University of Piraeus

Department of Digital Systems

Post graduate Programme in Digital Systems Security

Master Thesis

Privacy Techniques in Fourth Generation Heterogeneous Networks

Dimitris Gkikakis

Student No: MTE 1046

Supervising Professor: Christos Xenakis

Piraeus

March 2012

This thesis is dedicated to the memory of my grandmother

ΔΕΝ ΕΧΕΙ ΤΥΠΩΘΕΙ

Acknowledgements

My sincere thanks to Assistant Professor Christos Xenakis and the Postdoctoral researcher Christoforos Ntantogian, my project supervisors, for their valuable input, guidance and support.

Thanks to all the lecturers and students at the Postgraduate Programme for sharing their knowledge.

Special thanks to my family and friends for their patience, ongoing support and encouragement throughout the years.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΕΡΙΛΗΨΗ

Η ραγδαία αύξηση πώλησης κινητών συσκευών smartphones και η ολοένα μείωση των τιμών του mobile internet έχει κάνει δημοφιλή τη χρήση mobile Internet από Smartphones. Το επόμενο βήμα αναμένεται να είναι η πολλά υποσχόμενη ενοποίηση των κινητών δικτύων (3G) με τα δίκτυα WLAN και WIMAX ώστε να προκύψουν τα ετερογενή δίκτυα 4^{ης} Γενιάς. Η διαρροή προσωπικών πληροφοριών του χρήστη σε κακόβουλους είναι μία πτυχή, η οποία έχει μελετηθεί στο συμβατικό Internet, όχι όμως στο mobile Internet. Η διπλωματική αυτή εργασία έχει ως στόχο να πληροφορήσει τον αναγνώστη για τις υπάρχουσες τεχνικές Ιδιωτικότητας και να αναγνωρίσει τους κινδύνους Ιδιωτικότητας στο mobile Internet σε ετερογενή δίκτυα 4^{ης} Γενιάς. Τέλος σε αυτή τη διπλωματική εργασία προτείνουμε μία αρχιτεκτονική, η οποία θα προστατεύει σε υψηλό βαθμό την Ιδιωτικότητα του χρήστη.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Abstract

Mobile phones have become a part of our everyday life. Their computational power is increased in a daily basis. We live in smart phones era and mobile networks support data exchange in affordable prices. The vision of the convergence between mobile networks and broadband networks is too close in our future. The next step to be expected is the promising convergence between mobile networks (3G), WLAN and WIMAX, named as heterogeneous 4G networks. User's information disclosure is a subject that has already been studied in conventional Internet, but not in Mobile Internet. The aim of this thesis is to inform about the Privacy techniques that already exist and identify Privacy threats in Mobile Internet. Finally, we propose an architecture that aims to protect the user's Privacy.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Contents

List of Figures

UNEDITED DRAFT

1. Introduction

Mobile phones have become a part of our everyday life. Their computational power is increased in a daily basis. We live in smart phones era and mobile networks support data exchange in affordable prices. The vision of the convergence between mobile networks and broadband networks is too close in our future.

On the one hand, the smart phone market's expansion and the affordable prices of mobile internet for their holders, has increased the phenomenon of mobile surfing. On the other hand, there are users who want to be able to use such services anonymously or they don't want to be disturbed (the right to be left alone) for example by spam. Privacy seems to be a problem that users have begun to take into serious account. Research concerning this field applies only onto the internet through conventional ISPs or location based privacy.

According to our view the definition of privacy, for the ICT field, was given by Alan Westin [1] in 1967: Privacy is *"the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others"*. The definition above describes the way that users ought to control their data in communication. Privacy enhancement technologies (PETs) [2] name four basic ISO requirements: anonymity, pseudonymity, unlinkability and unobservability. These properties can be achieved but they are not suitable for services that require user's identification. Another property that has appeared lately is location privacy. Beresford and Stanjano [3] define location privacy as *"the ability to prevent other parties from learning one's current or past location"*. The term of location privacy was introduced in ICT through the use of mobile networks and became stronger with the use of Wi-Fi.

European Union is also concerned about privacy in Information and Communications Technology (ICT). This is proved by the Directives that have been issued, some of which are the following: the protection of individuals with regard to the processing of personal data and on the free movement of such data [4], the processing of personal data and the protection of privacy in the electronic communications sector [5], universal service and users' rights relating to electronic communications networks and services [6], the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [5].

Recently a directive was issued concerning the modification, firstly of Directive 2002/22/EC [6] for universal services and users' rights in electronic communication networks and services and secondly of Directive 2002/58/EC [5] for the process of personal data and the protection of privacy in the electronic communications sector and thirdly of Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. All these have been included in the Legal Framework of each country that is a member of the European Union. A law that has great value for our work and is worth mentioning was

issued in Greece (Law 3783/2009) and states the following: "*the provider of publicly available electronic communications services shall, to the extent technically feasible and permitted by this law, allow payment for these services anonymously or under a pseudonym. In case that the technical feasibility of anonymous and pseudonymous payment for those services is of doubt, consulted the National Telecommunications and Post Commission.*"

1.1. Goals and Motivations

The main goal of this thesis is to present the Privacy techniques that are implemented in different fields of electronic world and the upcoming mobile networks. Specifically, we present techniques from all kind of services, such as surfing, communications, e-commerce and entertainment, that a user can enjoy at the Internet.

The primary motivation of this thesis is to discover the privacy threats that mobile Internet introduces. There are several malicious individuals or organizations wanting to collect users' data in order to gain more revenues. We present these threats and based on them we present our proposal in the field of fourth generation heterogeneous networks.

1.2. Structure

The second chapter provides some information about the privacy techniques that have been created and implemented over the last twenty years. It tracks down Privacy techniques to its early days to examine its basic functions all the way up from the conversional Internet to the Location Based Services (LBS) that are rapidly being increased. In section 3, we present our proposed model. We discuss about the architecture of UMTS, the architecture of B3G networks, the role of all the components and how they are used in our model. In addition, we implement a new component that covers some new functions. Furthermore, we present a comprehensive signaling for UMTS architecture. In section 4, we present the security analysis, the benefits and drawbacks of our proposed model.

2. Privacy Techniques

2.1. Privacy Enhancing Technologies

PETs are techniques that have been developed in order to protect the user's privacy. PETS appeared in 90's and they try to solve the major problem in privacy, which is the number of information a website can gather from a connection with a client. In 1995, an experiment took place. Justin Boyan created a demonstration web page in order to show how much information a web site can gather from a user's visits. The user's email address, geographical location, operating system and web browser, were some of them.

PETs are divided in two categories: The first category consists of techniques that achieve the user's anonymity or pseudonymity (such as anonymizer, lpwa) and the second category consists of techniques that are based on privacy policies (P3P,

TRUSTe). The Anonymizer [7] belongs to the first category. The main idea of this mechanism is very simple. A user is connected with a third party web site (http://www.anonymizer.com) that acts as a middleman between the user and the site to be visited. If he wants to visit www.ds.unipi.gr, he will not create a direct connection, but he will be connected with www.anonymizer.com and will ask from it to redirect him to www.ds.unipi.gr without revealing any personal information. The Anonymizer requests a connection to the site, the site responses and then forwards the traffic to the user. The benefits from this technique is that the Anonymizer does not reveal the user's IP address and removes some headers like "User agent", "from", "referer", filters out of java applets and JavaScript which may compromise anonymity. The drawback of the Anonymizer is that privacy is based on the trust between the user and the Anonymizer. The Anonymizer gets much information about the user. If the Anonymizer acts maliciously, all of the user's information can be given to interested parties.

LPWA (Lucent Personalized Web Assistant) [8] enables users to enjoy personalized services on the Web while preserving the user's privacy. The problem that LPWA was called to solve was the number of information a web site needs in registration and the use of e-mail. LPWA generates a persona for every user. This is a generator of the user's identities every time a user fills registration forms. The user inserts his identity and password in LPWA site once and after that LPWA generates credentials for him in every web site. In addition, LPWA generates e-mail addresses for the user. The incoming messages to these e-mail addresses are forwarded to user's real email address. In this way, LPWA protects the user from junk e-mails. Web sites often give emails to marketers or spammers. When the user thinks that an e-mail address receives many spam e-mails, he can block the suspicious e-mail address that has been generated by LPWA. Finally, LPWA alleviates the risk of account compromise. In addition, most of the users use the same password for multiple web sites. If a malicious user compromises one user's account then all accounts can be compromised. The drawbacks of this mechanism is that privacy is based on the trust to the LPWA, the connection between the user and LPWA can be easily eavesdropped or modified, the performance of surfing is low and LPWA does not filter Java and JavaScript applications.

Crowds [9] is another PET, based on the fact that a big number of users want to protect their privacy and they create a "crowd". The user's actions are "hidden" in the actions of the rest users that belong to the crowd. In this way, anonymity is achieved. A crowd consists of a number of jondos and the path of routing is calculated by an algorithm, which creates virtual paths. These paths change after a number of requests. After that, a new path is calculated. The communication between jondos is encrypted with a symmetric key. Crowds' disinclines from IP address recording and eavesdroppers who monitor the user's messages.

Onion routing [10] is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes called onion routers. Like someone unpeeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message

to the next router where this is repeated. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message.

The idea of onion routing (OR) is to protect the privacy of the sender and recipient of a message, while also providing protection for message content as it traverses a network.

Onion routing accomplishes this according to the principle of Chaum's mix cascades: messages travel from source to destination via a sequence of proxies ("onion routers"),which re-routes messages in an unpredictable path. To prevent an adversary from eavesdropping on message content, messages are encrypted between routers. The advantage of onion routing (and mix cascades in general) is that it is not necessary to trust each cooperating router; if any router is compromised, anonymous communication can still be achieved. This is because each router in an OR network accepts messages, re-encrypts them, and transmits to another onion router. An attacker with the ability to monitor every onion router in a network might be able to trace the path of a message through the network, but an attacker with more limited capabilities will have difficulty even if he or she controls routers on the message's path.

Onion routing does not provide perfect sender or receiver anonymity against all possible eavesdroppers—that is, it is possible for a local eavesdropper to observe that an individual has sent or received a message. It does provide for a strong degree of *unlinkability*, the notion that an eavesdropper cannot easily determine both the sender and receiver of a given message. Even within these confines, onion routing does not provide any guarantee of privacy; rather, it provides a continuum in which the degree of privacy is generally a function of the number of participating routers versus the number of compromised or malicious routers.

A *routing onion* (or just *onion*) is a data structure formed by 'wrapping' a plaintext message with successive layers of encryption, such that each layer can be 'unwrapped' (decrypted) like the layer of an onion by one intermediary in a succession of intermediaries, with the original plaintext message only being viewable by at most:

1. the sender
2. the last intermediary
3. the recipient

If there is end-to-end encryption between the sender and the recipient, then not even the last intermediary can view the original message; this is similar to a game of 'pass the parcel'.

An intermediary is traditionally called a *node* or *router*.

To create and transmit an onion, the following steps are taken:

1. The sender picks nodes from a list provided by a special node called the *directory node* (traffic between the sender and the directory node may also be encrypted or otherwise anonymised or decentralised); the chosen nodes are ordered to provide a path through which the message may be transmitted; this ordering of the nodes is called a *chain* or a *circuit*.

2. Using asymmetric key cryptography, the sender uses the public key of each chosen node to wrap the plaintext message in the necessary layers of encryption: The public keys are retrieved from an advertised list or by on-the-spot negotiation for temporary use and the layers are applied in reverse order of the message's path from sender to receiver; with each layer, the client includes information for the corresponding node regarding the next node to which the onion should be transmitted.
3. As the onion passes to each node in the chain, a layer of encryption is peeled away by the receiving node (using the private key that corresponds to the public key with which the layer was encrypted), and then the newly diminished onion is transmitted to the next node in the chain.
4. The last node in the chain peels off the last layer and transmits the original message to the intended recipient.

Using this approach means each node in the chain is ideally aware of only two other nodes:

1. the preceding node from which the onion was transmitted.
2. the proceeding node to which the onion should next be transmitted.

The peeling away of each layer of the onion makes it difficult or impossible to track the onion without compromising a significant number of nodes.

As we already mentioned the second category consists of mechanisms that are based on privacy policy. In P3P [11] user states the information that he wants to reveal in a web site. From the other side, web site states the information that wants to gather from users. XML compares these two statements. If a web site wants to gather information that user is willing to reveal there is an agreement and the communication with the SP can go on. Otherwise, the user is informed about the information that SP wants to gather and he has not stated in the list with the information that wants to be revealed in order to decide if he wants to reveal them or to quit the web site.

TRUSTe [12] is another solution that is based on certification. Web sites are called to have a privacy policy for users' information and allow users to correct or change their personal information in order to be certified by TRUSTe. Some of criteria to get this certification are users' awareness about the information that are collected and the parties that these information can be revealed. In addition, the option of users to allow or block the distribution of information to third parties. Moreover, there should exist security measures in order to protect personal information and user's allowance to correct or update their information. The result of this certification is to ensure customers for the way that websites handle their personal information.

2.2. E-IDs

Another research area where privacy has been considered as one of the greatest requirements is the area of e-IDs. This area has a characteristic that makes it unique. Each country’s privacy design depends on its culture. The first country that introduced e-IDs was Estonia in 2002. In estonian e-ID [13] anybody can read the user's personal information. In addition, card's holder is exposed in basic privacy threats like behavioral profiling and location tracking.

The first card that implemented measures for privacy protection was the Belgian e-ID (belpic) [14]. Personal information is well protected, but card's holder is exposed to threats like behavioral profiling and location tracking.

German e-ID [15] is the most recent. This e-ID has taken privacy as top level requirement. Personal information is protected by a PIN. Only certified SPs can be connected to e-ID and after typing the PIN card's information are extracted. Behavioral profiling and location tracking are limited. Measures like block of forwarding information and the use of a different pseudonym for each SP protect from these attacks.

2.3. Voice over IP

Voice over IP (VoIP) is the modern technology for phone calls. This technology is based on packet switched networks. VoIP consists of two protocols. Session Initiation Protocol (SIP) that is responsible for establishing and controlling call sessions. The second protocol is Real-time Transport Protocol (RTP), which transfers data (e.g. voice).

Packets in SIP transfer some information like the identities of participants. Hiding these identities would be identical for privacy. There are three scenarios that a participant would wish be anonymous:

i. A participant wants to send a message and hide his identity from the final destination(s) while still communicate his identity to one or more intermediaries

ii. send a message and hide his identity from some or all intermediaries, but still communicate his identity to the final destination(s)

iii. send a message and hide his identity from both intermediaries and final destination(s)

The result of the anonymous communication is that the parties in question would be unable to call the anonymous party in the future.

It is important to discuss the reasons that a user would like to hide his identity

i. User may want to communicate with a particular party without revealing their identity in order to impart information with which they would not like to be associated.

ii. Users might fear that the exposure of their identity or personal information to some networks or destinations will make them a target for unsolicited advertising, legal censure or other undesirable consequences.

iii. Users might want to withhold from participants in a session the identity by which they are known to network intermediaries for the purposes of billing and accounting.

There are three ways to enhance user's privacy:

i. Add values in headers that correspond in privacy enhancement.

ii. Request more privacy services from the network.

iii. Use encryption in order to ensure confidentiality of headers and data.

Privacy starts from user. The bulk of steps that are necessary for hiding sender's personal information are sender's responsibility.

The following SIP headers can reveal sender's identity. These headers are: From, Contact, Reply-to, Via, Call-Info, User-agent, Organization, Server, Subject, Call-ID, In-Reply-To and Warning.

The first step is that users should not include any optional header that can reveal personal information. For example, there is not any reason to include the header "Call-Info". The second step is to create user name that not reveal user's identity.

The "call-id" header is usually constructed in a way that reveals sender's IP address or hostname. Users should change these values with random values.

A measure to enhance privacy can be achieved by choosing the creation of URIs and user names in a way that would not reveal user's identity. In some of the header fields, URIs are not used for signaling. In others header, like "contact', an inaccurate URI would result a routing failure.

The structure of a URI can reveal information about the user. For example, the URI: gkikakis@unipi.gr reveals user's full name and the organization. On the other hand the URI: b143@anonymous-sip.com reveals that the user wishes to be anonymous.

Sometimes, the URI change is not enough to hide user's identity. A SIP service provider (SP) can reveal user's identity. For this reason, the header "from" should be anonymous. The restriction in this header is that a parameter should be valid and unique in order to ensure the right routing; this parameter is called "tag". An example of this header is From: "Anonymous" <sip:anonymous@anonymous.invalid>; tag=12325467.

All the above give some directions about how to handle user' name in order to prevent an attacker to find user's identity without adding technical measures. A first attempt to add technical measures is presented in RFC 3325 [16]. In this document are presented two new headers: "P-Preferred-Identity" and "priv-value". The first header includes a SIP URI and optional a user name. This header is a result of the observation of RFC 3323 [17] that an anonymized identity in header "from" is a good practice. This header is revealed only in trusted nodes. In this point is necessary to mention that this RFC requires the separation of trusted and not trusted. A proxy server after authenticating a user adds the "P-Preffered-Identity" and forwards the message to other trusted proxies. In case that a message has to be forwarded to not trusted proxies, this header should be removed.

The presence of "priv-value" header states that user wants the Network Asserted Identity to be kept private with respect to SIP entities outside the Trust Domain.

Here is an example of a signaling:

INVITE sip:bob@tral.com SIP/2.0
Via: SIP/2.0/TCP useragent.unipi.gr;branch=023-wed
To: <sip:bob@tral.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=4532372
Call-ID: 322345667733455676
CSeq: 2 INVITE
Max-Forwards: 70
Privacy: id
P-Preferred-Identity: "Dimitris Gkikakis" <sip:gkikakis@unipi.gr>
Proxy-Authorization: .... realm="unipi.gr" user="gkikakis"

proxy.unipi.gr -> outbound.unipi.gr (trusted)

INVITE sip:bob@tral SIP/2.0
Via: SIP/2.0/TCP useragent.unipi.gr;branch=023-wed
Via: SIP/2.0/TCP proxy.unipi.gr;branch=023-wtd
To: <sip:bob@tral.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=4532372
Call-ID: 322345667733455676
CSeq: 2 INVITE
Max-Forwards: 69
P-Asserted-Identity: " Dimitris Gkikakis" <sip:gkikakis@unipi.gr>
Privacy: id

outbound.unipi.gr -> proxy.tral.com (not trusted)

INVITE sip:bob@tral SIP/2.0
Via: SIP/2.0/TCP useragent.unipi.gr;branch=023-wed
Via: SIP/2.0/TCP proxy.unipi.gr;branch=023-wtd
Via: SIP/2.0/TCP outbound.unipi.gr; branch=023-wlm
To: <sip:bob@tral.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=4532372
Call-ID: 322345667733455676
CSeq: 2 INVITE
Max-Forwards: 68
Privacy: id

2.4. E-commerce

In e-commerce environment, the usage of anonymous digital certificates has been proposed. In addition, these certificates offer traceability. The proposed mechanism [18] tries to decrease the possibilities of an attacker to obtain the private key, which was the main vulnerability of a previous version. Accountability, which this

mechanism offers, is achieved with the usage of digital signatures. In order to protect the sender's identity in the digital certificate, which the receiver uses to verify the digital signature, it is proposed that the sender will request the issue of an anonymous digital certificate, based on the initial digital certificate. The anonymous digital certificate consists of a new public key and a pseudonym. The Certification Authority (CA) is the only one that knows the correspondence between the real identity and the pseudonym. In this way, the sender's anonymity and the authenticity of the message are achieved. In addition, the traceability of pseudonym from the CA is possible when a security incident or a state of non repudiation happens. An entity can obtain an anonymous digital certificate from the real identity digital certificate or from another anonymous digital certificate. The benefit from this circle of anonymous digital certificates is the prevention of behavioral profiling. The attacker has to interconnect different anonymous certificates in order to obtain the initial certificate, which includes the user's real identity. In the improved version of this mechanism is proposed the usage of two real digital certificates or two anonymous digital certificates for the issue of one new anonymous certificate in order to ensure the security of the mechanism.

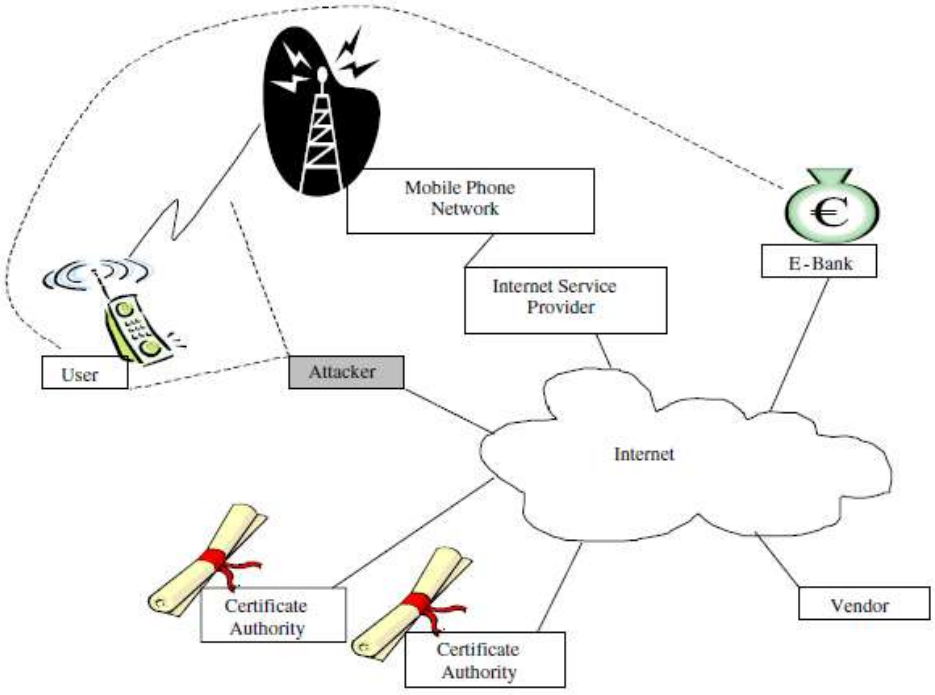

Figure 1: Mobile e-commerce infrastructure

- Let P_i denote the entity, which requests the issue if anonymous digital certificate, does not sign this request with the private key, but with CA's public key. In this way, CA does not know the entity's identity

- Let CA_{b-1} denote the CA of anonymous certificate does not reveal its identity to the other CAs, CA_{a-1} and CA_{a-2} from which it needs approval to continue. CA sends a quantity X_{a-1} and X_{a-2}, to CA_{a-1} and CA_{a-2}, which is encrypted with the public key of the corresponding CA in order to ensure the confidentiality of the message. This quantity includes the identity of P_i and an authentication token that refers to the certificate that belongs to P_i and is encrypted with the private key of P_i for its authentication. We mention that the quantities X_{a-1} και X_{a-2} is a secure way to obtain from CA_{a-1} and CA_{a-2} the approval for certifying the public key from CA_{b-1}, without letting CA_{a-1} and CA_{a-2} know the public key.

- The rights from CA_{a-1} and CA_{a-2} to CA_{b-1} do not include a piece of information for the digital certificates that have already been issued. If we combine this fact with the anonymity of $CA_{b-}1$, there is no way to interconnect the digital certificates. As a result, a malicious attacker cannot create a profile for the user. It is important to mention that CA_{a-1} and CA_{a-2} do not know the identity of CA_{b-1}, send the rights to CA_{b-1} encrypted with a session key, which has been sent from P_i.

This mechanism offers accountability through the below:

- Every digital certificate can be linked with the initial digital certificate only by the Legal Authority (LA).

- The P_i cannot repudiate the request for issuing an anonymous digital certificate from CA_{b-1}, because of the proof of the encrypted (with the private key) token. If another entity tries to obtain a certificate with the name of $P_{i,}$ it should find at least two private keys from CA_{a-1} and CA_{a-2}.

- Let $k_{i,\ b-1}$ denote a session key, which is created from P_i that exists in the token and as an encryption key of the rights. This key prevents from a malicious attacker, which tries to modify a public key ($pk_{i,\ b-1}$). The session key is equal to the function $h(A_{b-1}, pk_{i,\ b-1}, se_{i,\ b-1})$. Let $se_{i,\ b-1}$ denote a secret quantity selected by P_i in order to create a session key. We observe that id a public key ($pk_{i,\ b-1}$) is modified; the session key is also modified.

- Before the rights are encrypted with the session key, they are also encrypted with the private key of a CA. As a result, the sender cannot repudiate that he sent them.

The mechanism ensures anonymity with the below:

- A LA requests from a CA of an anonymous certificate that is at the lowest level of the hierarchy to ensure that the higher level approved of this issue. This can be denoted like a leaf node of a tree structure of digital certificates, having as root the real identity digital certificate. For example, the CA_{a-1} and CA_{a-2} approved the issue of CA_{b-1}. The request of LA is encrypted with the public key of CA_{b-1} in

order to ensure confidentiality and the requests that are sent from CA_{b-1} to CA_{a-1} and to CA_{a-2}, which are encrypted with the corresponding public keys.

- The evidence for who gave the approval of the next digital certificate, which comes from every level, is encrypted with the public key of LA. In this way they cannot be modified by a malicious CA.
- The LA has the ability to send direct to other CAs in order to avoid malicious intermediaries CAs. In this way, LA collects evidences, informing them to send the results direct to LA.

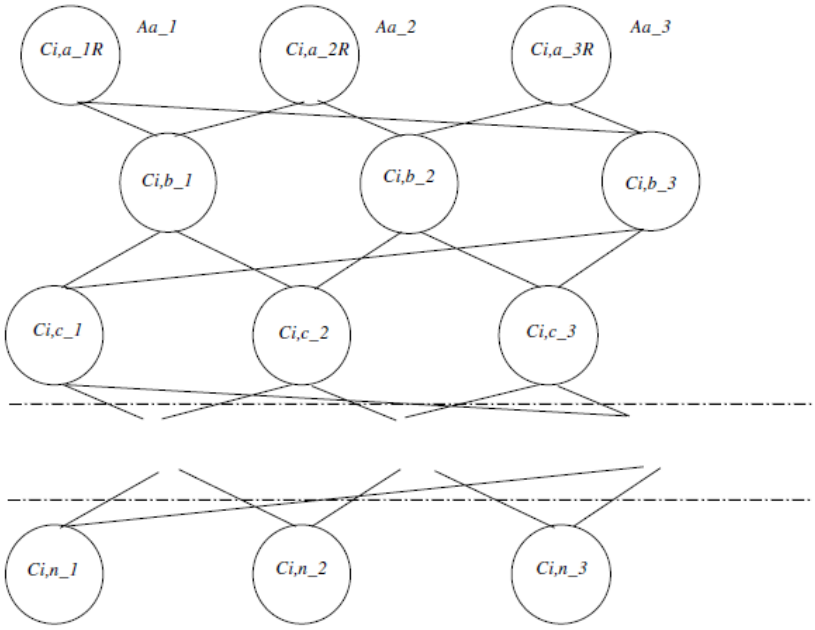

Figure 2: Figure graph

An alternative choice is the mechanism of "PyTHIA" (Privacy Through Hashes in Authentication) [19], which offers traceable privacy. This term is referred to the possibility of a sender to be authenticated to the receiver, without the latter knowing his identity. The specific mechanism uses a cryptographic token, which is called "Privacy - Protected Authentication Token (PPAT)". This token is created and distributed to users by a Trusted Third Party (TTP). The users can protect their privacy, be authenticated and make electronic transactions. This mechanism prevents the creation of profiles. If a security incident happens, then the TTP can trace the suspects through PPAT. However, in order to obtain a PPAT, the users should already have obtained a digital certificate by TTP. A PPAT is created from the function $H^n = (Cert_A, RV)$. Let H denote a hash function and n the difference between the dates of a user's (A) certificate expiration and the current date. The RV is a random value. The PPAT also consists of TTP's identification information, from a Uniform Resource Locator (URL), which refers to the revocation service and finally the date and the

time of issue and expiration. After the creation of PPAT, the TTP saves the PPAT and the link to a back up certificate. In addition, TTP sends to the user (A) the quantities H, n, RV και PPAT in order to save them securely.

When the user (A) tries to be authenticated by an entity B, sends the PPAT to entity B. After that, the user (A) sends the quantity H^{n-k}, to B. Let k denote the hours that have passed from the time of the certificate's issue. The entity B calculates k as well and verifies that the first element of the received $PPAT_A$ derives by applying k times the hash function H to the value H^{n-k} he has received from entity A. In order to ensure the property of "non repudiation", the entity B sends to TTP the quantities H^{n-k} and PPAT, which have been calculated from previous steps. TTP timestamps them through an independent Time stamping Authority. Entity B can be informed about PPAT revocation through the URL that already mentioned. The drawback of this solution is that despite the fact that entity A cannot repudiate that communicated with entity B, the last cannot prove the actions of entity A. In addition, PPAT mechanism cannot ensure the confidentiality and integrity of exchanged data. Other mechanisms, like SSL, could be used in order to protect these two security properties.

2.5.Location Based Services

Mobile web services include the benefits of web services in mobile devices, like mobile phones, wireless-LAN-enabled, PDAs and PCs. Smartphones, which offer Global Positioning System (GPS), have caused the market to develop LBS. This term includes every mobile web service, which makes use either of a satellite, or mobile beehives and offers an accurate location service. GPS is usually used for location identification but there are also techniques based on the network. Bibliography separates these services in four main categories [20]:

- *"Friend finder services" (Google Latitude)*

They allow location identification showing the location in a map or receiving notifications when a friend is near.

- *"Recommender services" (Loopt)*

This category matches a user's movement historic with another's in order to find common hobbies and propose new locations, like restaurants and stores. We have to mention that the users have not necessary any kind of relationship between them.

- *"City watch applications" (Citysense)*

Collects data, ideally from an entire city, in order to analyze behaviors. For example, monitors the traffic in order to identify traffic congestion or find the hot spots and propose specific places to the users. Moreover, the application "Citysense", updates the user for the Saturday night's hotspots that are linked with his preferences.

- *"Emergency services"*

  They identify the user's location when the user calls a specific number or send a SOS message to the service.

However, the computation of the user's geographical location reveals his location. A malicious user or SP can take advantage of this knowledge in order to send advertising messages for interesting points in this location (e.g. restaurants, bars) or track the user. All these are privacy incidents. In addition, the LBS do not offer privacy, but instead they violate it. LBS offer location sharing, they are based on wireless communications and are vulnerable to attacks like Man-in-the-Middle, Replay attack and Traffic analysis. Most of the solutions that have been presented are based on the modification of information that is exported for such services, like location generalization. However, LBS may require different level of information revealing. An example of the above is car navigation that simply requires location tracking. On the other side, when a SP tracks, usually needs his identity in order to offer services. In March 2011, a security protocol was proposed [21], which makes use of anonymity mechanisms in order to offer anonymity to users. The entities that participate in this protocol are an Anonymity Server (AS), which acts like TTP, that offers anonymous communication between the user (U) and SP. In addition, this solution makes use of location generalization, which shows a more generic location. This protocol is based on David Chaum's protocol [22], which had developed an anonymity protocol for e-mail systems. The specific solution offers hide of sender's identity, non traceability of the transaction and hides message's payload from non trusted entities through an intermediate server, called Mix.

The detail of the protocol is described in Figure 3. Throughout the explanation of the protocol we will use the following symbols:

U is the user of a smartphone.
AS is the anonymity server.
SP is the service provider.
PX is the public key of *X*.
SymX is a symmetric key of *X*.
CLocX is the current location of user *X*.
AX is the address of *X*.
TRX is a transaction of id *X*.
RX is a random number generated by *X*.
M is a message.

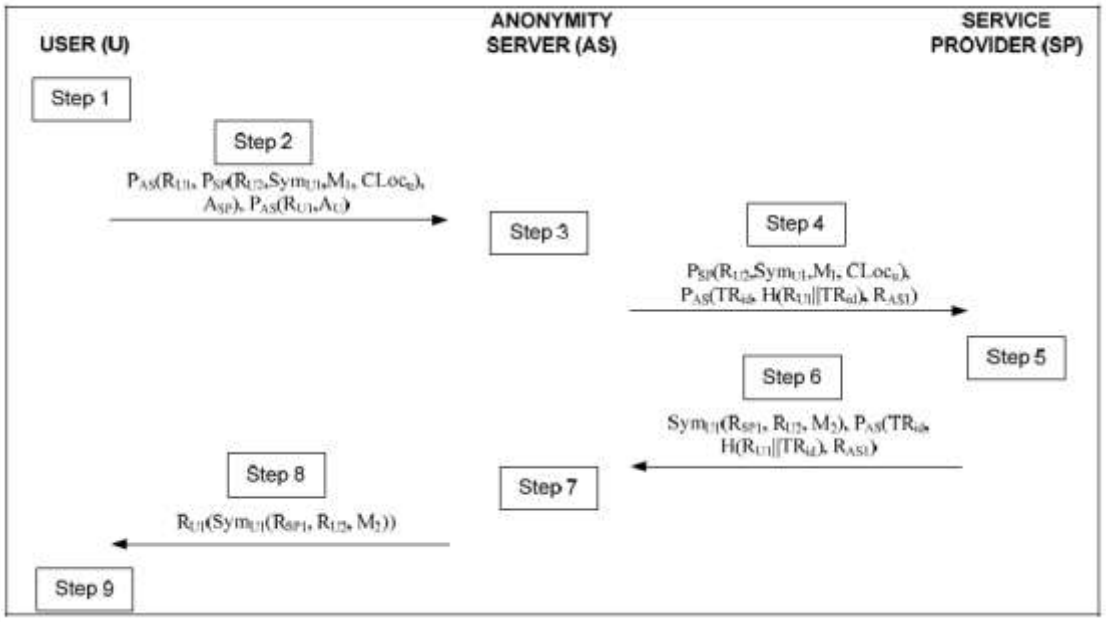

Figure 3:The proposed protocol

Step1. The protocol is initiated by the LBS application installed in the user's smartphone. The first job that the user (*U*) has to do is to create the whole message that will be navigated through the Anonymity Server (*AS*) in order to reach the *SP*. For instance, we will assume that the request message *M1* is to ask for the closest restaurant to him. The created message looks like the following:

PAS(RU1, PSP(RU2,SymU1,M1, CLocu), ASP), PAS(RU1,AU) (2)

where M1= "Get me the closest restaurant."

We can divide this message into two main parts. The first part (*PAS(RU1,PSP(RU2,SymU1,M1,CLocu), ASP)*) is responsible for delivering the request message (*M1*) to the *SP*. *M1* as well as a random number (*RU2*) all of which is encrypted by the public key of the *SP*. From the GPS enabled smartphone, the current location of the user (*CLocu*) is detected and added to the message. SymU1 is a temporary symmetric key created by the user which will be used by the *SP* to encrypt the response message in step 5.

To define which *SP* is to be communicated with, the address of the *SP* (*ASP*) is included in the message. It permits the *AS* to know which *SP* is intended to receive the request message (*M1*). Usually, *ASP* is the IP address of the server. Along with that, a random number (*RU1*) is included to ensure message freshness.

The second part (*PAS(RU1,AU)*) is used to allow the response message that is created by the *SP* to be sent back to the user (*U*). The user creates a return address that

contains the actual IP address of the user (*AU*). This part is mainly used by the *AS* (in step 7) to know the address of the user.

Although the message's two parts are encrypted with the same public key, they are actually separated in the structure of the message. Since the return address is only needed in step 7, the *AS* can directly store it (in step 3) while it is encrypted without the need for decrypting it and encrypting it again for safe storage.

Step2. The message created in the first step will be sent to the *AS.*

Step3. Once the message has been received, the *AS* will decrypt the first part of the message to deduce the address of the *SP* (*ASP*). The random number *RU1* will also be decrypted which later on will be checked (by the *AS*) against the random number (*RU1*) sent in step 8 to prevent any replay attack attempts. *PSP(RU2,SymU1,M1,CLocu)* will be kept as it is, since it is encrypted by the public key of the *SP* and hence the *AS* can't read the request message (*M1*).

The second part of the message will be stored in the *AS*. As indicated earlier, it contains the actual physical address of the user (in this situation it is the IP address). At a later stage, when the response from the *SP* is to be sent to the user (step 7) the *AS* will decrypt this part to get the actual address of the user. The *AS* creates a transaction id (*TRid*) for each request in order to refer to the corresponding stored return address. Since the part that includes the transaction id is encrypted by *AS*'s public key, an adversary that holds *AS*'s public key (which can be obtained easily, like from previous genuine transactions) can substitute this part with another one. Hence, the transaction id should be protected from tampering.

In order to protect the integrity of the transaction id, *RU1* and *TRid* are hashed and included in the message. Also, a new random number (*RAS1*) is generated in order to ensure freshness of the message. Those elements are encrypted by the public key of the *AS.*

One of the main characteristics of *AS* is that acts as a mixer. All requests sent from different users will be received by the *AS* and permutated before forwarding them on. In more details, if there are three users (*U1*, *U2*, *U3*) who sent three respective messages (*M1*, *M2*, *M3*), the order of forwarding these messages will be randomly changed. Hence, assuming that the order of receiving these messages is (*M1*, *M2*, *M3*), then, a possible forwarding order can be (*M3*, *M1*, *M2*). Achieving this can significantly reduce the effectiveness of traffic analysis attack. An attacker who tries to perform traffic analysis will have difficulty in matching the messages coming in and out of the *AS.*

The message after processing the previous step is the following:

PSP(RU2,SymU1,M1), PAS(TRid, H(RU1||TRid), RAS1) (3)
Step 4. *AS* passes the message modified in step 3 to the *SP*.

Step 5. Once the *SP* receives the message, it uses its private key to decrypt its first part. It reads the request message, processes it according to the user's request and produces the result. In our case where the closest restaurant is required by the user, the result produced might be a list of restaurants. The *SP* will form the result in another message (*M2*) and will encrypt it with the temporary symmetric key of the user (*SymU1*) which is included in the first part of the message. This symmetric key is known only by the user and the *SP*. It prevents the anonymity server from reading the response message created by the *SP*. In addition, a random number (*RSP1*) is included to the message. The second part of the message will be forwarded back to the *AS*.

The message can be formed as:

SymU1(RSP1, RU2, M2), PAS(TRid, H(RU1||TRid), RAS1) (4)

where *M2*= "Restaurant 1, Restaurant 2 and Restaurant 3."

Step 6. The previous message is then sent to the *AS*.

Step 7. The next step is to deliver the result message (*M2*) to the user. The *AS* needs firstly to retrieve the actual address of the user (*AU*). It can be done by identifying the transaction id (*TRid*) included in the second part of the message. The integrity and freshness of the transaction id are verified by using *RAS1* and the stored *RU1* (that is attached with the return address). The corresponding stored return address (*AU*) and random number (*RU1*) will be retrieved and decrypted. Accordingly, the *AS* will use *AU* to deliver the response message to the user. Since it is essential to eliminate any correspondences between *AS*'s input and output messages, the entire message is encrypted again by a new symmetric key deduced from the random number *RU1*. The final message that will be sent to the user will be:
RU1(SymU1(RSP1, RU2, M2)) (5)

Step 8. The *AS* forwards formula (5) to the user.

Step 9. The user receives the message and will use its random number *RU1* and the corresponding symmetric key to decrypt it and to get the response of the *SP*. Also the random number (*RU1*) will be checked in order to ensure the freshness of that message.

The proposed protocol can prevent from Man-in-the-Middle attacks, Replay attacks, through the random numbers $R_{U1,}$ R_{U2}, R_{AS1}, R_{SP1}. In addition, it offers anonymity properties like Forward anonymity and Backward anonymity through the symmetric session key. If a session key is revealed, the anonymity of previous or next transactions will not be revealed.

As we have already mentioned, this protocol offers location generalization. In some situations, providing high quality location information may violate a user's privacy. We assume that a user is asking for LBS while he/she is at home. In this case, the physical location of the user (which pinpoints his/her home) can effectively be used

by a malicious SP to identify that user, hence violating his/her privacy. Although the location information is protected from eavesdroppers, malicious SP's who have authorized access to location information can misuse them.

For this reason, the desire for generalizing location information that is sent to the SP is essential. To generalize location information, the quality of the submitted location information from the smartphone can be reduced. Therefore, instead of providing an exact physical location of where the user currently is, we can make it more general to include a range of physical locations or to include a larger area. Achieving this will strengthen the anonymity of the user and will solve the problem discussed above.

However, this protocol can be only supported by nonprofit services. This protocol cannot be used in e-commerce services.

At this point we will refer to an architecture that has been proposed in the research area of Mobile users Privacy. The specific architectures achieve unlinkability of the user's real identity. This architecture is based on mobile operators' architecture Parlay X [23]. The Parlay APIs are designed to enable the creation of telephony applications as well as to "telecom-enable" IT applications, but they are quite low-level APIs, requiring developers to have some understanding of telecommunications concepts. IT developers, who develop and deploy applications outside the traditional telecommunications' network space and business model, are viewed as crucial for creating a dramatic market growth in next generation applications, services and networks. The Parlay X Web Services are intended to stimulate the development of next generation network applications by IT developers who are not necessarily experts in telephony or telecommunications. The choice of Web Services will be driven not so much by technical elegance as by commercial utility. The main goals of Parlay X are that:

• each Web Service will be abstracted from the set of telecommunications capabilities exposed by the Parlay APIs, but may also expose related capabilities not currently supported in the Parlay APIs where there are compelling reasons.

• the capabilities offered by a building block may be homogeneous (e.g. call control only) or heterogeneous (e.g. mobility and presence).

•It is desirable for the messages to follow the synchronous request/responses model, initiated by the application.

• It is desirable for Parlay X Web Services invocations to be uncorrelated and for the Web Service to be stateless from the perspective of the application,

• A Parlay X Web Service will be neither application specific nor network specific.

• Parlay X Web Services will be judged on the 80/20 support 80% of applications using 20% of the available functionality, i.e. methods will not be unnecessarily complicated or overloaded,

• The Parlay X set of interfaces shall be extensible — integration of third-party-provided interfaces must be supported using proven, reliable, and Web Services-standard technologies.

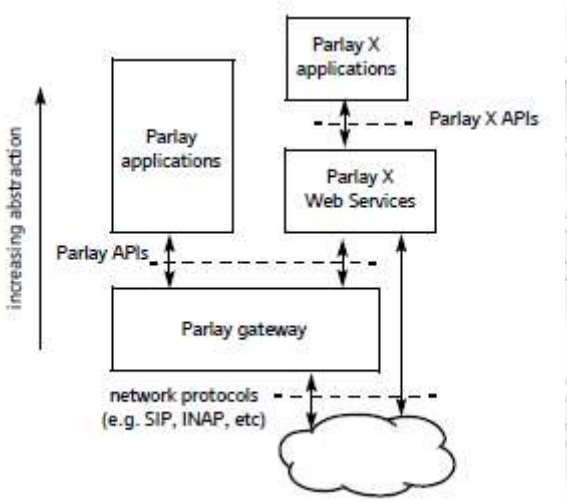

Figure 4: Parlay X architecture

PRIVES [24] is a technique that is based on Parlay X framework. The privacy API describes the interactions between a privacy user agent and the privacy service. The selected technology is SOAP over HTTP. The first interaction at startup, logon (password) is used for authentication of the user agents. The password is a shared secret which is defined at registration time (see Table 1).

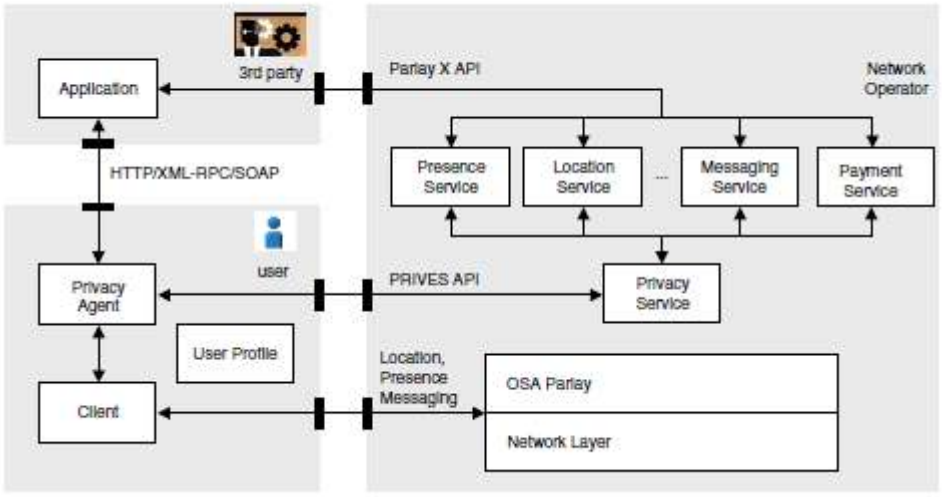

Figure 5: System Architecture

The privacy agent subscribes then to his own privacy information or to that of another user, depending of the application as illustrated in Figure 6. The subscription is either explicitly accepted or processed automatically by policy rules in the privacy service. Following the subscription, the *privacy agent* receives a seed code word *r* and can create pseudonyms. The operation's parameter allows restricting the subscription to a part of the private information (location, contact address, presence, etc.).

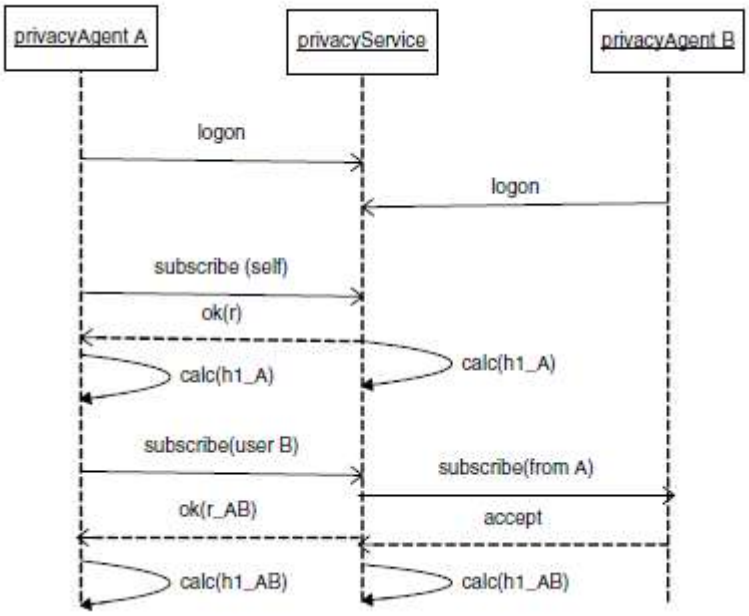

Figure 6: Initialization of the privacy service

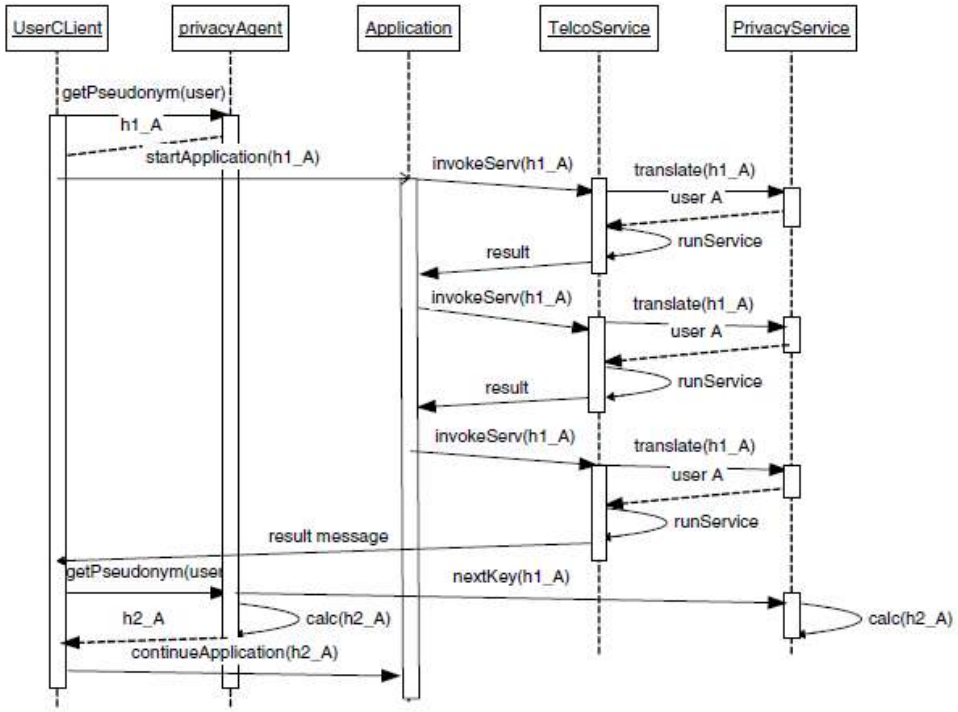

Figure 7: Invocation of the application and underlying services

The interaction between the user client and the application is not subject to standardization, the protocol can be HTTP, XML-RPC or SOAP. The client invokes the application with some start application message without necessarily authenticating himself. The pseudonym *h1A* received by the application in this start message is used as EndUserIdentifier, across the Parlay X interfaces (see Figure 7). At the service side, the *privacy service* translates the pseudonym back to the real username or address, so that the Parlay X telecommunication service can work properly.

Basically, a new pseudonym can be created each time the user client addresses the application. However, frequent change of pseudonyms does not necessarily increase the anonymity of the user, since most applications keep anyway a session with the current state of the application workflow and the message history. To control the establishment of a new pseudonym at both sides, the privacy agent calls the method nextKey(). The problem encountered when switching to a new pseudonym is one of synchronization: the application has to have closed the transactions towards the services and the user, so that the latter can establish with the privacy service a new pseudonym (with nextKey). The most common synchronization cases are easy to realize with the help of the messaging service:

• the application completes a transaction and sends a final message using the messaging service to the user (for example informing him about the payment).

• the user decides to stop or to abort the application, which first causes all the telecommunication services to finish and then sends a last message to the user. This message is used to trigger the nextKey() message.

PRIVES is based on hash value calculation using the HMAC scheme that makes it useful for small devices such as smart phones and PDAs. HMAC uses the known hash schemes MD5 and SHA-1 with comparable computation times. It allows creating a hash value from a previous one, using in addition the password as a shared secret between the *privacy service* and the watcher.

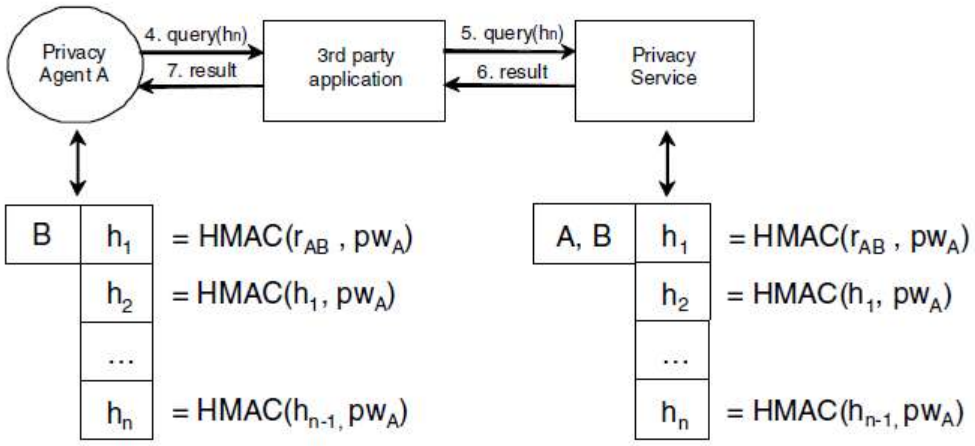

Figure 8: The PRIVES scheme

In Figure 8, user A creates hash values to allow the application to query the profile of user B. The hash values are created in a synchronized way by the privacy agent of user A and the privacy service from the previous hash value h(n-1) and A's password by applying the HMAC operator H(). The only information the user A needs is the anchor r(AB), which is initially created by the *privacy service* and is a function of the password, and a random number. When the privacy service receives from the application a localization request for the user identified by the hash value h(1), it checks its validity and determines from h(1), who the watcher and the target user are. Once the request is processed, the requesting user and the privacy service have already prepared the next hash value h(2) for the subsequent request and so on.

Nonetheless, some disadvantages still exist to mention:

- The existence of "Parlay X" infrastructure is required.
- The pseudonym is computed in the mobile terminal, which implies suitable software and resources consumption.
- The reasons to trust "Privacy Service", as well as its architecture, are not clearly referred.

Synchronization problem of different pseudonyms occurs. For instance, in case of an uncompleted transaction because of session termination, a new pseudonym must be created to manage smooth termination.

In order to solve as many of the above problems as possible, the use of a "Privacy Web Service" was proposed [25], which is integrated into the "Parlay X" architecture and operates as anonymizing proxy, giving emphasis to location protection of mobile terminal. They propose to add a novel API dedicated to privacy policy. We argue that there is a separation between privacy managing and target services, which can be location service, presence service, instant messaging service, etc. The new Parlay X web service has to validate the privacy policy defined by users and to ensure the anonymity of users through pseudonymity. It is designed to enhance the security at the application level and to facilitate privacy enforcement in Parlay X gateway. To validate our solution, we apply it to location service, which is a major capability provided by 2G and 3G cellular networks. Location-based services (LBS) use positions of users, which are sensitive information, to offer more enhanced services. In cellular networks, different methods have to cooperate in order to retrieve and deliver the location information. They don't however offer the same privacy level. We propose to control the privacy of such sensitive data through a dedicated web service, which can encapsulate other specialized Parlay X web services.

For the purpose of illustrating the contribution of the new privacy service, a new call flow is presented in this section. The scenario of the call flow is a third party location request, shown below. The provider knows only a user's pseudonym, so it interrogates Privacy web service to check the pseudonym and validate the request. Privacy web service, in its turn, asks the PMD functionality, which is integrated in the GMLC or a standalone entity in the core network.

First, pseudonyms must indicate the operator network to which the user is subscribed. In this example (figure 7), Privacy web service verifies that a pseudonym exists and is supported by the PMD functionality.

The following steps involve the new call flow based on Privacy web service:

1) The normal location request is replaced by a privacy service request to the new web service.

2) Privacy web service asks the PMD functionality if the pseudonym is active at this moment and is valid.

3) PMD verifies pseudonyms.

4) The PMD sends Privacy web service response.

5) Privacy web service will formulate the location request to the terminal location web service.

6) Normal location request is treated by the terminal location web service, and location data is returned to the privacy web service.

7) Location result will be sent to the application.

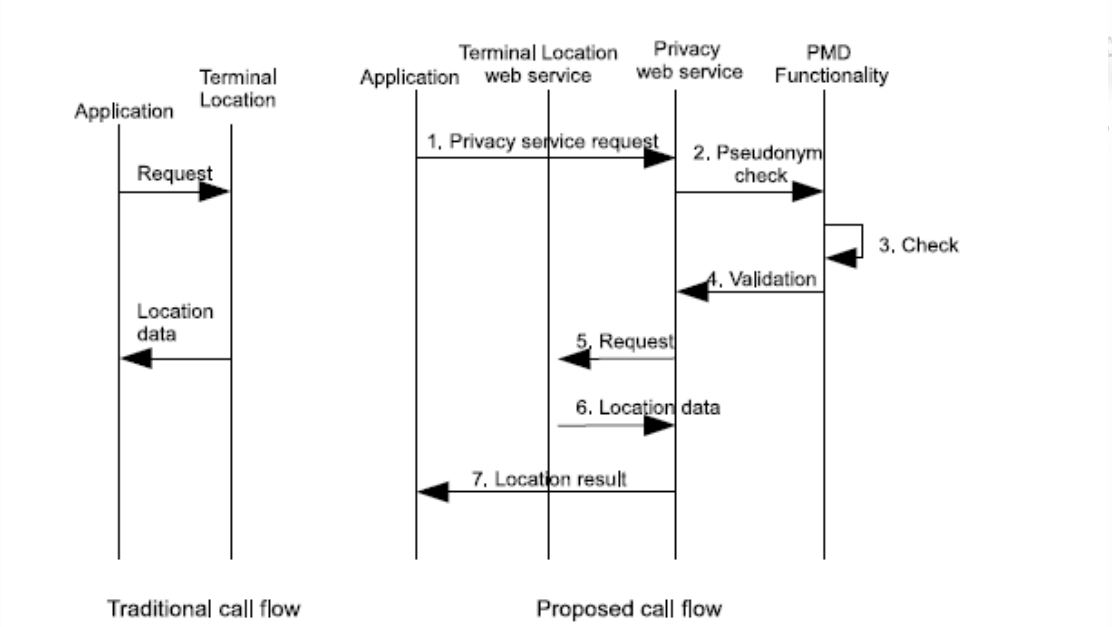

Figure 9: Sequence diagram of terminal location query: new proposed call flow vs the traditional

3. Proposed Privacy solution

The proposed solution is used when a Mobile Subscriber (MS) wants to access SP's services pseudonymously without giving any personal information to SP. This solution can be deployed on beyond 2G mobile networks architectures including GPRS (2.5 G), UMTS (3G) and 4G networks that integrate WLANs as well as WIMAX with UMTS. The entities that participate in this solution are mobile operators, MSs and SPs. The operator of the underlying mobile network serves as Third Trusted Party (TTP) to the employed communication model that also consists of MSs and SPs. This is not far from the reality since the MSs already trust mobile operators to keep personal data of them including location, service, billing, etc. On the other hand SPs are willing to trust mobile operators in order to ensure payment for the granted services to MSs. Acting as a TTP the mobile operator may generate, store, sign and encrypt pseudonyms for each MS ensuring confidentiality and authenticity of each one by employing digital certificates and public key cryptography.

The proposed solution offers authentication, authorization, accounting (AAA), security and privacy. Mobile operator generates a pseudonym that is sent to a SP with

which the MS can be authenticated and authorized to use SP services. The process has taken into account security risks and implemented measures for them. In addition, in this process we do not reveal personal information and allow the fruition of all the kind of services such as e-commerce, location based services, etc.

3.1. Requirements

The proposed solution requires the introduction of a new network node in the core network of the mobile operator named as pseudonyms' provider (PSP), which has interface to the Home Location Register/Home Subscriber Server (HLR/HSS). HLR/HSS contains details of each MS such as the International Mobile Subscriber Identity (IMSI), service subscription information and service restrictions. We create a new table in the Database for every MS. The table is shown in abstract type in figure 10, where PSP receives requests from MS for accessing the SP pseudonymously. PSP asks the HLR/HSS if a pseudonym for a specific MS and SP already exists and can be used. If not, it generates one, updates HLR/HSS with the new generated pseudonym and routes traffic to other components.

MS INFO

IMSI	SP	PSEUDONYM
202011234567890	www.ebay.com	ydgoanffean
202011234557890	wwwa.ds.unipi.gr	gakfjfkfksf
202011254567890	www.tanea.gr	fkffkfkffkf

Figure 10: MS INFO

We assume that SPs possess digital certificates. Each time PSP wants to send a pseudonym, retrieves SP digital certificate, looking up in its database for the providers' certificate and verifies it, checking also an updated certificate revocation list (CRL). Otherwise, PSP requests SP for its certificate, ensures its validity, process the pseudonym and stores the certificate for future use. Together with the pseudonym, PSP includes a sequence number in it. The first time the pseudonym is sent the value of sequence number is zero and every time the pseudonym is sent the sequence number is growing by one. Both PSP and SP keep a record of the last sequence number. PSP keeps the record in order to know the value of sequence number that has to send the next time and SP to know the if the sequence number is valid and accept it or not.

The proposed solution utilizes a different IP address for each connection with a different SP. In this way, it achieves unlinkability between different connections of the same MS with SPs. The component that provides IP addresses allocation depends on the specific architecture of the network.

Roaming can be supported by our proposed solution. Home mobile operator can send the corresponding IMSI, pseudonyms and SPs to the visited mobile operator. The involved parts have to communicate in a secure way. Mobile operators can use symmetric or asymmetric cryptography.

3.2. Network Architecture

3.2.1. UMTS Architecture

UMTS architecture is based on the following components. Radio Network Controller (RNC) controls the Node B and is responsible for radio resource management. Serving GPRS Support Node (SGSN), which allows the incoming and outcoming traffic from MS to the rest of the network. It is also responsible for mobility management, security, etc. Gateway GPRS Support Node (GGSN) is responsible for the interworking between UMTS and external networks. Moreover, GGSN converts the packets to the appropriate type, routes the traffic and manages the IP address pool of the mobile operator. GGSN acts as a black box for external networks because hides the rest of UMTS network from the externals. HLR/HSS is a Database, which contains information about MSs. Some types of information that can be stored in HLR/HSS are the services that a MS is allowed to use, current location and settings.

PSP provides an additional service to UMTS network. This component has to be in a position that can receive request from MSs and have access to the MSs information, where pseudonyms are stored. PSP could be connected to SGSN, which is the first component in the core network. MSs requests for Privacy Service (PS) can be forwarded from SGSN to PSP without high signaling cost. The interface that could connect SGSN to PSP is the same (Gr), which connects HLR/HSS to SGSN. Gr interface is used primarily to get information about MSs. The interface that connects PSP with SGSN conveys: (i) requests and responses for pseudonyms, (ii) requests and responses for digital certificates. PSP could also be connected to HLR/HSS in order to retrieve existing pseudonyms. The interface that connects PSP to HLR/HSS transmits requests and responses for pseudonyms. The appropriate interface for this connection is Gr. All the above take place using Mobile Application Part (MAP) [26] of the SS7 protocol stack.

The last requirement of our solution is the utilization of a different IP address for each connection with a different SP. Every MS holds at least two IP addresses. An internal that is used for the internal network (SGGSN, GGSN) and at least one external that is

used for GGSN and the external networks (e.g. Internet) [27]. In [28] is mentioned that GGSN can allocate multiple external IP addresses for each MS. Based on that, we assume that every MS can be allocated one IP address for our new PS, which can change every time a MS wants to visit another SP. The functionality of allocating a new external IP address is implemented by sending a message from PSP to GGSN requesting a new external IP address allocation for the specific MS.

3.2.2. Architecture for Integrating UMTS and WLAN

UMTS and WLAN are not designed to work together, but there is a growing interest for integration. Based on this interest, we deploy our model in this kind of integration.

The network consists of the following components. The WLAN Gateway, which connects WLAN Access Points with AAA server, WLAN Access Gateway (WAG) and Packet Data Gateway (PDG). WAG is responsible for enforcing routing through the PDG, performing collection of accounting information, etc. AAA server retrieves authentication and other information from HLR/HSS and validates the credentials that MSs provide. HLR/HSS provide information about MSs to AAA server. PDG is responsible for providing access to external networks. An interface connects PDG with AAA server in order to provide authentication services to WLAN.

In this architecture we require PSP to be connected with the network through a component, which is responsible for collecting MS data and forwarding them. This component is the AAA server, which collects information from HLR/HSS and forwards them. A kind of information can be pseudonyms. AAA server can request pseudonyms from PSP, which can interact with HLR/HSS in order to retrieve or store a pseudonym.

PDG is designed to re-use existing GGSN functionalities such as IP address allocation and Charging Gateway interfaces [29]. Having this knowledge we assume that the utilization of a different external IP address for each connection with a different SP can be implemented as we explained in GGSN.

3.2.3. Architecture for Integrating UMTS and WIMAX

WIMAX is one wireless broadband standard that offers high speed transmissions. WIMAX and UMTS interworking is a high level interest research area. Many proposals have been presented, but none of them has been implemented as standard yet. We study our model based on the architecture presented in [30].

The main components of this architecture are Access Service Network (ASN) Gateway, Home Agent (HA), WAG and PDG. HA manages the mobility inside the WIMAX network. The rest of components have already been described in the architecture for Integrating UMTS and WIMAX. The modifications that are necessary for our model are the same with UMTS and WLAN.

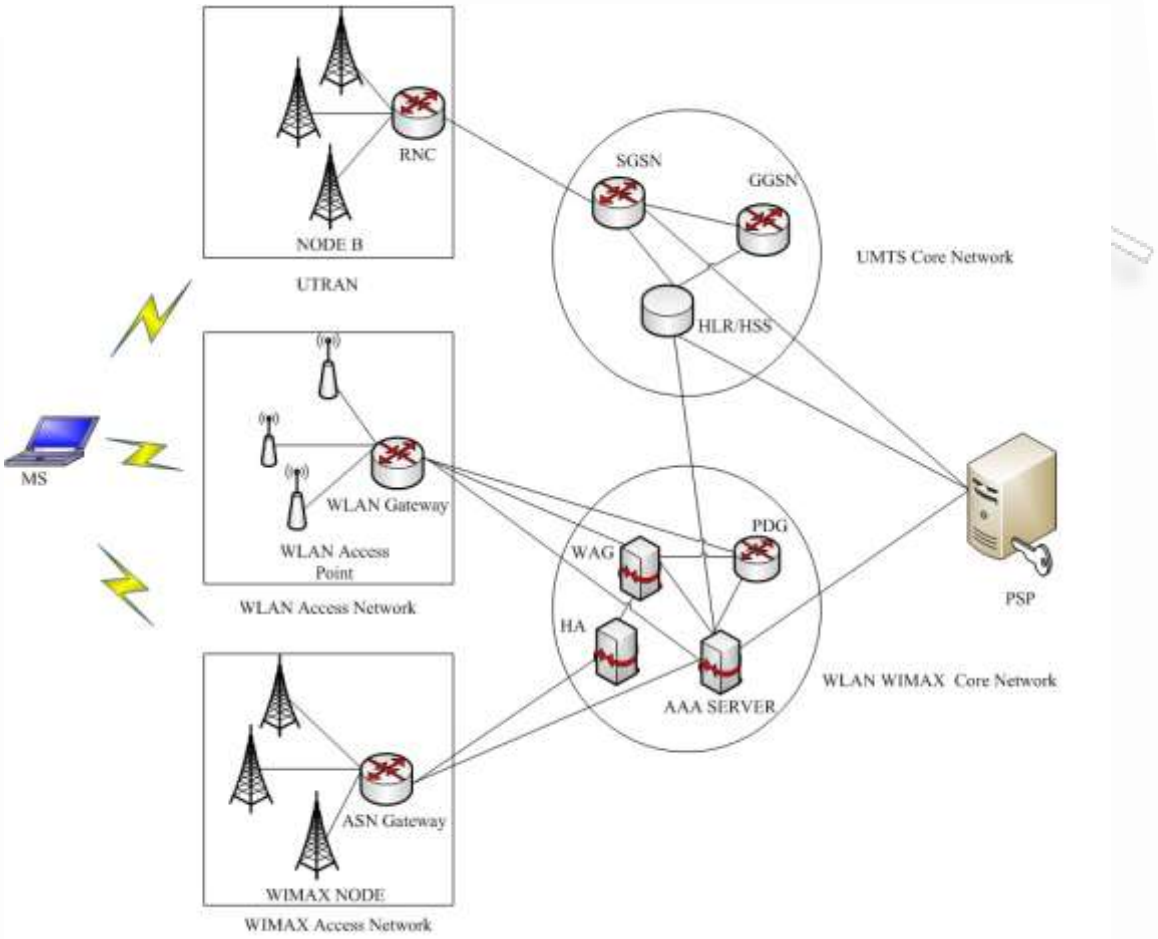

Figure 11: Model Architecture

4. Functionality

This section reveals the functionality (figure 12) of the proposed solution. We describe the messages exchange for retrieving an existing pseudonym and the messages exchange for a new pseudonym for a specific MS that access a particular SP. We present the functionality of the model in UMTS networks. The rest of architectures can implement this functionality following the above guidelines.

4.1. Messages exchange description

The initial step starts when the MS requests the mobile operator to access a specific SP pseudonymously. We suppose that the Radio Resource Control (RRC) protocol has already established a connection and a MS internal IP address has been assigned. In step 1, MS requests the PS from the mobile operator for accessing a SP by sending to the involved SGSN a message that includes the type of service (PS), as well as the name of the SP (e.g., www.google.com). Upon receiving this, the SGSN retrieves the permanent identity (International Mobile Subscriber Identity – IMSI) of the requesting MS. In step 2, SGSN adds the retrieved IMSI and forwards a message that

includes IMSI and SP to PSP. After receiving this message PSP forwards it to HLR/HSS (step 3). When HLR/HSS receives this message, creates a query, which is sent to database in order to retrieve an existing pseudonym that matches to IMSI and SP. If a pseudonym exists, HLR/HSS creates and sends to PSP a message that contains IMSI, SP and the retrieved pseudonym of MS (step 4). At this point PSP retrieves SP's digital certificate from its database.

If a pseudonym does not exist, HLR/HSS returns a message "not found" (step 4a). In this case, PSP generates a pseudonym and then updates HLR/HSS entries for the new pseudonym (step 4b). If PSP does not hold SP's digital certificate, PSP looks up for it on the Internet by following the routing: SGSN, GGSN, Internet (step 4c).

By the time PSP holds the pseudonym and SP's digital certificate, PSP initializes the digital signature and encryption process as follow: Let M denote the concatenation of MS pseudonym and a fresh sequence number, which is generated by PSP. Using a hash function, which accepts M as input, a message digest H(M) is computed. After, using H(M) and the private key of PSP (KPpsp), a digital signature is computed: $DS=E_{KPpsp}\{H(m)\}$. Then, a new message, which consists of the digital signature (DS) and the plaintext of message M, is created: N= DS||M, providing authenticity and integrity. Next, PSP encrypts N using SP's public key (KUsp) and an asymmetric algorithm as $C=E_{KUsp}(N)$, providing confidentiality. At this point the process of digital signature and encryption has been finalized.

In step 5, PSP sends a message to SGSN, which contains IMSI, requesting a new MS's external IP address assignment for the PS. At this point SGSN forwards the message to GGSN (step 6). In step 7, GGSN sends to SGSN a response OK that simply indicates a successful assignment of a new MS's external IP address for the PS. SGSN forwards this message to PSP (step 8). In step 9, PSP creates and sends to SGSN a message that contains C and the name of SP as a response for the PS. In step 10, SGSN forwards this message to the specific GGSN, which is the final destination for the internal network. In step 11, GGSN converts the packets into the appropriate packet data protocol (PDP), adds the MS's external IP address for the PS and sends them to the corresponding SP through Internet.

SP decrypts the C using its private key and the asymmetric algorithm (KPsp): $N=D_{KPsp}(C)$ and verifies the digital signature DS using PSP public key (KUpsp). Finally, SP compares the received sequence number with the previous received. If the received sequence number is increased by one from the previous, the sequence number is valid. SP rejects the message in two cases. If the digital signature is not valid or the sequence number is not the expected. At the end of this message exchange, the SP has received a pseudonym with which the MS can be authenticated and authorized to use SP's resources.

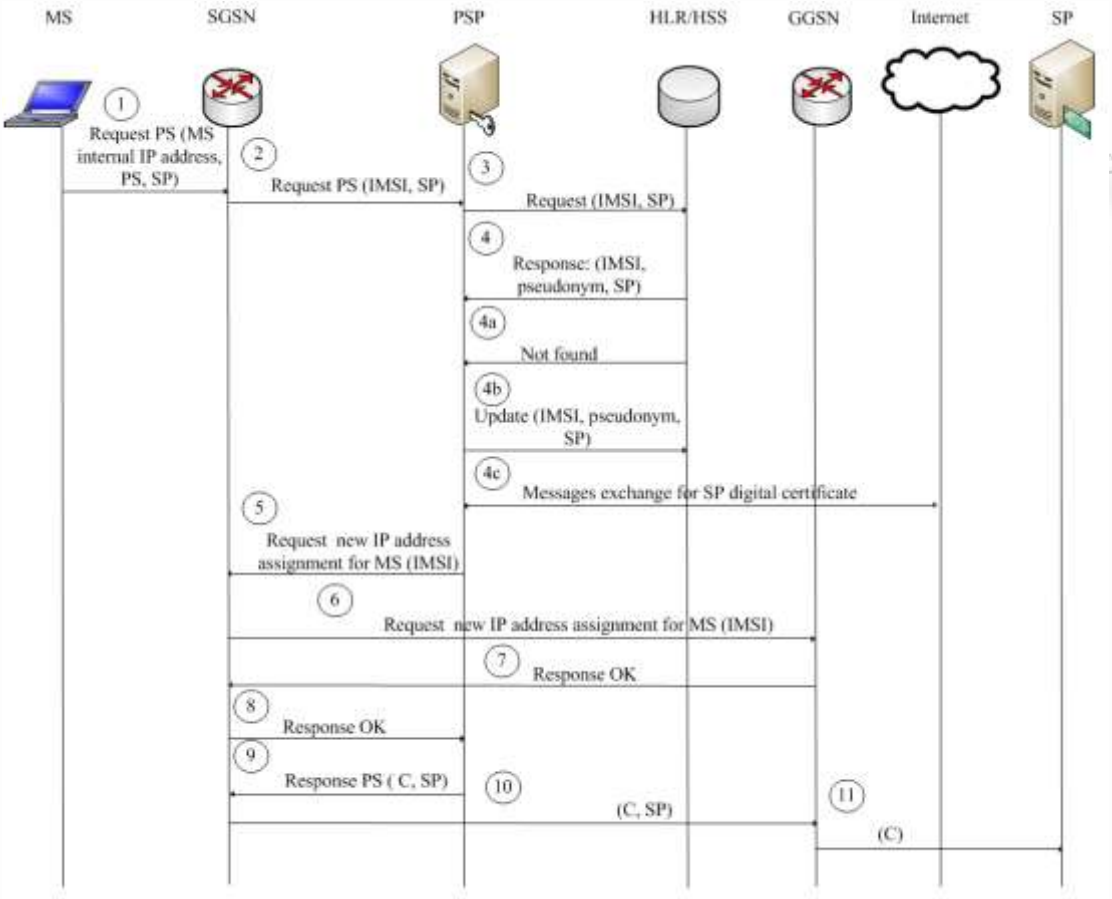

Figure 12: : Messages exchange

5. Evaluation

In this section we demonstrate the reasons that make our solution valuable and also the drawbacks of it. First of all, our solution offers privacy. The real identity of the MS is not exposed outside the mobile operator network. SP receives a pseudonym from the mobile operator. The owner of this pseudonym can be any MS of the specific mobile operator. In addition, MS holds a different pseudonym for every SP, which does not allow SPs to profile habits or locations of a real person. Moreover, the proposed solution utilizes a different IP address for each connection with a different SP. In this way malicious SPs cannot link IP addresses with pseudonyms in order to conclude that specific pseudonyms belong to the same MS. Summarizing at the field of privacy, we cover the properties of pseudonymity and unlinkability between a MS and his actions or between different pseudonyms of a MS. These properties protect from threats like location tracking, behavioral profiling and data interconnection.

The proposed solution uses some security measures in order to avoid malicious attacks. Encryption of pseudonyms has been implemented in order to achieve the confidentiality of pseudonym. Two other properties of security are protected with

digital signature. PSP signs pseudonyms in order to achieve integrity and authenticity. With the above, the model is protected from man in the middle attacks. A man in the middle cannot eavesdrop pseudonyms of MSs because they are encrypted and also can not alter the message. If a message is altered by a man in the middle, the message will be aborted because it will not be signed by the PSP. The proposed solution is also protected from replay attacks. The measure for this attack is the sequence number that is sent with pseudonym. If the attacker tries to resend a message, it will be aborted because the sequence number will not be valid.

Another advantage of the proposed solution is the ease of deployment and the suggestion of a specific architecture and signaling data. Core network change is small and does not require high investment. We respect the standardized architectures; we do not change anything on it, but only add one component. The new component can use already implemented interfaces, as already has been described, which connect other components in the existing architectures. In addition, we present a detailed signaling data. All the parameters that have to be exchanged have been presented. This practice makes our solution feasible to be implemented. The cost of the model, both network and financial, is low in relation to the goal we achieve.

From the point of e-commerce the proposed solution allows the financial transactions without exposing personal information, such as MS credit card or bank account. Moreover, MS have not to follow complicated processes in order to pay SPs. The MS enjoys SP e-services and the SP charges the mobile operator. This can be achieved by sending a list to mobile operators with the pseudonyms and their charges every month. The mobile operator traces the pseudonym and charges the MS, who holds the specific pseudonym.

The main drawback of the proposed solution is the new IP address allocation for each connection with a different SP. This measure achieves high level of privacy protection but adds signaling and administrative cost to the GGSN or PDG. We will analyze how our requirements can be covered by existing GGSN functionalities [27]. We study GGSN because PDG has the same functionalities with GGSN. As we already mentioned, MS holds at least two IP addresses. An internal that is used for the internal network (SGGSN, GGSN) and at least one external (public) that is used for GGSN and the external networks (e.g. Internet). Every MS holds one different public IP for every service (e.g. Internet, WAP). GGSN uses a table where records the correspondence of internal and external IP addresses. These addresses are dynamically allocated through Dynamic Host Configuration Protocol (DHCP).

The great problem is the limited number of IP addresses. Mobile operators hold a specific pool of IP addresses and a huge number of MSs. To solve this problem, mobile operators use Network Address Translation (NAT). In this way MS are allocated an internal IP address and NAT performs the translation to an external IP address. For external IP addresses mobile operators take advantage of the ports of IP addresses. Conventional packets (TCP, UDP) packets have 16-bit number for the port value, allowing 2^{16} unique ports per IP address. A small number of them is reserved for specific services, the rest of them are available for MS. In this way mobile

operators can allocate one IP address to thousands MS. According to the above, we consider that a new IP address for every new communication does not exhaust the pool of IP addresses.

The proposed solution is also vulnerable to the insider threat. A malicious inside the mobile operator can gain access to HLR/HSS, collect a pseudonym, the IMSI, pseudonyms and the SPs that these pseudonyms are used to. An insider can also act as man in the middle between HLR/HSS and PSP in order to eavesdrop the pseudonym, IMSI and SP. The above threats are owed to vulnerabilities of B3G architecture and not to vulnerabilities of our proposed solution.

6. Conclusion

New technologies and applications development will generate privacy consideration. Researchers will face new technologies in which they will have to develop new techniques in order to protect users' privacy. Malicious users and organizations will always have a motivation that will drive them in malicious actions. The motivation for these actions is the profit.

With the curing of a new technology the researchers will have to prove that their solutions are effective and the users are willing to use these solutions.

Mobile Internet is not a new technology achievement, but the high level of its penetration in market is an achievement of the past three years. Mobile Internet will thrive the next years. However, we are not sure about the networks that will transmit Mobile Internet. UMTS could continue its solitary journey. On the other hand, market could demand the convergence of UMTS, WLAN and WIMAX networks. The technologies already exists. When the market is ready, this technology will become a part of our life. We should be ready to present privacy solutions that can be implemented in all these scenarios.

In this era we presented a solution that offers privacy in mobile surfing and e-commerce. In general, the MS authenticates in a SP without it to know the real identity of MS, trusting the mobile operator. The whole communication is carried out taking in account privacy, security and the existing topologies of B3G networks. At the evaluation section we proved that our model offers high level of security and privacy, we know well the architectures of B3G networks, we recognize the existing vulnerabilities of these networks and the signaling overhead that is added for new IP address allocation for each connection with a different SP.

7. References

[1] Alan Westin, "Privacy And Freedom", Atheneum, New York, 1967.

[2] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology", May 2006.

[3] Beresford, A.R. and F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing Magazine, p. 46-55, 2003.

[4] European Parliament, Directive 95/46/EC of the European Parliament and the Council of 24 October, 1995

[5] European Parliament, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002.

[6] European Parliament, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006.

[7] J. Boyan, "The anonymizer: Protecting user privacy on the web", Computer-Mediated Communication 4, 9, September 1997.

[8] Eran Gabber , Phillip B. Gibbons , David M. Kristol , Yossi Matias , Alain Mayer, "Consistent, yet anonymous, Web access with LPWA", Communications of the ACM, v.42 n.2, p.42-47, Feb. 1999.

[9] M. K. Reiter and A. D. Rubin "Crowds: Anonymous Web Transactions", *ACM Transactions on Information and System Security (TISSEC)*, vol. 1, no. 1, pp. 66-92, November 1998.

[10] David Goldschlag , Michael Reed , Paul Syverson, "Onion routing", Communications of the ACM, v.42 n.2, p.39-41, Feb. 1999

[11] L. Cranor, "P3P: Making privacy policies more useful", *IEEE Secur. Priv.*, vol. 1, no. 6, pp.50 - 55 , 2003.

[12] Paola Benassi, "TRUSTe: an online privacy seal program", Communications of the ACM, v.42 n.2, p.56-59, Feb. 1999.

[13] R. Cimander, A. Aarma and A. Jary, "Good Practice Case -eID in Estonia", Prepared for the eGovernment Unit. 17 October 2006.

[14] D. De Cock, K. Wouters, B. Preneel, "Introduction to the Belgian EID Card: BELPIC", in 1st EuroPKI, Greece 2004.

[15] J. Benders, D. Kugler, M. Margaf and I. Naumann, "Privacy friendly revocation management without unique identifiers for the German national ID card", Computer Fraud & Security, Vol. 2010 Issue 9, September 2010, pp. 14-17.

[16] C. Jennings, J. Peterson, and M. Watson. RFC 3325 - private extensions to the session initiaion protocol (SIP) for as serted identity within trusted networks. http://www.ietf.org/ rfc/rfc3325.txt, Nov. 2002.

[17] J. Peterson. RFC 3323 - A privacy Mechanism for the Session Initiation Protocol (SIP). http://www.ietf.org/ rfc/rfc3323.txt, Nov. 2002.

[18] D. Critchlow, N. Zhang, "Security enhanced accountable anonymous PKI certificates for mobile e-commerce", Computer Networks 45, pp. 483–503, 2004.

[19] K. Moulinos, J. Iliadis, C. Lambrinoudakis, S. Xarhoulakos, D. Gritzalis, "Pythia: Towards anonymity in authentication", in *Proceedings of the IFIP TC11 16th International Conference on Information Security (Sec 2001)*, Paris, France, June 2001, pp. 1-17.

[20] M.P. Scipioni and M. Langheinrich, "I'm Here! Privacy Challenges in Mobile Location Sharing", in Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), May 2010.

[21] M. Alzaabi, C.Y. Yeun and T. Anthony, "Ensuring Anonymity for LBSs in Smartphone Environment", *Journal of Information Processing Systems*, vol. 23, no. 2, pp. 121-136, March 2011.

[22] D. Chaum, "Untraceable Electronic, Mail Return Addresses, and Digital Pseudonyms", *Communication of the ACM*, Vol.24, No.2, 1981, pp.84-90.

[23] Parlay X Web Service Specification, Version 3.0

[24] O. Jorns, S. Bessler and R. Pailer "An efficient mechanism to ensure location privacy in telecom service applications", in *Net-Con 2004*, Spain, 2004.

[25] N. Ajam, "Privacy Based Access to Parlay X Location Services", in *Proceedings of the Fourth International Conference on Networking and Services (ICNS)*, Guadeloupe, France, March 2008, pp. 204-206.

[26] 3GPP TS 29.002 (v. 8.8.1), "Mobile Application Part (MAP) specification", Release 8, 2008.

[27] J. Bannister, P. Mather, S. Coope. "Convergence Technologies for 3G Networks". Wiley, 2004.

[28] Yuan-Kai Chen and Y. -B. Lin, "IP Connectivity for Gateway GPRS Support Node," IEEE Wireless Communications, Vol. 12, Issue 1, Feb. 2005, Pp. 37-46.

[29] 3GPP TS 23.234 (v9.0.0), "3GPP System to WLAN Interworking; System description", Release 9, 2009.

[30] Venkat Annadata, "802.16e & 3GPP Systems Network Handover Interworking", Tech Mahindra Limited, April 2010.

UNDER THE TERM