed web access from desktop computers within the next years [1]. As the technological capabilities of these devices are increasing, new services are also emerging. For instance, location based services (e.g., geosocial networking, proximity based recommendations, resource tracking, location-based mobile payments, etc.) are expected to flourish, since mobile devices are integrating Global Positioning System (GPS) [2] technology allowing location tracking.

This trend creates a favorable environment for mobile commerce (m-commerce) [3] to emerge and become a profitable market. However, for the proliferation of m-commerce two major issues need to be addressed. The first has to do with the fact that m-commerce poses various privacy threats, including behavioral profiling, tracking of money spent and visited websites, etc. These have also been acknowledged in the EU Directives [4], which identify specific privacy requirements. The second issue is that m-commerce, usually, involves micropayments, which are financial transactions with small or very small amount of money. In cases that the fixed processing cost is greater than the monetary amount of the transaction itself, micropayments become inefficient for the provided goods or services and the involved merchants or service providers (MorSPs) cannot develop their businesses. To overcome this fundamental limitation, new purchase and billing approaches are required [5].

An elegant solution that simultaneously addresses privacy and micropayment requirements is to allow mobile/wireless operators to act as trusted third parties (TTP) between the mobile/wireless subscribers equipped with mobile stations (MSs) and MorSPs. Subscribers already trust operators to maintain and process sensitive information that refer to them, including communication and contacts information, locations, service preferences, billing data, etc. For this reason, operators are obliged to follow specific security procedures and policies when capture, record, process, store and destroy such information. On the other hand, MorSPs are willing to trust mobile/wireless operators in order to charge them for the goods and services that MorSPs offer to their subscribers, ensuring micropayments. This is also strengthen by two facts: a) MorSPs are already subscribers of the mobile/wireless operators and, thus, they have already signed contracts or service level agreements between them; and b) the penetration of mobile/wireless subscriptions is very high, higher than the fixed internet counterpart, which means that mobile/wireless subscribers constitute a big candidate market for e-commence and e-services.

Driven by this observation, this paper proposes a privacy preserving architecture that enables micropayments or any other kind of financial transactions, through mobile/wireless operators in a secure and efficient manner. The proposed architecture, called PRIPAY, introduces a new entity to the mobile/wireless network, called pseudonym provider (PSP), which enables the operator to generate and assign to each requesting MS a different pseudonym, every time MS wishes to have access to a MorSP, achieving anonymity and unlinkability [6]. To efficiently verify that a generated pseudonym has not been previously assigned, a PSP uses a data structure based on bloom filters [7] to store the allocated pseudonyms. PRIPAY hides the real identity of an MS from a remote MorSPs, but, at the same time it allows the operator to track the MS's activities achieving traceability. Moreover, it includes a pseudonym assignment protocol that uses public key cryptography to ensure authenticity, integrity and

 ISBN: 978-1-61208-231-8

confidentiality of the assigned pseudonyms. Apart from privacy, PRIPAY constitutes an efficient micropayment solution that enables the operator to aggregate and charge all the subscriber's micropayment/financial transactions during a charging time period (CTP) (i.e., monthly) within its mobile telephone bill. It can be easily installed in the existing network infrastructure, since it is compatible with the employed technologies. Finally, it minimizes the required typing and configuration effort by mobile users on the reduced-sized smartphones' screens, facilitating m-commerce.

The rest of the paper is structured as follows. In Section 2, the proposed PRIPAY architecture is presented by analyzing its deployment in a representative networking scenario. The basic functionality such as the pseudonym generation and the pseudonym assignment protocol are also elaborated. Section 3 evaluates PRIPAY. Finally, Section 4 includes the related work, while Section 5 contains the conclusions.

II. THE PRIPAY ARCHITECTURE AND DEPLOYMENT

The proposed PRIPAY architecture can be mounted and operate in the most prominent mobile (i.e., 2G, 3G and 4G) and wireless technologies including, General Packet Radio Services (GPRS), Universal Mobile Telecommunication System (UMTS), Wireless Local Area Networks (WLAN), Worldwide Interoperability for Microwave Access (WiMax), and 3G-WLANs integrated networks. In this paper, we describe and analyze the deployment of PRIPAY in a 3G-WLAN integrated network [8], which is a representative scenario of the candidate technologies on which PRIPAY can be deployed (see Figure 1).

A. Network Architecture and Required Enhancments

The 3G part of the integrated 3G-WLAN network [8] architecture mainly includes: a) the Radio Network Controller (RNC) that is responsible for the radio resource management and controls the wireless transceivers (Node Bs); b) the Serving GPRS Support Node (SGSN) that undertakes packet routing and transfer, mobility management, location management and logical link management; c) the Gateway GPRS Support Node (GGSN) which is responsible for the interworking between 3G and external networks (e.g., Internet), as well as for IP allocation to MSs; and d) the Home Location Register/Home Subscriber Server (HLR/HSS) which is a database that contains subscription, authentication and billing information for mobile users. On the other side, the WLAN technology that participates in the 3G-WLAN architecture consists of: i) the Authentication Authorization and Accounting (AAA) server which retrieves subscription and authentication information from the HLR/HSS and validates the authentication credentials that MSs provide; ii) the Packet Data Gateway (PDG) which provides access to external networks; and c) the WLAN Gateway that connects WLAN access points with the AAA server and PDG.

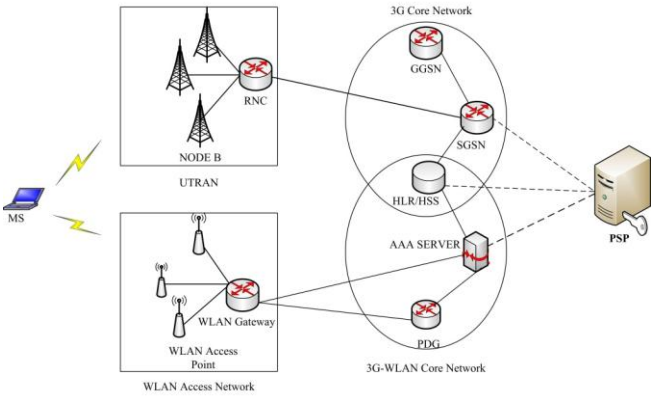

Figure 1. PRIPAY deployment in a 3G-WLAN integrated network

The key functional component of PRIPAY is PSP, which generates and assigns pseudonyms to the requesting MSs in a secure and efficient manner. In the considered 3G-WALN network architecture, PSP is placed within the core network of the mobile/wireless operator, which is deployed on a private/controlled network environment interconnected to the public Internet. This network and the included entities are protected from the security threats of the public Internet by establishing specific security measures (e.g., Firewalls, Intrusion Detection Systems, Virtual Private Networks, etc.) and following definite security policies.

PSP interfaces and interacts with SGSN and the AAA server, in order to make available the PRIPAY functionality and the provided services to the underlying networks and their subscribers. SGSN and the AAA server play similar roles in managing mobile/wireless subscribers in an integrated 3G-WLAN network architecture, where the subscribers wish to have access to external networks and services. PSP also interfaces to HLR/HSS, which records every assigned pseudonym to a specific subscriber for accessing an explicit remote MorSP. The interfaces between PSP and the core network components (i.e., SGSN, HLR/HSS and the AAA server) are based on the Mobile Application Part (MAP) of the SS7 protocol stack, where some new message exchanges need to be developed, as shown in Section II.C. As the three network nodes already execute the MAP protocol, the required enhancements have minimum impact on the existing infrastructure.

Except for the enhancements on the interfaces, PRIPAY requires some extensions to the existing HLR/HSS database scheme. More specifically, for each subscribed user the new extended scheme will include a list of pseudonyms that have been assigned to it, together with the MorSP that each pseudonym has been issued as well as the time of assignment. These entries will be updated by PSP when a new pseudonym is generated, as mentioned below. Finally, the operation of PRIPAY requires from each of the involved parties (i.e., mobile/wireless operators and the participating MoSPs) to possess a valid public key certificate.

B. Pseudonym Generation and Assignment

An essential requirement of PRIPAY is that within a particular CTP a specific pseudonym should be used only

 ISBN: 978-1-61208-231-8

once, and only from one MS. In this way, the architecture achieves unlinkability between different actions of the same MS, as well as ensures secure charging in cases of micropayment or financial transactions. For this reason, PSP maintains a bloom filter to keep record of all the generated pseudonyms and efficiently check whether a pseudonym has been previously assigned. As bloom filters have been applied and analyzed extensively in many networking applications [8], we highlight only the basic functionality of them.

A bloom filter is a data structure for representing a set S $=\{x_1, x_2, x_3,\ldots,x_n\}$ of n elements by an array of m bits. Initially, all bits of the array are set to 0. A bloom filter uses k independent hash functions $h_1, h_2, h_3,\ldots,h_k$ with range $\{1,2,3,\ldots,m\}$. To insert a new element x in the set S, the bits $h_i(x)$ are set to 1 for $1 \leq i \leq k$. To check if an element y belongs to S, we check whether all $h_i(y)$ are set to 1. If not, then y is not a member of S. If all $h_i(y)$ are set to 1, it is assumed that y is in S. However, this may be wrong with some probability *p*, due to collusions of the hash functions employed. Hence, a bloom filter may yield a false positive, where it outputs that an element x is in S, even though it is not. Figure 2 depicts a bloom filter with k=3 hash functions that inserts the x_1 and x_2 elements and checks whether the y_1 and y_2 elements belong to this set. The key advantage of bloom filters lies in the fact that the time needed either to add new elements or to check whether an element is in the set, is a fixed constant O(k) (k is the number of hash functions employed), independent of the number of elements already in the set.

In PRIPAY, the assigned pseudonyms represent the set of elements S of the bloom filter. When a new pseudonym is generated, PSP uses the bloom filter to efficiently check whether the pseudonym is already in the set. If it is (i.e., this means that the pseudonym has been already assigned to an MS), PSP generates a new one, and, then, checks whether the new pseudonym is included in the set. This procedure continues until PSP generates a pseudonym that is not included in the bloom filter (i.e., means that it has not been assigned yet). Next, PSP inserts this pseudonym into the bloom filter (i.e., sets the appropriate locations in the array of the bloom filter equal to 1). The operation of PRIPAY continues until its runtime reaches the predefined CTP value. Then, the operator processes the PRIPAY records included in HLR/HSS (i.e., International Mobile Subscriber Identities - IMSIs, pseudonymous, accessed MorSP, access time) and provides charges to the subscribers involved in micropayments or financial transactions. The charges are completed and verified by using the related expenses that the accessed MorSPs have requested from the operator. The recorded and processed data can be stored in a secure place for a certain period of time (i.e., one or two years), according to the operator's policies and the government regulations. Having finished the processing and storing of PRIPAY records, HLR/HSS resets the assigned pseudonyms (and the related information), PSP initializes the employed bloom filter by setting all bits with 0s and both of them continue operation for another CTP.

As mentioned previously, the main drawback of a bloom filter is the occurrence of false positives, where it erroneously indicates that an element belongs to the considered set, but, actually, it does not. However, false positives do not have any impact on the functionality of PRIPAY and impose some minor effects on its performance. More specifically, in case of a false positive, PSP aborts a fresh pseudonym, generates a new one and checks again if it is included in the maintained bloom filter. The cost of this operation is O(k), which is constant and does not affect the performance of the architecture. In addition, in every CTP, PRIPAY resets the bloom filter reducing the occurrence of false positives.

The probability *p* of a false positive in a bloom filter is given by the formula $p \approx (1 - e^{-kn/m})^k$, where k is the number of hash functions, m is the number of bits in the array of the bloom filter, and n is the number of elements in the bloom filter. It is evident that the probability of a false positive *p* reduces when the number of bits m is increased or the number of elements n is reduced. Moreover, the optimal value of k is given by k= ln2(m/n). In PRIPAY, the number of elements n (i.e., the assigned pseudonyms) is equal to the total number X of the privacy service requests, performed in a CTP. To estimate the storage cost of a bloom filter implementation (i.e., the number of bits m) in the PRIPAY architecture, we consider three representative values of X: i) $X= 10^4$, ii) $X= 10^5$, iii) $X= 10^6$. In all cases, we keep an optimal value of k= ln2(m/n) = 17 and a small value *p* (i.e., $p=10^{-5}$) to minimize false positives. As shown in Table I, the storage cost is very low in all three cases and even for $X=10^6$, the storage cost is approximately 3MB, which is a negligible cost. Based on this finding, it can be inferred that if the value of X increases (e.g., due to an increase of the total number of subscribers or of the privacy service requests), the mobile operators can easily increase the storage cost to preserve the probability of false positives very low.

TABLE I. MEAN NUMBER OF PRIVACY REQUESTS IN A CTP VS. STORAGE COST (K=17 AND P=10^{-5})

Number of Privacy Requests X	Storage Costs
10^4	29,25
10^5	292,51
10^6	2925,12

C. Pseudonym Assignment Protocol

The proposed pseudonym assignment protocol of PRIPAY is performed when an MS wants to have anonymous access to a remote MorSP (see Figure 3). In this paper, we analyze the protocol execution over 3G, omitting the rest technologies (2G, WLAN, WiMAX and 3G-WLAN) that are deployed in a similar way. The protocol functionality and execution are independent of the specific features of the underlying mobile/wireless technology, facilitating maximum transparency and portability. For the analyzed 3G scenario, the network entities that participate are: i) MS, ii) SGSN, iii) PSP, iv) HLR/HSS, v) GGSN and vi) MorSP. Prior to the protocol execution, it assumed that MS has been authenticated and attached to the network. Moreover, we assume that there is a pre-established secure channel between the MorSP and the 3G network based on a Service Layer

 ISBN: 978-1-61208-231-8

Agreement (SLA). The proposed protocol is called before the Packet Data Protocol (PDP) activation procedure, which creates a context that contains all the service parameters of a connection to an external network by means of end-point addresses, quality of service, etc.

The pseudonym assignment protocol execution is triggered (step 1) by a Privacy Service Context Request message that MS sends to SGSN, indicating the mobile subscriber's wish for traceable anonymous access to a remote MorSP (e.g., ssl.ds.unipi.gr). Upon receiving this message, SGSN retrieves the permanent identity of MS (i.e., IMSI) and sends it (i.e., Privacy Service Request message) together with the MorSP address to PSP (step 2). The latter generates a new pseudonym for the specific subscriber, as described in section II.B, and, then, sends it together with the subscriber's IMSI and the remote MorSP address to HLR/HSS for updating the operator database (Privacy Update Request message) (step 3). HLR/HSS confirms updating by replying with a Privacy Update Confirm message. After that (step 4), PSP obtains the digital certificate of the remote MorSP, which is required for providing authentication and integrity between the mobile operator and MorSP as well as encrypting specific fields in the communication between MS and MorSP, as presented below.

At step 5, PSP initializes a digital signature and encryption process as follows: Let M denote the generated pseudonym of MS. PSP computes a message digest h(M) of the pseudonym, using a hash function (e.g., SHA1), and, then, produces a digital signature of the pseudonym $DS=E[KP_{PSP}, h(M)]$, using the computed h(M) as well as the private key of PSP (i.e., KP_{PSP}), (i.e., PSP represents the mobile operator). The produced digital signature, which authenticates the issuing mobile operator and provides integrity to the generated pseudonym, is concatenated with M, creating a new value N (i.e., N= DS||M). PSP encrypts N using MorSP's public key (i.e., KU_{MorSP}), obtained from the digital certificate of MorSP, as $C=E[KU_{MorSP}, N]$ ensuring its confidentiality. Next, PSP sends to GGSN a Privacy Context Request that includes C and the MorSP address to GGSN. The latter sends to PSP a Privacy Context Confirm message indicating the successful reception of C and MorSP address. At step 6, PSP sends a Privacy Service Response message to SGSN that includes the MorSP's address. The latter forwards the MorSP address to MS in a Privacy Service Context Response message.

In step 7, a primary PDP context is activated, which creates internal service tunnels within the mobile network for the data flow and assigns an external IP address (i.e., static or dynamic) to MS. In the same step (i.e., step 7), GGSN sends C to MorSP through a pre-established secure channel (e.g., a VPN). Next, MorSP decrypts C using its private key (i.e., KP_{MorSP}) to obtain N, and, then, verifies the digital signature DS (N= DS||M), using the PSP public key (i.e., KU_{PSP}). If the digital signature DS is not valid, MorSP rejects the provided pseudonym. Otherwise, (i.e., in case of a successful verification of DS), MS may have anonymous access to MorSP using the pseudonym M. It is important to mention that if MS wants to have access to another MorSP, a new pseudonym will be requested and a new primary PDP context will be activated in which a new IP address will be allocated to MS.

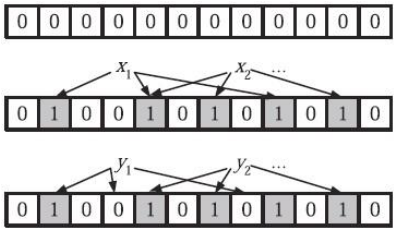

Figure 2. An example of a bloom filter taken from [8]. The filter begins as an array of all 0s. Each item in the set x_i is hashed k=3 times, with each hash yielding a bit location; these bits are set to 1. The element y_1 is not in the set, since a 0 is found at one of the bits. The element y_2 is either in the set or the filter has yielded a false positive.

III. EVALUATION

In this section, we attempt to evaluate the proposed privacy architecture by analyzing its advantages and possible drawbacks. The main objective of PRIPAY is to ensure privacy to mobile users, while enabling anonymous micropayments through the mediation of mobile/wireless operators. The identity or any other personal information of users, such as credit card details etc., is never disclosed to anyone, whilst MorSPs receive only verifiable pseudonyms. Every time a user accesses a remote MorSP, it is assigned to it a different pseudonym, guaranteeing unlinkability. Therefore, the accessed MorSP cannot link preferences and behaviors of the user or track its location. To avoid using the same pseudonym for a second time in a particular CTP, PRIPAY utilizes a bloom filter that allows PSP to efficiently verify that a new generated pseudonym has not been previously assigned. The time needed for this operation is a fixed constant O(k), independent of the number of elements (i.e., assigned pseudonyms) already in the set. Although pseudonym verification may present false positives, their probability p can be relatively low with no functional implication to PRIPAY and negligible impact on its performance (i.e., PSP has to repeat the procedure of generating a new pseudonym and verifying its freshness using the bloom filter).

The proposed architecture allows MS to use one Radio Resource Control (RRC) connection and activate multiple primary PDP contexts that each of them employs a different IP address. In this way, MS may access several MorSPs (using the same RRC), not only with a different pseudonym, but also with a different IP address. If MS uses the same IP address to access different MorSPs, they may collaborate each other compromising unlikablity. An alternative solution would be MS to drop the RRC connection and establish a new one in order to obtain a new IP address, but this may deteriorate the overall network performance and the usability of PRIPAY.

PRIPAY incorporates a set of security features (e.g., digital certificates, public key cryptography, digital signature, etc.) in order to protect its operation and prevent the occurrence of malicious actions. Towards this direction, the generated pseudonyms are digitally signed using the issuer's (i.e., mobile operator) private key and encrypted

 ISBN: 978-1-61208-231-8

using the remote MorSP public key. In this way, we achieve non-repudiation and security against misbehaving MorSP. Moreover, since there is a pre-established secure channel between the mobile operator and the MorSP, the conveyance of C over the public Internet does not pose any security risk, such as replay attacks, man-in-the-middle attacks or modification in the exchanges messages. The generated pseudonyms of a mobile operator, which have been assigned to its subscribers for accessing remote MorSPs during a CTP, are stored in the HLR/HSS database. HRL/HSS already stores sensitive users' (i.e., identities, locations, billing data, etc.) and network information (i.e., authentication information) and, thus, all the security measures and procedures required to protect it and the included information are in place. Hence, no extra security measure is required to protect the generated pseudonyms from internal or external attacks. Moreover, any information exchange between the mobile operator and remote cooperative MorSPs that refer to pseudonyms or charging will be carried encrypted out using public key cryptography.

From the viewpoint of m-commerce, the proposed architecture constitutes an efficient solution for micropayments, since it delegates the billing process to mobile operators. Each operator has already established a micropayment platform to charge mobile subscribers for the network usage, as charges mainly refer to an amount of short duration phone calls, short messages service (SMS) and small volume data sessions. Thus, a mobile operator that installs PRIPAY, may aggregate and charge carried micropayments together with the bills of mobile phones, every CTP. The mobile operator is also able to verify and trace all the used pseudonyms (i.e., traceability) charged by cooperative MorSP within a specific CTP, because the HLR/HSS database is extended to store the assigned pseudonyms for each registered IMSI as well as the remote MorSPs that have been issued for.

The delegation of charging to mobile operators enable micropayments and, in general, financial transactions of mobile subscribers with remote MorSP, without the need of credit cards or specialized accounts (e.g., paypal). This is especially useful for users that do not like credit cards (or specialized accounts) or they don't want to use them either for security reasons or privacy considerations. Moreover, using PRIPAY, the mobile users do not have to complete time-consuming and error prone forms on the reduced-sized screens of MSs.

The deployment of the proposed architecture does not impose extensive modifications to the current technology and existing infrastructure of mobile/wireless operators. It requires: a) the introduction of PSP within the core network of the operator which generates and assigns pseudonyms; b) the development of four new MAP-based messages that are exchanged between SGSN, PSP and HLR/HSS; c) the extension of the HLR/HSS database scheme in order to include the assigned pseudonyms for each IMSI as well as the remote MorSP for which each pseudonym has been issued for; and d) the development of a lightweight application that resides at MS and enables the user to initiate PRIPAY as well as the related communication messages with SGSN. Therefore, the PRIPAY installation and operation do not requires much investment from the operators. On the other hand, PRIPAY will increase the operators' income by increasing the network usage and the related traffic as well as returning a small share of the PRIPAY turnover to them.

Finally, a possible drawback of PRIPAY has to do with the fact that the activation of multiple primary PDP contexts leads to the allocation of multiple IP addresses. This may cause an administrative problem to the operator, as it may exhaust the available IP addresses at GGSN. However, it has to be mentioned that this is enabled only when an MS wants to have anonymous access to several MorSP, simultaneously, using the same RRC connection, which is not the normal case.

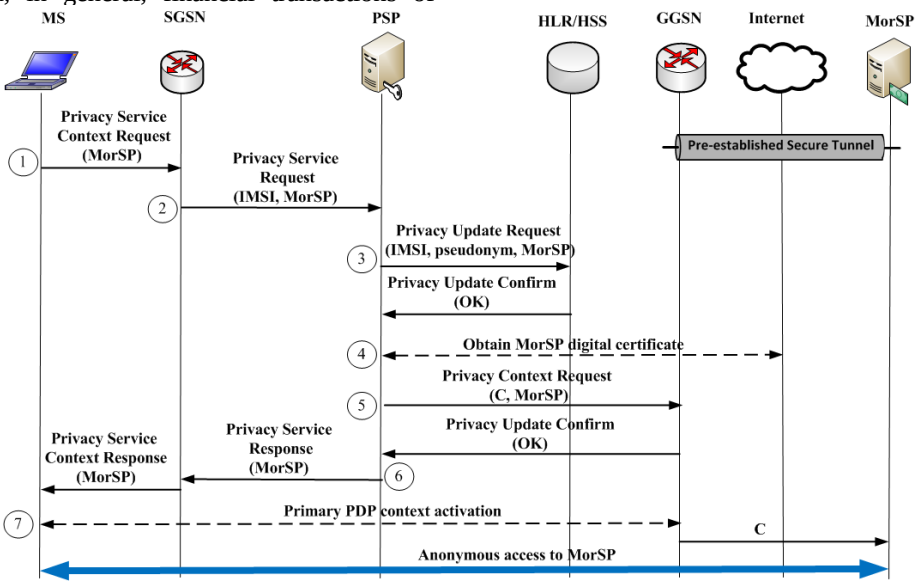

Figure 3. Pseudonym assignment protocol

IV. RELATED WORK

There is a rather limited literature that deals with privacy in mobile/wireless networks. Bessler et al. [9] have proposed a privacy preserving architecture that ensures presence and location privacy in the context of web services, specified by the Parlay X standard. In this architecture, a server, called Privacy Service (resides within the mobile/wireless network), generates pseudonyms for the registered MSs. In order to achieve authentication and authorization, keyed hash chain values are employed between MSs and the Privacy Service. Although this architecture offers an adequate level of privacy, its main drawback is that the involved MSs should execute cryptographic algorithms increasing energy consumption. To address this limitation, Ajam [10] has proposed to incorporate within the deployed Parlay X gateway a privacy web service, which is responsible for managing and ensuring the privacy of MSs. This privacy web service uses a pseudonym database to map pseudonyms to real identities or subscribers' numbers. The main limitation of this architecture is that it provides privacy only for services that are based on OSA/Parlay.

Gritzalis et al. [11] proposed a mechanism called Pythia that ensures privacy in e-commerce and offers both traceability and anonymity. The main idea of this mechanism is that the sender of a message can be authenticated at the receiver, without the latter knowing the former's identity. However, the sender reveals its identity in an intermediary, in order to ensure traceability. This mechanism uses a cryptographic token, which is distributed to the involved users through a TTP. As the employed token is not protected for confidentiality and data integrity, the employment of an additional general purpose security mechanism like the SSL protocol is required increasing the overall operation cost.

Finally, there are some third-party commercial micropayment systems that leverage micropayment transactions through mobile operators [12], [13]. Initially, service and cooperation agreements are required between the micropayment providers and i) the mobile/wireless network operators that will allow their subscriber to use the provided payment systems; and ii) MorSPs that accept payments through the deployed third-party micropayment systems. During a transaction, a mobile subscriber sends its mobile phone number to a MorSP, and the latter sends back to the subscriber's mobile phone an SMS including a random number. The subscriber must submit this number back to MorSP to prove that it is the legitimate owner of the mobile phone number. In this way, all payments made by the mobile subscriber are charged to its mobile phone bill by its operator. Although such systems enable micropayments, they do not offer privacy services, fact that MorSPs may take advantage for their own purposes. For example, MorSPs may use the collected phone numbers for advertisement purposes.

V. CONCLUSIONS AND FUTURE WORK

PRIPAY leverages the trust relationship between mobile users and mobile operators offering anonymous and secure micropayments. Each time a user accesses a remote MorSP, it is assigned a different pseudonym, guaranteeing anonymity and unlinkability. Thus, the accessed MorSP cannot link preferences/behaviors of the user or track its location. The generated pseudonyms are signed using the mobile operator's private key and encrypted using the remote MorSP public key. Thus, their conveyance over the Internet does not pose any security risk. PRIPAY eliminates the need of credit cards or specialized accounts (e.g., paypal), a feature especially useful for users that do not want to use credit cards or specialized accounts for security or privacy considerations. The charging process of micropayments can be easily performed, since the mobile operator can aggregate and charge carried micropayments along with the bills of mobile phones in every CTP. The deployment of the proposed architecture does not impose extensive modifications in the existing infrastructure of mobile/wireless operators. As a future work, we plan to perform simulations to estimate and evaluate the performance (i.e., overhead, possible delays and the energy consumption at the level of mobile devices) of the pseudonym assignment protocol of PRIPAY.

REFERENCES

[1] S. Teltscher and S. Parkes, ITU, http://www.itu.int/newsroom/press_releases/2010/06.html [retrieved: September 2012]

[2] I. A. Getting, "The Global Positioning System," IEEE Spectrum, Vol. 30, pp. 36-47, December 1993.

[3] U. Varshney, R. J. Vetter, and R. Kalakota, "Mobile e-commerce: a new frontier", IEEE Computer, Vol. 33, No. 10, pp. 32-38, October 2000.

[4] European Parliament, Directive 2006/24/EC of the European Parliament and of the Council, March 2006.

[5] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – v0.34", Aug. 2010.

[6] M. V. Tripunitara and T. S. Messerges, "Resolving the micropayment problem", IEEE Computer magazine, Vol. 40, No. 2, pp. 104-106, 2007.

[7] A. Broder and M. Mitzenmacher, "Network applications of bloom filters: a survey", Internet Mathematics, Vol. 1, No. 4, pp. 485-509, July 2003.

[8] 3GPP TS 23.234 (v11.0.0), "3GPP system to WLAN interworking; system description", Release 11, Sept. 2012.

[9] S. Bessler and O. Jorns, "A privacy enhanced service architecture for mobile users", in Proceedings of the third IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2005), pp. 125 - 129, Hawaii, USA, March 2005.

[10] N. Ajam, "Privacy based access to Parlay X location services", in Proceedings of the Fourth International Conference on Networking and Services (ICNS 2008), pp. 204-206, Guadeloupe, France, March 2008.

[11] D. Gritzalis, K. Moulinos, J. Iliadis, C. Lambrinoudakis, and S. Xarhoulakos, "Pythia: towards anonymity in authentication", in proceedings of the IFIP 16th International Conference on Information Security (SEC 2001), pp. 1-17, Paris, France, June 2001.

[12] Mcoin mobile payments, http://www.mcoin.com [retrieved: September 2012]

[13] Zong a paypal service, http://www.zong.com [retrieved: September 2012]

 ISBN: 978-1-61208-231-8