Grant Agreement no. 215056

Title:	***D2.3 Contextual Framework***
Editor:	*Eleni Kosta & Jos Dumortier (Katholieke Universiteit Leuven - Interdisciplinary Centre for Law & ICT)*
Reviewers:	*John O'Connell (Hewlett-Packard Centre de Competence France)*
	Vashek Matyas (Masaryk University)
Identifier:	*D2.3*
Type:	*Deliverable*
Version:	*1.0*
Date:	*20.11.2008*
Status:	*Final*
Class:	*Public*

Summary

With European citizens increasingly demanding community-related services and subscribing to a greater number of communities (i.e. social groups of entities sharing an environment, normally with shared interests), inter-disciplinary solutions for identity, trust and privacy management will be increasingly seen as a cornerstone for the success of online communities, especially in mobile-based usage contexts. PICOS specifically addresses these types of contexts by dealing with a number of privacy, identity and trust-related requirements of online mobile communities. The present deliverable builds a framework that in the first place integrates the legal, socio-economic, application-specific and technical views and rules on trust, data protection, privacy and identity management in communities. It is aimed to be generic enough to include universal requirements for community applications, which are reported in detail in deliverable D2.4 "Requirements". As the name of the deliverable indicates, this framework will also be "contextualized". For this reason we have identified the problem space by using three scenarios in the beginning of the document. These scenarios belong to three different categories of communities, i.e. Anglers, Taxi Drivers and Online Gamers, and clearly illustrate the problems that exist today in such communities.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Members of the PICOS consortium

Johann Wolfgang Goethe-Universität (Coordinator)	Germany
Hewlett-Packard Laboratories Bristol	United Kingdom
Hewlett-Packard Centre de Competence France	France
Universidad de Málaga	Spain
Center for Usability Research & Engineering	Austria
Katholieke Universiteit Leuven	Belgium
IT-Objects GmbH	Germany
Atos Origin	Spain
T-Mobile International AG	Germany
Leibniz Institute of Marine Sciences	Germany
Masaryk University	Czech Republic

The PICOS Deliverable Series

These documents are all available from the project website http://picos-project.eu.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

The PICOS Deliverable Series

Vision and Objectives of PICOS

With the emergence of services for professional and private online collaboration via the Internet, many European citizens spend work and leisure time in online communities. Users often consciously leave private information online, but they may also be unaware of leaving such information. The objective of the project is to advance state-of-the-art technologies that provide privacy-enhanced identity and trust management features within complex community-supporting services that are, in turn, built on Next Generation Networks and delivered by multiple communication service providers. The approach taken by the project is to research, develop, build, trial and evaluate an open, privacy-respecting, trust-enabling platform that supports the provision of community services by mobile communication service providers.

The following PICOS materials are available from the project website http://www.picos-project.eu.

PICOS documentation

- Slide presentations, press releases, and further public documents that outline the project objectives, approach, and expected results.
- The PICOS global work plan, which provides an excerpt of the contract with the European Commission.

Planned PICOS results

- *PICOS Foundation* is for the technical work in PICOS, and is built on the categorization of communities, a common taxonomy, requirements, and a contextual framework for PICOS platform research and development;
- *PICOS Platform Architecture and Design* provides the basis of the PICOS identity management platform;
- *PICOS Platform Prototype* demonstrates the provision of state-of-the-art privacy and trust technology to the leisure and business communities;
- *Community Application Prototype* is built and used to validate the concepts of the platform architecture and design, and their acceptability, in private and professional community scenarios;
- *PICOS Trials* validate the acceptability of the PICOS concepts and approach chosen, from the end-user point of view;
- *PICOS Evaluations* assess the prototypes from a technical, legal and social-economic perspective, and result in conclusions and policy recommendations;
- *PICOS-related scientific publications* are produced within the scope of the project.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Foreword

PICOS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1. Introduction	Eleni Kosta (ICRI – K.U.Leuven), Stephen Crane (HPL), Jos Dumortier (ICRI – K.U.Leuven)
2.1 Angling community scenario	Christian Kahl, Tobias Scherner (GUF)
2.2 Taxi driver scenario	Christina Köffel, Johann Schrammel (CURE)
2.3 Gaming scenario	Petr Švenda (Masaryk University), Christian Kahl (GUF)
3.1.1 Privacy, trust and IdM in existing communities	Stephen Crane and Pete Bramhall (HPL)
3.1.2 Reputation in online communities	Isaac Agudo (Universidad de Málaga)
3.1.3 Privacy technologies and PETs	Marek Kumpošt, Petr Švenda, Vashek Matyas (Masaryk University)
3.1.4 PETs in mobile environments	3.1.4.1 – 3.1.4.2 Georg Kramer (TMO) 3.1.4.3 – 3.1.4.6 Petr Švenda, Vashek Matyas (Masaryk University)
3.1.5 Anonymity and pseudonymity	Vicente Benjumea (Universidad de Málaga)
3.1.6 The assurance process	José-Luis Vivas (Universidad de Málaga)
3.2.1 Community platforms	Jean-Francois Coudeyre, John O'Connell (HPF)
3.2.2 Mobile technologies	Tobias Kölsch, Georg Kramer (TMO)
3.3 Business aspects of trust, IdM and privacy	Christian Kahl (GUF)
3.4 HCI and security, privacy, trust and IdM issues	Johann Schrammel, Christina Köffel (CURE)
4 Regulatory framework on privacy and IdM	Eleni Kosta, Jos Dumortier (ICRI – K.U.Leuven)
5 PICOS vision and mission statement	Alberto Crespo García (ATOS), Stephen Crane (HPL), Petr Švenda (Masaryk University), Georg Kramer (TMO), Eleni Kosta(ICRI – K.U.Leuven)

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Table of Contents

The PICOS project receives research funding from the Community's Seventh Framework Programme.

List of acronyms

AA	*Attribute Authority (X.509)*
AC	*Attribute Certificate (X.509)*
API	*Application Programming Interface*
CA	*Certification Authority (X.509)*
CED	*Computation with Encrypted Data*
CEF	*Computing with Encrypted Function*
CRL	*Certificate Revocation List (X.509)*
DES	*Data Encryption Standard*
DRM	*Digital Rights Management*
FTMGS	*Fair Traceable Multi-Group Signature*
GS	*Group Signature*
HSM	*Hardware Security Modules*
IDE	*Integrated Development Environment*
IdM	*Identity Management*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ITU	*International Telecommunication Union*
ITU-T	*ITU Telecommunication Standardization Sector*
Java Card	*Java-based platform for execution applets on smartcards*
JavaME	*Java Micro Edition*
JSR	*Java Specification Request*
MMOG	*Massively Multiplayer Online Game*
MMS	*Multimedia Messaging Service*
MULTOS	*Multi-application operating system for smartcards*
OCSP	*Online Certificate Status Protocol (X.509)*
PDA	*Personal Digital Assistant*

The PICOS project receives research funding from the Community's Seventh Framework Programme.

PETs	*Privacy Enhancing Technologies*
PKC	*Public-Key Certificate (X.509)*
PKCS#11	*Public Key Cryptographic Standard #11 [Cryptographic Token Interface (Cryptoki)]*
PKI	*Public Key Infrastructure*
PMI	*Privilege Management Infrastructure*
PRM	*Privacy Rights Management*
RFC	*Request for Comments*
RS	*Ring Signature*
SIM	*Subscriber Identity Module*
SMS	*Short Message Service*
SPKI	*Simple Public Key Infrastructure (IETF RFC specification)*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
TPM	*Trusted Platform Module*
TRNG	*True Random Number Generator*
TS	*Traceable Signature*
URI	*Uniform Resource Identifier*
X.509	*ITU-T standard for public-key infrastructures*

The PICOS project receives research funding from the Community's Seventh Framework Programme.

1 Introduction

As described in the "Description of Work" of the PICOS project, the objective of the project is to advance state-of-the-art technologies that provide privacy-enhanced identity and trust management features within complex community-supporting services that are built on Next Generation Networks and delivered by multiple communication service providers. The approach taken by the project is to research, develop, build trial and evaluate an open, privacy-respecting, trust-enabling identity management platform that supports the provision of community services by mobile communication service providers.

Looking into the future, it is clear that the justifications for individuals to trust those who process their information will be questioned more than ever before. The online digital world, while offering many benefits to individuals and organisations, brings greater risks to personal information and individual privacy. Personal privacy is being invaded, and individuals' awareness and concern over the attendant risks is increasing.

The need to understand these risks will lead to individuals becoming better educated and more questioning, partly because those who process information will recognise the need to be open and transparent. It is said that, currently, distrust is running high and increasing, and confidence is absent. We will thus see a shift towards individuals taking greater responsibility for the safety of their personal information and exercising informed choices. Personalised service will increase demand for personalised security. Individuals will seek guarantees, and choose service providers who offer the lowest risk at the greatest convenience. They will also look for indicators, e.g. a 'good privacy' mark. As individuals strive to regain control of their information, they will come to value bilateral/multilateral agreements that are fairly negotiated, rather than the mostly one-sided situation that we have today.

The Internet is evolving and problems are emerging that may call for a fundamental redesign of how the Internet works. This evolution is led by researchers, who need to take responsibility for the consequences of their innovation. As the risks change, security and privacy protection must evolve (European Commission, 2007). However, when we look at recent advances in technologies, we see more privacy-invading technologies being developed than privacy-enhancing ones.

Protective technologies, for example Privacy Enhancing Technologies (PETs), are developed to address particular concerns. In some situations, these technologies "make the impossible possible". For example, credentials that demonstrate entitlement to high value services, and which do not reveal the identity of the claimant, are relatively easy to conceive online but rare in the real world. Without these technologies, it becomes difficult to protect vulnerable people (e.g., children and the elderly), and new services are unlikely to be developed because they introduce insurmountable risks; without these technologies the risk of fraud would deter all but the most risk-seeking users.

Data represents power, and the ability to access vast pools of data that reflect the many aspects of a community, or of a country's population, is compelling. Reducing the cost of providing services to society is become increasing important, and being able to analyse such data in a reliably privacy-respecting manner is vital. The difficulty for designers of PETs is that they cannot easily anticipate secondary/future uses of personal information prior to collection. This means that data collection/consent policies must be presented in a way that ensures individuals understand the authority they give to data collectors and the potential long-term consequences.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Web 2.0 services also raise new privacy concerns. Researchers thus need to once again take responsibility for the consequences of their innovation. Designers need help to understand how to recognise the danger of the quick win solution, whether it is ID theft or DNA profiling. Security and privacy protection must be able to evolve in step with risks (European Commission, 2007). The 'point security solutions' that we have today, e.g. encryption, biometrics and anonymisation, will never be as satisfactory as a well thought-out system architecture.

As far as privacy is concerned, most privacy researchers are agreed that, wherever possible, the principle of data minimisation (anonymisation, pseudonymisation) should be the priority. These technologies return control to the individual, while also future-proofing solutions against unforeseen circumstances of which the designers cannot conceive. However, there are many situations where data minimisation is not the best option. Service delivery often requires information about the individual, whether to tailor the service or simply to deliver the product. Those that protect our society, especially law enforcement agencies and, to a growing extent, law-abiding citizens, are also uncomfortable with the prospect of being unable to identify those that present a threat.

Surveillance is here to stay, but currently, it has the image of technology designed to help the state rather than to help the individual. This might change as these technologies adopt more 'intelligent' privacy respecting modes of operation, instead of the current 'all or nothing' approach. Only then would the full benefit of surveillance, which many commentators can articulate but few technologists can deliver, be truly realised.

We are approaching a time when technology will, to a greater extent, assume the role of the human, taking decisions that the individual would otherwise take, and performing automated, autonomous actions on behalf of the individual. This means that technology will need to know much more about the individual it represents if it to confidently act on his or her behalf. The technology will probably need to take on the individual's identity. In fact, people might even have completely independent online and offline personas, perhaps existing in multiple virtual worlds. Clearly, this represents a significant potential risk.

Technologies are now emerging that should reduce, to a manageable level, the many different risks to privacy and identity that we have discussed. The ability of individuals to easily specify personal preferences (e.g. by using rule-based, policy/privacy languages), and for these preferences to be bound to the data they control through sticky policies, is becoming possible with the introduction of trusted computing platforms. Technologies that provide automatic privacy breach detection and notification, auditing and enforcement, tracking and data use/misuse notifications, all help to build consumer confidence.

All communities are now, and will continue to be, challenged when trying to cope with the conflicting demands of managing personal information. On the one hand personal information is required to build a successful community, but on the other hand it is a source of potential damage, if not properly managed. The present deliverable builds a framework that, in the first place, integrates the legal, socio-economic, application-specific and technical views and rules on trust, data protection, privacy and identity management in communities. It is aimed to be generic enough to include universal requirements for community applications, which are reported in detail in deliverable D2.4 "Requirements". As the name of the deliverable indicates, this framework will also be "contextualized". For this reason, we have identified the problem space by using three scenarios in the beginning of the document. These scenarios belong to three different categories of communities, i.e.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Anglers, Taxi Drivers and Online Gamers, and clearly illustrate the problems that exist today in such communities.

Starting from this point, the deliverable then presents the technical (architectural), legal and socio-economic options, available today, and possible business cases and the technical challenges. In particular, the "Contextual Framework" includes an analysis of technical architectures that focus on how the various mechanisms can or must interrelate. Among other matters, it verifies whether privacy-friendly / enhancing IdM models that are being researched in other European funded projects can be adapted and applied to communities. The legal analysis of the technical architecture will focus on the specific rules applying to privacy, data protection and e-commerce. As the services are provided through electronic communications networks, the provisions of the e-Privacy Directive should be taken into account, assessing where they are applicable and the specific obligations they introduce for the service providers. The socio-economic analysis examines which properties of trust, data protection, privacy and identity management are important in which types of communities. The legal contribution to this deliverable describes the general legal framework, which is further specified as detailed legal requirements in the "D2.4: Requirements" deliverable.

2 Starting up with PICOS via user scenarios

Before presenting the technical, legal and socio-economic options that are available today, it is important to illustrate why PICOS is needed for today's communities. In this chapter, we present three representative scenarios, which belong to three different categories of communities, i.e. Anglers, Taxi Drivers and Online Gamers. Through these scenarios, it will become obvious what the problems of such communities are with regard to privacy, trust and identity management. In each of these scenarios, it will be discussed what the added value of PICOS is and how PICOS can help the users of these communities.

2.1 Angling community scenario

2.1.1 Context

Recreational fishing has a long history and is becoming more and more popular around the world. As a consequence, it has a growing socio-economic and ecological impact, which is suggested by several recent studies. For example, a recently published socio-economic study from Germany showed that recreational fisheries have a productivity effect of about 5.2 billion € in Germany, with approximately 52,000 jobs depending on the expenditure of anglers (Arlinghaus, 2004). The jobs generated by recreational fisheries have been found to be of equal magnitude to the whole commercial fishing sector in Germany. Important tourism and gear industries crucially depend on recreational fisheries. The overall benefit to the German economy was more than 6.2 billion € in 2002 (Arlinghaus, 2004). Similar impacts in other highly industrialised countries have also been reported in other studies, such as (Outdoorfoundation, 2007).

In addition to its economic relevance, recreational fisheries systems also provide tremendous social benefits to society. Fishing for recreation is an activity that lies at the core of the life-style of millions of people in Europe and world-wide, and has social and cultural benefits, including psychological and health-related aspects.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

2.1.2 Users

Regarding fishing as a common interest of millions of people worldwide, the relationships between these enthusiasts form various kinds of communities. Such communities may be organized as clubs or associations, or networks of loose and informal relations. The members of these communities interact in various ways. For instance, they arrange meetings, share information about their last angling trip with friends, or just inform themselves on weather or environmental information for their next trip.

One such community, which represents an economically powerful sector within the tourism industry, is the sports fishing community. It is stated in the aforementioned study (Arlinghaus 2004), in which the author analysed different statistics, that there is no exact number of recreational fishers in Germany available, but that more than 3.4 million Germans go fishing from time to time.[1] Normally, fishing trips are characterised by different subsequent phases: the planning phase, the event itself, and a recollection phase (Arlinghaus, 2002). In the recollection phase, fishers maintain their equipment, sort their taken pictures, and synchronise these pictures with location data tracks (in the case that they are using such technologies).

Due to the fact that fishing is a location-dependent activity, and that fishers do have some need for communication and the sharing of information (such as hints, images, knowledge, etc.) among each other, mobile technologies could help to satisfy these needs. Therefore, the users' demand for accordant mobile services increases shortly before the event, in order to coordinate with others or get and share information about the fishing location; and during the event, in order to stay connected and to immediately access location related information (e.g. weather conditions).

The aforementioned sport fishers could benefit from various mobile interactions. These interactions depend on many factors such as the interactions between fishers, interactions between fishers and local authorities, and multilateral interactions. In the case of interactions between different fishers, one could differentiate other subcategories of fishing, such as fly-fishing or carp fishing. In the first case, the fishing is often characterized by frequently changing fishing places during one trip, while carp fishers normally remain at the same place. Fly-fishers might interact with each other in the same area to have a meal together. In contrast, carp fishers might use the time between two catches to broadcast their latest catches to their friends.

Interactions between fishers and local authorities comprise, for instance, not only of the online acquisition of fishing permits (Carlson 2008), but also the getting into contact with environmental agencies to report water pollution and increased fish mortality.

Multilateral interactions such as sharing pictures, or recommending favourite fishing places and other more or less secret information, do often require more than only one party with which to interact. This is often done via community platforms where users administer their account, including privacy settings. One way of applying these settings is to define how much access other users may have to sensitive data, the quality of data they have access to, and other restrictions. One of these features applying privacy-preserving mechanisms is, therefore, allowing only persons with a high level of

[1] The number of recreational fishers in Germany is estimated to be between 3.3 million and 5.8 million people, depending on the statistics.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

trustworthiness to have access to information on lately visited fishing places, with exact geographic coordinates and the corresponding catch statistics. Besides such confidential information, other information could be exchanged via such community platforms. Popular information for anglers concerns, for example, well-stocked tackling shops, where to acquire permits, and bait restrictions in certain water courses.

To meet such needs for the provision of adequate community services, mobile technology could be used, in particular, for activities such as:

- Provision, collection, storage and sharing of fishing related information (e.g. personal statistics, information about environmental conditions like weather, water quality, etc.).
- Analysis of fishing statistics (e.g. regarding fishing quotas).
- Provision of legal information (non-fishing seasons, etc.).
- Acquisition of permits.
- Delivery of services and products (e.g. physical services/products like lures).
- Navigation services.
- Finding of fishing hotspots (places with a high probability of catching fish).
- Identification of fish types.
- Provision of recommender systems for angling places.
- Utilisation of fishing-related services (e.g. monitoring of the development of fish populations).

2.1.3 Relationships

As outlined before, fishers may be organised in numerous different communities and the aforementioned sport fishers represent only one of them. Consequently, the members of such an angling, or fishing, community could be related in many different ways. In order to provide an adequate support for them and to properly design the respective mobile services, the relationships among the members and their context need to be depicted.

The following picture shows in detail the interconnections between the members of an angling community, the mobile community platform and their services, and further contextual elements, such as databases and public services.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

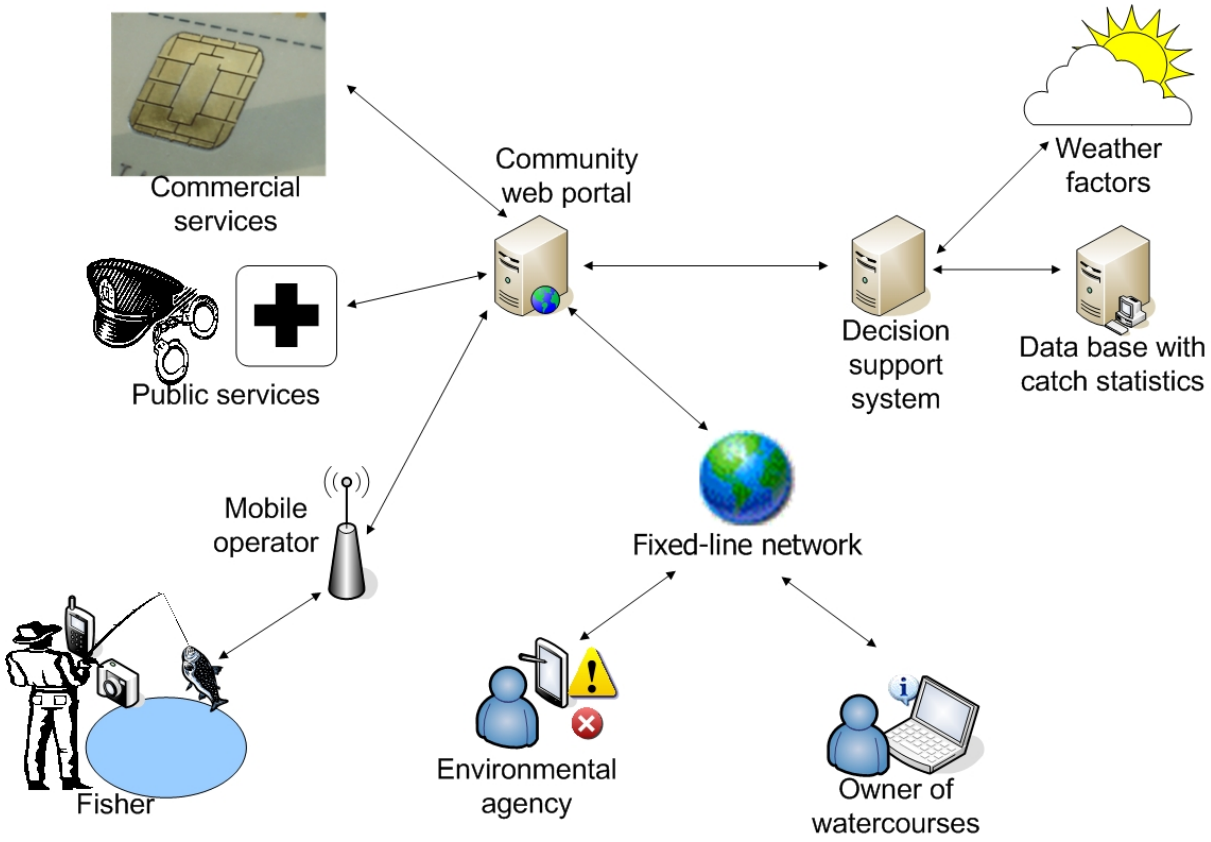

Figure 1: Mobile Angling Community and its stakeholders (Scherner, 2006)

2.1.4 Use case

To gain a better understanding of the needs of an angling community and the resulting potential for mobile support services, the example of a single person, named John F., is now given, which is an excerpt from (Scherner, 2006).

"John F. is an urban man, who is working for a company, which develops e-collaboration tools. He lives near the North Sea and normally he visits the same fishing place close to his residence at the coast. However, for his next holiday, he decided to book a special offer for a fishing holiday in the Alps to gather new experiences with fresh-water fish.

After arriving at the booked hotel, he recognises that he has forgotten nearly everything about how to distinguish unerringly between fishes with similar outer appearance and about the preferences of bait and living space of certain fish groups. He had learned all this during his youth, but lost it over the years not fishing in foreign areas.

During supper, he tries to get in contact with local anglers. Naturally, they protect their knowledge about their favourite fishing places and most popular baits and John has to leave without any inspirations for the coming days. A little bit worried and sceptical, he starts very early the next morning trying to find a nice fishing place around his hotel. Following a small valley with a mountain stream with his car, he tries to discover an attractive fishing place from the streets. Unfortunately, trees and rocks obstruct his view. After a while, he decides to take the next parking place, and go down to the water to find a pleasing place.

Nevertheless, his actual problem that he has forgotten how to attract certain kind of fish with the right bait (and even worse not knowing which kind of fish he should expect in such a river) complicates the choice of equipment and fishing method. He decides to go for a pose and earthworms and to enjoy a sunny morning – unfortunately without having a single snap.

During his lunch, he sees that fish quickly catch maggots that are falling from the trees. Therefore, he immediately changes over to the apparently better bait and gets rewarded with several snaps within a few minutes. After some failed attempts, he finally accomplishes to hook a pugnacious fish, wangles to get it into his brailer and starts carefully examining his catch. Consulting his fishing permit he tries to figure out which kind of fish this might be. Finally, he concludes that it may be one of a few possible fish species but he is not able to find out which on exactly it is.

However, this is not a satisfying answer, because all these species have different open seasons and minimum length. Furthermore, one of the species, which the fish could belong to, is protected throughout the year. John is very unsure how to proceed. On one hand, taking a protected species with him will endanger him to get a fine of several thousand Euros, if the local authority controls him. On the other hand, releasing the fish might mean to go home empty-handed today. He tries to call a friend who is very experienced in such fishing affairs using his mobile phone but only reaches his mailbox. John ponders with the decision on how to proceed for a while and decides to release the fish to avoid potential trouble.

On his way back to the hotel he remembers that some travelling anglers share their knowledge over different online fora. This would be very helpful, he thinks, regarding his experiences on this day, for gaining more information and sharing knowledge with others. However, he fears a bit the disclosure of private information and the loss of control over the circulation of such information. Ideally he concludes, there should be ways to include privacy mechanisms in community platforms and their services, to ease up anglers' life" (Scherner, 2006).

2.1.5 PICOS added value

The outlined use case example already shows that there is the potential to support angling communities with mobile services. In addition to the identified users and their needs, however, the question arises of what added value the PICOS project could provide in this context.

To answer this question, it should at first be emphasised that the traditional perception, that anglers are naturalists who neglect the use of modern communication techniques (e.g. Internet, mobile devices), is not true anymore. With increasing participation by the younger generation, recreational angling has adopted a high-tech attitude, involving fishing equipment as well as the use of the modern communication technology. The participation of anglers in numerous Internet portals dealing with

their interests has proven that the majority of recreational anglers acknowledge the coupling of their activities to a technical environment.

The convergence of telecommunications systems technologies and Internet technologies, especially in a mobile context, such as the one that PICOS is focusing on, will allow the delivery of information to the angler while being at the waterfront. In consequence, the use of mobile devices is in favour here. But within the angler community, there is not only the need for reliable and peer-reviewed knowledge about fish from an information system like FishBase (http://fishbase.org/) (Froese, 2008). Such communities also have a need for the more dynamic exchange of information between fishing individuals. Here, the spread and rapidly increasing power of mobile communication devices can be harnessed. At the same time, aspects of privacy and trust have to be ensured while personal and sensitive information is exchanged. PICOS could, in particular, provide answers to such questions and needs, which should serve as a basis and guidance for the design and development of appropriate mobile services.

2.2 Taxi driver scenario

2.2.1 Context

Taxicabs have a long history. They provide transportation services to people, especially in urban areas and areas where other public means of transport were/are not yet available. Generally, taxicabs are a part of paratransit transportation, which is the layer between private automobiles and public transport. There are three categories of paratransit systems: hire and drive systems, hail or phone systems, and systems that require prior arrangements (Bailey and Clark, 1987 - Bailey and Clark, 1992).

The coordination and planning of a taxi fleet requires a lot of organisational work. The taxis have to be sent to the customers, and in time without any delay. Furthermore, the waiting time of the customers has to be minimised and the booking of the cabs has to be made efficiently. Currently, different systems are employed for this process, such as radio communication, global positioning systems (Liao, 2003), mobile phones and location based services (Silva and Mateus, 2003).

2.2.2 Users

Small taxi companies usually do not use radio systems or location based services. They instead rely on mobile phones to take the orders from clients and to coordinate different cabs. Accurate coordination is especially important in the case of rather small taxi companies that run pre-booked services. The installation of a radio communication centre for the coordination of the cars would not be economical for only a few cabs.

The planning is either done using simple software, notebooks, or in the head of the owner of the business. Furthermore, the image of the company to the outside and the relationship to regular customers is very important. The cars have to be clean and the drivers have to have a trustworthy and appealing appearance. This is in part because companies are entrusted with credit card information given to them by customers.

Furthermore, one can distinguish between coordination within one company (community) and coordination between different companies (communities) that collaborate with each other (thus creating another broader community). To meet such needs through the provision of adequate community services, mobile technology could be used, in particular, for activities such as:

- Provision, collection, storage, coordination and sharing of customer related information (e.g. name, address, credit card information, etc.).
- Analysis of cab efficiency (e.g. calculation of vacant periods).
- Acquisition of new customers.
- Coordination of cabs within a company.
- Coordination of cabs between different companies.
- Navigation and route planning.
- Provision of recommender systems.

2.2.3 Relationships

As mentioned above, different taxi companies collaborate with each other when needed. In case of overbookings, they delegate the orders to other taxi companies with which they have established trusted business relationships. Collaboration is also established for longer distance trips to find, for most of the time, a fare for both directions. In order to make this system work, the companies have to trust each other. As there is always the possibility of one company taking away the other companies' customers, trust becomes an essential part of collaboration. The amount of information given to other companies can be restricted, while information within the company should not be restricted.

Furthermore, trust between the company and the customers has to be established. The customers trust the taxi company with their credit card information. This trust implies that the car company will not misuse this information nor share it freely with others.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

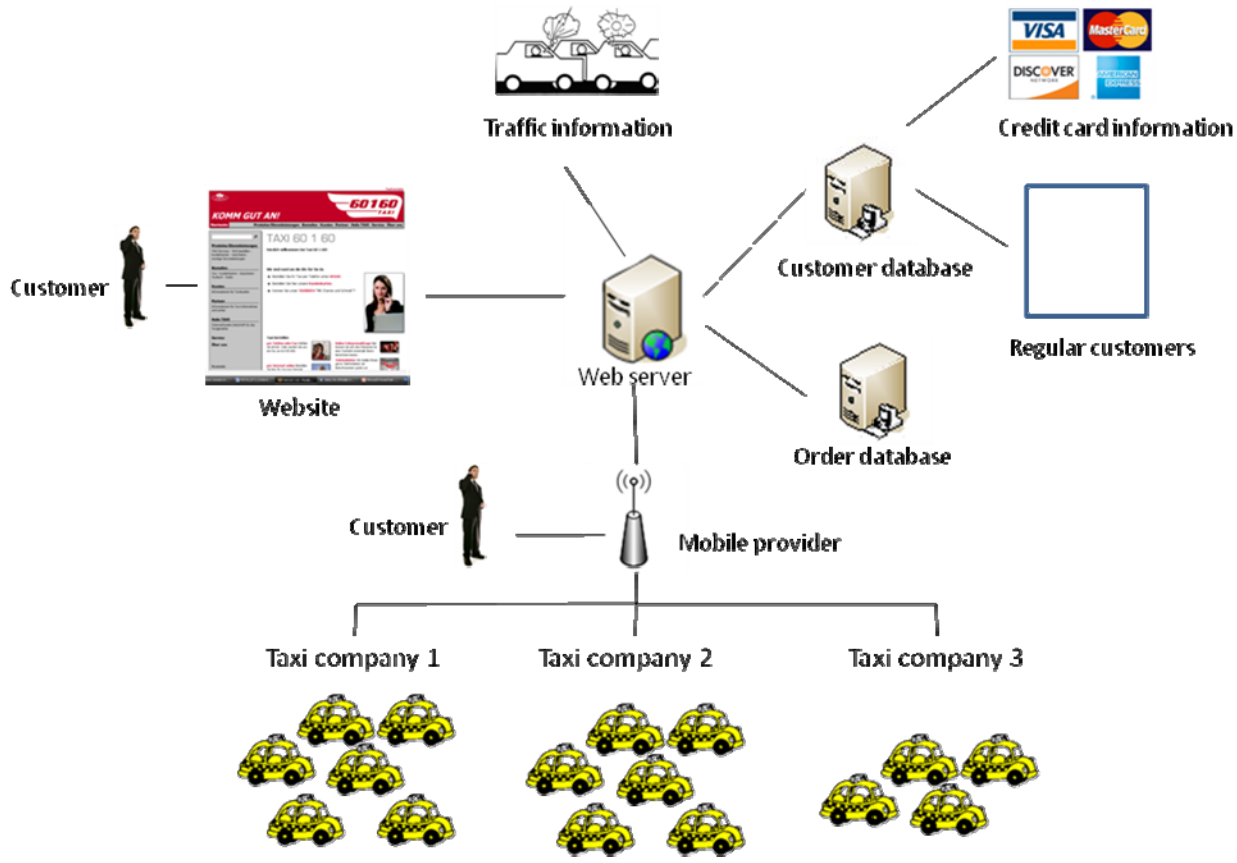

Figure 2: Pre-order taxi community and its stakeholders.

The following scenarios give a short overview of the possible uses of the PICOS project.

2.2.3.1 Push to talk scenario

Sarah is the owner of a small pre-order taxi company, comprising of three cars. The business is family owned and was created by her father about 30 years ago. Since three cars are more easily coordinated using mobile devices than a person employed in a central cb radio station, only mobile devices are used. Recently, Sarah adopted the PICOS technology for her taxi service.

Each day, customers call her on her mobile to arrange pick-ups. Over the last few years she has acquired a larger number of regular customers that prefer her service because of her reliability. Even when her cars are overbooked, Sarah reliably organises the pick-up. In such a case, the PICOS project eases the coordination with acquainted and trusted taxi companies. The PICOS system allows Sarah to reach all the business partners she trusts only by choosing the desired network and pushing one button. Therefore, a lot of time that would be spent on calling the different companies individually is saved. Furthermore Sarah can do this kind of coordination while driving, because she does not have to look up all her phone numbers, which means she can concentrate on the street.

2.2.3.2 Cooperative website

Roger founded his pre-order taxi company about 2 years ago. Before that, he was taxi driver for a big company. Taking all his knowledge, he decided to become self-employed and opened a small company with four cabs.

His prior knowledge helped him set up the necessary infrastructure. Using the PICOS technology, he is running a cooperative website. Through this site, customers can book cars easily over a secure page. Regular customers also have the possibility to create an account and log on. Ordering a cab now takes less than a minute. As soon as the customers submit the request, Roger and his co-workers receive an encrypted e-mail. Since the PICOS technology runs on a central system that connects the handheld devices of all taxi drivers in the company and synchronises the appointments and pick-up times, it immediately displays the desired pick-up time and location in the calendar. It is then automatically assigned to the driver who best fits the job, in consideration of the other bookings. In case of overbookings, a warning sign is displayed to Roger and his co-workers.

Roger can easily accept an appointment or delegate it to business partners in the case of overbookings by just toggling one button (either “accept” or “delegate order”) on the display. An e-mail to confirm the modalities of the pick-up order (date, time, estimated price) is sent to the customer. The associated companies that can be contacted in case of overbookings are also part of the network. Using the same method as described above, these companies can also accept or reject the appointment.

The trust between the customers and Roger’s company is established through different channels. Firstly, all communications are transmitted using secure channels. Secondly, the taxi company has obtained credentials from the government that designate it as a pre-order cab company. Through these online credentials, the users are assured that Roger’s company is in fact a taxi company. Thirdly, PICOS enables the customers to track all information they submit to the company’s website. This includes credit card information as well as personal data. The website is partially financed by advertisements and therefore it is essential for the customers to know where their data has gone and that it is not given to other companies. Furthermore, the customers get an e-mail stating the name of the driver and the number of the car that is going to pick them up. In case of overbookings or changes, the customers will also be notified either by e-mail or by text message.

2.2.3.3 Security solutions for BlackBerries

At CMO cabs, a small pre-order taxi company with three cars, the entire booking system is based on phone communication and e-mail services via BlackBerry phones. The customers can book cabs by calling the company or by writing an e-mail.

Since the possibility of somebody losing a BlackBerry or getting it destroyed is quite likely, the company has recently adapted the PICOS framework. The framework establishes trust between the company and its customers. Daily backups of the stored data (e-mails, contacts, appointments) and credentials for the user of the phone prevent data loss and access by unauthorised personnel.

2.2.4 PICOS added value

The scenarios introduced above show the possibilities that the PICOS system can offer to the taxi community. In this context, the PICOS system allows for an optimised coordination of cabs within a company and between acquainted taxi companies.

While previously (mobile) phones, paper sheets and the human brain were used for the coordination and arrangement of the pick ups, the employment of mobile technologies makes this system more efficient and reliable. While critical situations such as overbookings could be overlooked in the past, they are now highlighted by the system. Time consuming searches of the address book for potential partners is unnecessary, and sheets of paper that can be lost or simply disappear do not exist anymore. Instead, the information is stored in a database and backups are made frequently.

The advanced security paradigms implemented in the PICOS system foster trust between different companies and between the offering company and its customers. Only the customer information needed to carry out the order (e.g. pick-up location and time) is immediately delivered to the taxi drivers, and the customers get valuable feedback (e.g. name of taxi driver). Information that the driver does not necessarily need to execute the order (e.g. credit card information) is not submitted. The use of mobile devices eases the employment of the system in a mobile environment such as taxis, and allows for the flexibility needed.

2.3 Gaming scenario

2.3.1 Context

Computer and video games today entertain many people around the world. Playing games online with real players instead of artificial computer players (like in single player games) has become increasingly important over the last number of years. Due to ubiquitous Internet access and increasing connection speed, this form of multiplayer gaming has now become available for millions of people.

There are various types of online games. Next to ad-hoc or casual games, and extensions of existing single player games, the so called “Massively Multiplayer Online Games” (MMOG) are one of the most widespread forms of online games. These games exist only online. Therein, players are usually part of a huge online world (e.g. in a fictional country or island), which they may build up, extend or explore to a certain degree with their in-game character, the so-called “avatar”.

The players have to complete various tasks, such as solve riddles, collect particular items, fight against enemies or reach specific game states. Therefore, such games do not have a defined goal, such as conventional single player games. Instead, the game concept is based on the continuous evolvement of the world and/or the players’ characters. To achieve this goal, collaboration with other players is usually required. Consequently, MMOGs can often be played for an unlimited time, as long as a player is subscribed to the game.

According to (MMOGHART, 2008), in 2007 more than 16 million players were active subscribers of a MMOG. “World of Warcraft” (WoW) with 10 million members and “Lineage II” with 1 million members are two of the most played ones.

Beyond the entertainment aspect, such games also form specific types of communities, as they unite millions of players. In this respect they could be compared to online communities such as fora or social networking sites (e.g. MySpace, Facebook), as their members also share a common interest through their playing together. Additionally, the members are not only part of the same game, but are also organised in various groups (sub-communities) within it. They interact with players in their own groups and members of other groups. This interaction also comprises of different forms of collaboration and collaborative strategies (Fleming, 2004).

With increasing technological progress in the development of mobile devices and the growing availability of mobile Internet, gaming communities are about to get more and more mobile. First approaches to make existing online games also available on mobile devices are already in development (Massiverly, 2007; Pocketgamer, 2008). Among the reasons for this development is the need of people to take their games with them wherever they are, and thereby the need to accommodate the mobility of these users. The aspect of location independence, which characterises mobile services, is of special importance in this context, because various in-game activities are time-dependent. They require simultaneous actions, e.g. from members of one clan or a member of the same group, or actions at a specific point in time, e.g. taking part in a battle, which may be decisive for the completion of a task. Some other tasks (e.g. management of resources) may also be processed while being en-route, as they are time-consuming but necessary.

One gam, that has already taken the step into the mobile world is the strategy game “Travian” (http://www.travian.com/), which is popular in more than 40 countries. Travian is a browser-based strategy game, situated in the ancient Rome. The players are building the city and its army, fight and trade, and communicate with other players to form alliances. Since it is browser-based and does not need any installation of additional software, the game can be played on mobile devices. Regarding commercial aspects, there are, so far, no targeted advertisements and no prize money for winning. However, there is some money flow from players to game developers for virtual gold coins, which speed up actions like the construction of buildings.

2.3.2 Users

The users of games like Travian or WoW cannot be easily clustered by specific demographic or socio-cultural characteristics. In fact, there is no typical Travian or WoW player, but a wide range of player types (Yee, 2007). For playing, no real name is required. Instead, players usually use fixed nicknames (which cannot be changed during game). Profile information consists of age, gender, address and optional additional properties.

Regarding game play in Travian, the nature of this game conveniently allows one to play at all times, and gives the possibility of temporarily (e.g., few hours, one day, or sometimes even several days) interrupting play at any time. Thus, the group of players in this game consists of students as well as office workers and people with only limited access to Internet (e.g., in the evening only). The players are able to be geographically distributed; the main unifying factor is only the default communication language of the gaming server.

In any case, the players are driven by the same shared interest, which leads them to collaborate with each other and to organise themselves in groups. This implies a certain demand for trust, because the progress within the game is often strongly connected to a working collaboration. This collaboration assumes a trustful exchange of information. In order to improve relationships, physical meetings of those who know each other from the game sometimes take place, e.g. due to the fact that they are part of the same group.

Levels of trust are not only given by the personal knowledge of the player (pre-established trust), but are also based on the players' behaviour in the game. The process of building trust in the latter case is usually based on activity in the game forum, and reliability in agreed upon actions (attacks/defences), which lead to more and more trusted players within alliances. A need for deeper trust exists between leaders of an alliance and geographically close members that can actively support each other.

Further, there are explicit rules for illegal behaviour in Travian – the so-called "Travian rules" and "Travian ethics". They are enforced by server-side monitoring daemons, encoded limits on resources, and the possibility to ban players based on evidence provided by other players. In addition, only one account per person is allowed as a protection against a player supporting him or herself using multiple virtual villages.

Regarding technical aspects, the players need some degree of continuous Internet connectivity, but even a few days without interaction usually does not harm a player significantly. However, players with frequent access have a competitive advantage, as they can actively react to incoming attacks (by moving their army, or ask for support from other players). The players who are temporarily without connectivity can set up two "assistants" with limited gaming possibilities, but only for 14 days without a login of the original player (i.e., legitimate account owner).

2.3.3 Relationships

As stated before, players in MMOGs are often organised in groups within the game. In some games, especially role playing games, the existence of such groups and participation within them are essential elements of the gameplay. In strategy games like Travian, players usually need to form alliances with other players. They have different types of communication tools, e.g. chat or text/voice messaging. Further, they can use additional external voice chat or similar applications to talk during the game and e.g., to develop strategies or coordinate their behaviour (Nardi and Harris, 2006).

Relationships normally start when players meet each other in the game. This may happen by coincidence or due to the fact that they already know each other from real life or even other games (and therefore meet consciously). The relationships, which are built within the game, can be continued and intensified within groups. Moreover, just as real-life relationships are transferred to the game, online relationships are also sometimes transferred to the real-life. For instance, on one hand, according to a recently published study, schoolmates and friends often play together. On the other hand, players who are members of groups sometimes meet each other physically, and thereby extend their relationship to the real world, maybe just to get to know the persons behind the avatars, or even to better coordinate possible future strategies (Nardi and Harris, 2006).

Regarding again the example of Travian, the first contact is often made through fights. Communication later follows to either warn an attacking player of consequences, e.g. that the player being attacked is a member of an alliance, or to agree on some type of royalty fee to prevent further attacks. Some players can also exploit the fact that they are stronger to blackmail the weak players (by demanding, e.g., taxes for protection and non-attacking).

Regarding the origin of relationships between players, three main types of prior relations can be identified:

- No relations:
  Complete newcomers, with no previous relations to other players (majority of players).
- Virtual relations:
  already existing relations from other online games (mainly mature players).
- Physical relations:
  prior physical contact from school, work (minority of players).

The types of relations that evolve during the game may be distinguished using the following four categories:

- Neighbour relation:
  relation to direct neighbours on the map of virtual world (starting as competitors, later neighbours are usually either destroyed or become alliance members).
- Intra-Alliance relation:
  relation to a members within the same alliance.
- Inter-Alliance relation:
  positive or negative relation to a member from another alliances.
- Personal relation:
  personal relation after a personal meeting (in real-life).

To maintain relationships in some games, players have their own friends list, which works in the same way as friends lists on social network sites. These list all other players who have confirmed their friendship with a player (friends), and inform the player about friends who log on to or who log off from the game. Furthermore, in some cases (e.g. WoW) the list reveals information about the current level and location of friends, or their online activity (Travian) – awareness aspects. Thereby, it is a means for players that allows them to stay in touch with other players and to share information about the game progress of each player.

Aspects of trust and privacy are relevant to these forms of interactions, as they are the basis of a trusted collaboration. However, in contrast to other communities, the relationships may be of shorter duration because of more dynamic game play, which might cause players to change memberships of groups, or players who are simply leaving the game. Of course, this is only the case if relationships are not continued outside of the game.

In Travian, the underlying platform provides various communication tools. These are message-boards, which allow 1:1 communications with selected players, as well as 1:N communication for all players inside an alliance, and online chat, where everybody is allowed to participate. The platform further provides statistics about game progress, e.g. about ongoing and past attacks, which are visible to all members within an alliance (number of involved soldiers, results, etc.). Travian alows a wide range of

different interactions that players may arrange. They are able to manage resources (e.g. soldiers), coordinate and launch attacks, or build alliances. Further, they can exchange relevant information and have the possibility to negotiate or discuss strategies.

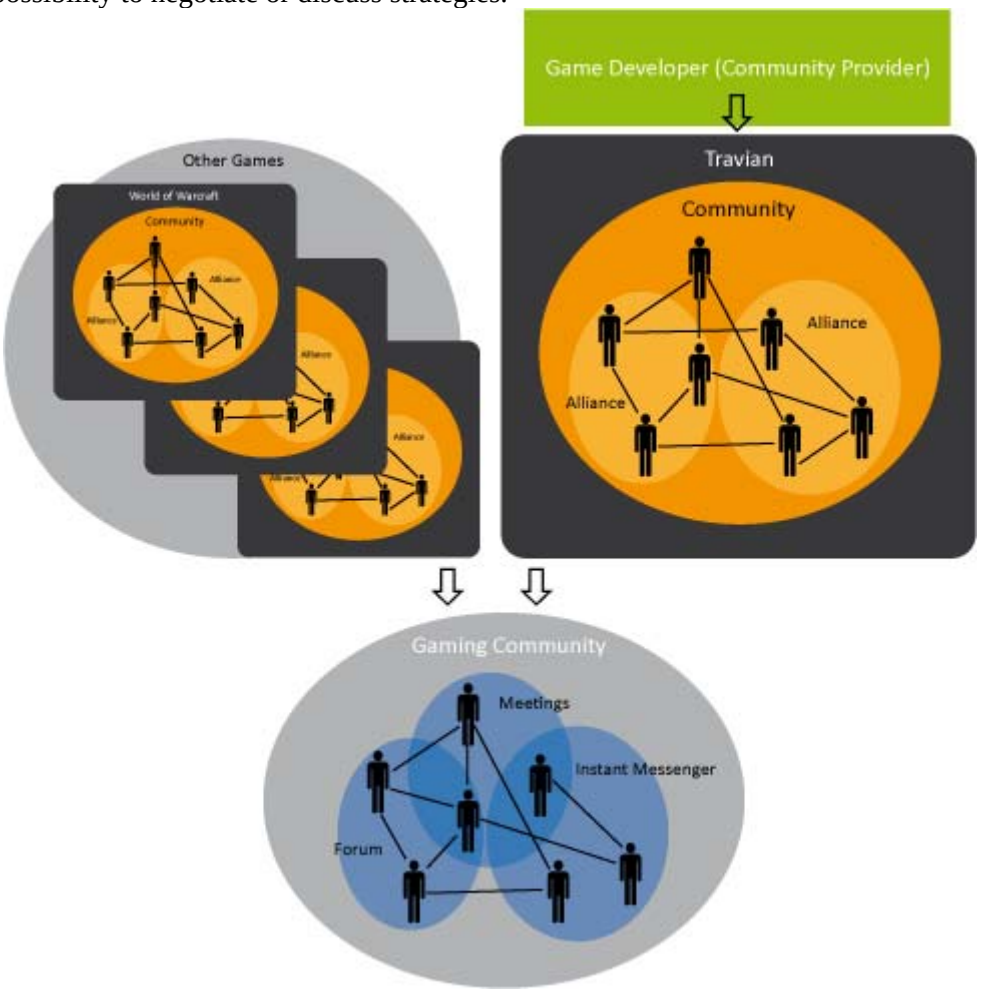

Figure 3: Relationships of gaming communities.

2.3.4 Use Cases

Among typical use cases in Travian, the coordination of attacks and defence can be mentioned. The coordination of a new attack involves the exchange of general information to all members of the respective alliance. The details, however, are communicated only between selected members of the alliance. A problem which occurs in this context is the existence of "substitutes" (persons with temporal access to someone else's account) who are, otherwise, from other alliances, as they can read the messages from internal forums and also from direct 1:1 communications. Unfortunately, this cannot be controlled by the alliance. Defence coordination usually contains the broadcast of support requests to all members of the alliance.

One further problem against the background of these typical interactions is so-called spying. In this scenario, a member of alliance A is corrupted by alliance B to provide information about the internal actions of A to B. Such activities are sometimes processed via dead accounts of inactive players. Even though accounts may be deactivated, and further separate message-boards were introduced to limit available information to members of alliances and limit the severe threat of spying, the danger of such actions has not been completely eliminated.

2.3.5 PICOS added value

Considering the previously mentioned aspects of gaming communities, three main needs can be identified, which should be addressed in the future.

- At first, stronger **interconnectivity between different gaming communities**.
  So far, the players of each online game build their own community, which consists of various sub-communities (clans, guilds, alliances, etc.). But many players do not only play one specific game, and are thus part of more than one such community. Due to this, the need for communication and interaction tools, which allow access to multiple games and thereby let players connect independently of specific games, is probable to increase. Such interconnectivity between gaming communities would also require considering aspects of interconnected trust and reputation.
- Second, a stronger **connection between the on- and off-line worlds**.
  Many players are organized in sub-communities (e.g. clans), who also exist physically in the offline world and, consequently, represent a mechanism to connect people on- and offline. To maintain these relationships, an appropriate infrastructure is needed to allow communication and interaction within these closed groups, even outside of a game like Travian or WoW itself.
- Third, an increase in the **mobility of gaming communities**. Considering the mentioned fact that gaming communities will tend to become more mobile in the future, players need seamless access not only to the games itself, but also to the respective supporting community services.

In consequence, the players could benefit from PICOS, at first, by the provision of community tools and services that address the identified needs, and which need to be accessible in a mobile context. These services and their underlying platform have to be game and location independent, to support the multiplicity of memberships in a few different games and, at the same time, support the real life dimensions of community structures.

Additionally, with all these needs, aspects of trust and aspects regarding the usage and revelation of personal information (Privacy, IdM) have to be considered. However, it should be noted that the previously described aspects may not be valid for all types of online games. As games range from strategy and role-playing, to action and various sports games, the services for the correspondent communities have to be adaptable.

3 State of the art

3.1 State-of-the-art technologies

3.1.1 Privacy, trust and IdM in existing communities

3.1.1.1 Introduction

All communities are now, and will continue to be, challenged when trying to cope with the conflicting demands of managing personal information. On the one hand, personal information is required to build a successful community, but on the other, it is a source of potential damage, if not properly managed. In this section we describe the current state-of-the-art technologies designed to deliver privacy, trust and identity management services to communities and community members. We subsequently categorise each technology according to the contribution that it makes to communities, especially mobile communities. Finally, we identify the five technologies which we feel would make the greatest contribution to enhancing community privacy, trust and identity management.

Privacy Enhancing Technologies (PETs) are the subject of intense research; the term spans a wide range of very different approaches to enhancing privacy, many of which can be used concurrently in a complementary fashion. These technologies are continually evolving, as is the understanding of how they can be applied to practical situations. Consequently, we can at best only provide a snapshot of PETs and their role in today's world. However, we can speculate with some degree of confidence on how PETs might evolve, which we begin to do in this section, and do more fully in section 3.1.3. Some of the technologies presented in this part will be further analysed in more detail in the following sections in the context of specific technologies.

Trust is predominantly concentrated around trusted platform technologies, e.g. TPMs, and reputation management schemes, similar to those used by Amazon and eBay. Virtualisation technology, which offers isolation and containment security primitives, is receiving significant attention too. After-the-event controls, e.g. audit and reporting, is another area where consideration is being given to more robust solutions that offer a sense of guaranteed functionality.

IdM is a complex but generally well understood area. It includes identification of the individual entity – i.e. unique identity, biometrics, pseudonymity – and the management of identifying information. The latter is the more difficult of the two to deal with in practice, mainly because so many different interpretations and requirements exist, and because, when done properly, it does require rigorous processes. A federated identity, in which an identity established with one controlling authority is valid with another, is conceptually a nice solution, and potentially popular with users, but requires significant trust between relying organisations. This trust extends to liability, but is often the stumbling block for implementation.

Privacy, trust and IdM converge when high value is placed in an identity. The theft or misuse of an identity raises privacy concerns, which in turn lead to distrust. Managing identity, possibly at a personal level, is becoming a priority; we are now thus seeing established yet rarely used identity management techniques like pseudonymity and anonymity becoming increasingly important.

The motivation for Privacy/Trust/IdM technologies is currently based on: 1) a user-driven desire to control access to and use of personal information, prompting the idea of personal privacy preferences, and 2) a similar desire for stronger, robust access control and authentication. The perceived increase

in trust derived through using active notification and access to a reliable risk indicator is helping individuals better understand personal exposure.

3.1.1.2 State-of-the-art privacy/trust/IdM technologies

When considering different types of technology, especially PETs, it is very easy to focus on exciting techniques rooted in cryptography and other esoteric principles. It is true that some of the most widely published and intellectually influential developments in recent times do have these origins, but many conventional security techniques can still have a significant bearing on privacy and identity management. For example, strong access control, isolation between machines and domains, and secure backups all enhance privacy.

Given the broad range of technologies, it is perhaps better to think in terms of systems rather than discrete technologies (Marsh, 2008). This broader appreciation demands that PETs work in harmony to fulfil a higher-level objective.

In the following table, we present a first categorisation of the technologies according to whether they have been designed to specifically satisfy privacy, trust or general security goals.[2]

	Privacy enhancing technologies	
Name	Description	Application to PICOS
Privacy Rights Management (PRM)	Similar to Digital Rights Management (DRM), PRM guarantees, as far as technology will allow, that the use of personal information is restricted according to limitations imposed by the technology that processes the information. For example, it may be possible to read but not copy information.	Any community that relies on a mobile appliance may be able to rely on the design of the appliance to enforce how the information sent to that appliance is used. For example, a mobile phone could be designed to delete downloaded data after a fixed period.
Controlled sharing	Similar to Privacy Preferences, controlled sharing implies that the originator of the information is its owner and can dictate how the information is processed by others who receive the information.	Community members who share their information with the community, but are not able to determine beforehand who might see the data, can state restrictions that control access to the information by others.

[2] Parts of this list (but not the definitions) were taken from (Koor, 2004).

Cookie management	Cookies which store personal information on a user's appliance often, possibly unbeknown to the appliance/information owner, need to be monitored and, if necessary, deleted.	Although not so commonplace in mobile networks, cookies are a potential risk that users will have to manage themselves. Easy-to-use tools will need to be made available for this purpose.
Personal Privacy Profile and Privacy Preference management	Personal Privacy Preferences state how an individual's information can be used by others. Privacy Profiles are a simple way to express preferences that apply to similar situations in which information is shared. They can be used to represent a base-line set of Privacy Preferences.	Community members who share their information with many other users, or in many different situations, and who wish to express how their information is used, will benefit from the convenience of Privacy Preferences and Profiles.
De-identification (obfuscation, redaction)	There are many situations where it is not necessary to have data that contains personal information which can identify individuals, e.g. when performing statistical or trend analysis. Obfuscation is a process that removes personal information from data sets.	Most likely to be called on by community operators, obfuscation will safeguard privacy and demonstrate to community members that the community operator takes privacy seriously. It may also be a legal requirement and minimises the risk to personal privacy if data is lost. It also reduces the security necessary to protect backed up data.
Anonymisation	Typically applies to identity, and involves the de-identification of individuals, i.e., the removal of the possibility to identify a particular individual within a given set of individuals.	Members may wish to request services without providing their identity.
Data minimisation	The principle of not revealing or collecting personal information unless it is absolutely necessary to do so for a specified purpose.	The PICOS architectures should be designed with data minimisation as its primary method for providing privacy and protecting identities.
Mix networks	A method of ensuring the anonymity of a sender of a message.	A community (or more likely multiple interacting communities) may offer its members the facility to community anonymously.

Blind (electronic) signatures	A cryptographic process by which the signature applied to a message can be verified by revealing the content of the message.	Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties.
Digital Rights Management (DRM)	Similar to Privacy Rights Management, but the technology is more established. DRM applies robust control in favour of one party (usually the originator/owner).	See Privacy Rights Management. May also be applied to shared media, e.g. personal video.
Sticky policies	A method of attaching, to data, some metadata in which is encoded a set of policies and other information, which stipulates the constraints and conditions within which use of the data is limited. By virtue of being so attached, to some degree of fastness, the metadata travels and is stored with the data, thus aiding or requiring subsequent processing of the data to conform to the policies.	Potentially as a method of implementing Controlled sharing, DRM or PRM.
Pseudonymisation	Sometimes described as conditional anonymisation, meaning that anonymity is dependent on an external condition, which usually implies that a third party who is trusted to protect the identity behind the anonymous identity can breach that trust.	After data minimisation, pseudonymity, in the form of pseudonymous credentials, is arguably the most useful mechanism available to protect identities.
	Trust enhancing technologies	
Reputation management	Reputation is the basis of trust in many communities. Usually formed as a subjective assessment of another party, but can also be based on objective measures.	It is likely that some form of reputation management system will be available across the community, for example to help members evaluate each other prior to sharing information.
	IdM enhancing technologies	

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Identity and Identity Managers	Identity and identity management will be required at various points in any community in order to authenticate those accessing the community services and confirm levels of authorisation. (Other technologies to consider under identity management include unique identity, biometrics and token-based identity.)	It is difficult to imagine that any community can survive without needing to know the identity of those who participate, even if the means of identification does not always reveal the full and absolute identity of the members.
	Security enhancing technologies	
Encryption	The application of cryptography to provide message confidentiality.	Communications, e.g., between members or between members and services, will need to be protected from eavesdroppers. Stored data will also need to be protected against loss of the storage media and breaches of the security surrounding these.
Segmentation/Compartmentalisation/Separation of data and duties	Communities are typically sub-divided according to role, e.g. administrator, member, special interest group. Separation is a common security technique used to restrict access to sensitive resources.	All communities will most likely consist of several compartmentalised areas, defined by function, information and role of those members with access, depending on the role of the community.
Secure Archive (storage)	Communities will need to archive information, for safety and operational needs. The information will need to be at least as well protected as the original data was when resident within the community.	All communities need backups.
File and data management (esp. secure deletion)	For operational purposes, data will need to be moved, copied, modified and destroyed. This must occur in a secure, controlled way so that the data contained in the files is protected.	Administrators will require file and data management facilities in order to operate in the community efficiently, and deal with anomalies that may arise.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Secure Communication	Communication security covers all aspects of the exchange of information between two or more parties, and ensures that no information is unintentionally made available to an 'external' party.	Communications between members, whether voice or instant messaging, will need to be protected (content and addressing information) to preserve privacy.
Trusted computing	The application of mechanisms to assure the integrity of data processing, communication and storage devices, i.e., to detect if unauthorised or unverified modifications to their programmed functionality have been made.	To protect devices, particularly client devices, from stealthy attacks.

Table 1: Privacy/Trust/IdM technologies.

3.1.1.3 Categorisation of technologies for communities

It is difficult to fully understanding the way in which existing communities manage privacy/trust and IdM on behalf of their members, because limited information is publicly available. It is mostly through personal use of a community that we can appreciate the services on offer that specifically handle security for members and for the community operator.

The set of common features that are visible cover:

- Privacy preferences: Mainly opt-out, but increasingly opt-in.
- Identity: UserID and password.
- Privacy management: Basic notification of access and sharing.

Perhaps a better impression of how well privacy/trust/IdM is managed by communities can be ascertained from the reported problems. While the problems do not relate to all communities, and in fact may not represent an endemic problem, they do show where potential weaknesses lie. It is these weaknesses that we are attempting to minimise in the PICOS solution that we will build, derived from this analysis and the requirements gathering exercise that runs in parallel. This approach to categorisation is a much better fit to the 'system' design philosophy (as opposed to add-on component design) that we are adopting in PICOS.

Identified weaknesses (threats) include:

- Unappreciated risk to privacy.
- Default open security options.
- Weak identification/authorisation/not 'hacker resistant'.
- Difficult to comprehend, non-transparent privacy policies.

- Inability of community websites to adequately secure data.
- Unpredicted use of personal information, e.g. by employers.
- Attacks: phishing, spear phishing, pharming, vishing.[3]

  (See http://www.privcom.gc.ca/id/phishing_e.asp for example definitions.)
- Susceptibility to social engineering attacks.
- Enhanced features that unwittingly compromise privacy.
- Balancing advertising and privacy.
- Accidental disclosure.
- Legislation at odds with personal privacy expectations.
- Users disclosing 'too much'.
- Third party access to a community (unknown functionality and viruses).

3.1.1.4 Mechanism/Service matrix

Table 2 below shows the Privacy/Trust/IdM functionality/solutions matrix.

Technology solution	Privacy functionality	IdM functionality	Trust functionality
Privacy Rights Management	✓		✓
Controlled sharing	✓		✓
Cookie management	✓	✓	✓
Personal profile and preference management	✓		✓
De-identification (obfuscation, redaction)	✓	✓	✓
Anonymisation	✓	✓	✓
Data minimisation	✓		✓
Mix networks	✓	✓	✓
Blind (electronic) signatures	✓	✓	✓
Digital Rights Management	✓		✓
Sticky policies	✓		✓
Pseudonymisation	✓	✓	✓
Reputation management			✓
Identity and identity managers	✓	✓	
Encryption	✓	✓	✓
Segmentation/Compartmentalisation/Separation of data and duties	✓		✓
Secure archive (storage)	✓	✓	✓
File management (esp. secure deletion)			✓

[3] Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Secure Communication	✓	✓	✓
Trusted Computing	✓	✓	✓

Table 2: Privacy/Trust/IdM functionality/solutions.

3.1.2 Reputation in online communities

Deciding whom you trust in an online community is a difficult task. It is easier when the online community is built upon an existing real community, like the angler community, where the interactions between members are both physical and virtual.

Managing trust is a real problem in the Internet world, which means that trust is becoming a hot topic and is the focus of several research initiatives that are going in this direction. Annex I provides a list of some of these initiatives.

One way of establishing trust is to build upon the reputation of users. Trusting one user in the community may require knowing many things about him or her. The problem is that this information might not always be available, maybe because it does not exist, or because users do not want to make it public to the community. The latter is consistent with the case of PICOS, which promotes a platform that will be privacy friendly. PICOS users may want to hide personal details to the community or show them only to people they trust. If we follow this approach, this private information that really describes the user will never be available to distrusted users. However, it would also restrict the possible creation of new trust relationships. If we are to look for a neutral parameter that might help us deciding whether to trust or not trust a given user in the community, we may find out that reputation is a good candidate.

The concept of reputation is defined as "what is generally said or believed about a person's or thing's character or standing" by the *Concise Oxford Dictionary*. This definition corresponds well to the view of social network researchers (Wasserman, 1994). The concept of reputation is closely linked to that of trustworthiness (Josang et al., 2007). As commented in this work, the difference between trust and reputation can be easily understood by looking at these two statements:

1. "I trust you because of your good reputation".
2. "I trust you despite your bad reputation".

These two sentences illustrate how subjective the concept of trust is, compared to the concept of reputation. Trust is based on various factors or evidence apart from reputation, although in absence of any other previous experience, reputation is a useful mechanism to establish trust relationships.

In online communities, we have to solve two problems. First, we have to be sure that members are who they claim to be (authentication) and then we have to be sure that we can trust them. Using user reputation to build trust relationships can be a clever approach, although limited by the accuracy of the reputation system.

There are several reputation systems running on actual applications. At present, a total of 36 are listed on the Reputations Research Network site, (http://databases.si.umich.edu/reputations/index.html). Some are used to help people decide if a seller is reliable; others to judge if a book is worth reading; and others just to order news items according to their relevance. Although they use different measures of reputation, all of them have the same objective: to improve user experience.

According to (Resnick et al., 2000), a working reputation system must, at minimum, have the following three properties:

1. **Entities must be long lived**, so that with every interaction there is always an expectation of future interactions.
2. **Feedback about current interactions is captured and distributed**. Such information must be visible in the future.
3. **Past feedback guides buyer decisions**. People must pay attention to reputations.

The third principle is focused on an e-commerce scenario, although changing *buyer* to *member of the community* makes this perfectly clear. None of these properties is exempt from difficulties. One of the main risks is the use of pseudonyms, which allows one single person to have multiple online identities, which makes it difficult to compute a unique reputation value for this person.

The first principle may interfere with the PICOS philosophy, as we want to cover the widest range of communities we can. If we strictly follow this principle, ad-hoc communities or communities that only exist for a short period of time might be excluded. We have to note that under the essence of this principle is the idea that users behaving badly have to expect their exclusion or isolation from the community. This way, users will tend to behave honestly in order to be part of the community. The shorter the life of users is, the smaller the fear of being excluded will be.

A reputation system is more effective when there some incentives for maintaining a good reputation level, and when it is difficult to get rid of bad ratings (e.g., by creating a new account). There are some systems, like Epinions.com which give a reward to members who try to maintain a good reputation. In others, e.g. Ebay.com, the reputation itself is the reward as it influences your future sales. In other communities that are not profit oriented, e.g. Advogato.com, there is no reward and it is just the ego of the members that leads him or her to improve his or her reputation.

Therefore, the desire to improve our reputation can be for:

- **Profit.** A higher reputation will directly provide more profit to the user. Ebay.com model.
- **Reward.** A higher reputation will provide a reward to the user. Epinions.com model.
- **Ego.** A higher reputation does not give any profit to the user, just a higher status in the community and maybe some privileges not related with profit. Advogato.com model.

This distinction is a little bit fuzzy, but can help us to understand the mechanisms that build trust upon reputation. The reward model can be seen as an intermediate model between the ego and profit models, and can be applied to any kind of community.

Within PICOS, the reward model fits very well as it can be founded by advertising companies. In the angler and online gaming communities, marketing activities can support the reward system, whereas in the taxi driver one, there is not even a need for a reward.

One of the main difficulties when defining a reputation system is the mechanism to aggregate reputation values from different interactions. For example, eBay computes the reputation of a seller by just subtracting the negative feedbacks from the positive ones. Other sites like Amazon use the average. In Resnick's opinion, to which we agree, these simple numerical ratings fail to convey

important subtleties of online interactions. Other factors like the value of the interaction and the reputation of the user providing the feedback should be also taken into account.

One way to classify reputation systems could be according to the aims that lead users to improve their reputation (as commented before). Another way could be according to the way reputation is computed, differentiating between Centralised reputation systems, in which reputation is stored, updated and made available to other users in a central server; and Distributed reputation systems, in which reputation is stored and distributed, and is usually computed, on demand by collecting reputation values from the distributed system. Another important factor for a reputation system is time. Timeless reputation systems will consider all reputation values as if they were gathered in the same instant, whereas a time aware reputation system will use the time instant when the reputation value was gathered to adjust it and modify the final reputation value.

As we have commented before, there are many factor that define a reputation system. Among these factors are also the ones identified by Jeff Ubois (Ubois, 2003):

- **Participants.** Who's rating whom? Is the system customer-about-buyer, or peer-to-peer? Do the users that provide feedback have reputations themselves? Are they known or anonymous?
- **Incentives.** Are the participants explicitly taking part in a reputation system, or are they performing "normal" tasks such as writing a newspaper article or offering advice in a Usenet group?
- **Criteria.** What issues matter to the users? Do they care about prompt shipping or about product quality? That is, what factors go into calculating a reputation: numeric feedback from counterparts to a transaction, observed behaviour, seals and credentials, press coverage, etc.?
- **Access and recourse.** Who gets to see the data, and who gets to change it? Who gets to know about that change? Who knows about who has rated whom? Can someone respond to a reputation he is assigned? Can an opinion be corroborated?
- **Presentation and tools.** Offline, reputation is rich and nuanced: people can use all five senses to determine reputation. Online users can only see and interact with data points. With what tools can users interact with and filter data? To what extent is the data abstracted or aggregated?

3.1.2.1 Review of three existing reputation systems

eBay's feedback forum

eBay is a popular online auction site where anyone can sell practically anything at any time. In eBay, the feedback represents a person's permanent reputation as a buyer or seller on eBay. It is made up of comments and ratings left by other eBay members you bought from and sold to. There are three types of feedback ratings: positive, neutral and negative. The sum of these feedback ratings are shown as a number in parentheses next to your User ID.

This feedback system has been updated recently with the intention of increasing buyer and seller accountability. eBay has remove the ability to produce negative ratings on buyers. Instead, sellers may contact the eBay's Seller Reporting Hub to solve disputes. Also neutral ratings will not be taken into account so suspended buyers can no longer negatively impact a seller's record.

Epinions

Epinions is a place where members can write reviews, as well as other kinds of opinions. To post a review, members must rate the product or service on a rating scale from 1 to 5 stars, one star being the worst rating, five stars being the best. A rating scale is a set of categories designed to elicit information about a quantitative attribute in social science. For several years now, all opinions also come with brief Pro and Con sections, and a "The Bottom Line".

Epinions offers an Income Share, which ostensibly rewards reviewers for how much help they have given users in deciding to purchase products. All members can rate opinions by others as Off-Topic (OT), Not Helpful (NH), Somewhat Helpful (SH), Helpful (H), and Very Helpful (VH). Opinions shorter than 200 words are called Express Opinions and rated "Show" (S) or "Don't Show" (NS).

Members can also decide to "trust" or "block" (formerly known as "distrust") each other. All the trust and block relationships interact and form a hierarchy known as the Web of Trust. This Web of Trust (WOT) combines with ratings to determine in what order opinions are shown. The order members see depends on their own ratings and their own trust and block choices. The order a visitor sees is determined by a default list of members a visitor supposedly trusts. The Web of Trust formula is secret.

Advogato

Advogato is an online community site dedicated to free software development, created by Raph Levien. It describes itself as "the free software developer's advocate". Advogato was an early pioneer of "online diaries", which later became known as blogs, and one of the earliest social networking websites. Advogato combined the most recent entries from each user's diary together into a single continuous feed called the recentlog.

Many high profile members of the free software and open source software movements are or have been users of the site, including Richard M. Stallman, Eric Raymond, Alan Cox, Bruce Perens, Jamie Zawinski and others.

The idea behind Advogato was to put into practice Levien's ideas about attack resistant trust metrics, which involves users certifying each other in a kind of peer review process, and using this information to avoid the abuses that plague open community sites. Levien observed that his notion of an attack resistant trust metric was fundamentally very similar to the PageRank algorithm used by Google to rate article interest. In the case of Advogato, the trust metric is designed to include all individuals who could reasonably be considered members of the Free Software and Open Source communities, while excluding others.

3.1.3 Privacy technologies and PETs

This section discusses techniques for protecting privacy in databases and the protection of user agents in potentially non-trusted environments. Various techniques for sanitizing queries in statistical databases to protect user privacy are described and discussed, together with implications for the

PICOS scenarios. The protection of information and ensuring the execution integrity of an application executed in a non-trusted environment possibly under attacker control is a notoriously difficult task. The situation is better when secure hardware is available, yet problems related to data presentation to users, and secure input, remain. From the PICOS perspective, additional protection for applications might be welcome both on the client and server sides. The server side may benefit from increased security against inside attackers, and more trust in technology may be obtained if processed data are unavailable to unauthorized yet powerful users like system administrators.

3.1.3.1 Techniques for providing privacy in databases

The need for techniques for preserving privacy in public databases (databases that are publicly available) or statistical databases is obvious, as these may contain very sensitive information about individuals. Anyone who has access to these databases and has adequate rights for performing queries on data can learn a lot. Even more dangerous are aggregation queries that can combine lots of data together and infer new information that is not explicitly stored in the database. This can be done for both statistical purposes, and for the purpose of getting information about a particular user(s). Even if the data is anonymized, it is possible to indirectly identify entities by combining some "innocuously" looking attributes.

Statistical databases allow users to retrieve only overall results about a set of entities in the database. Any attempt to retrieve information about any particular entity must be strictly forbidden. As stated above, one can easily conclude that the most important issue is preserving privacy while allowing data to be used for statistical investigations. But these requirements – privacy for the responders and usefulness of the data – are in mutual conflict. Perfect privacy can be achieved by publishing nothing, but this has no utility; perfect utility can be obtained by publishing data exactly as received from responders, but this offers no privacy. Data perturbation should permit data analysts (statisticians) to work with the data while preserving privacy of individuals. This section surveys current techniques for both dealing with privacy and data perturbation in statistical and publicly available databases.

An inference attack on statistical database involves a set of database queries that (if properly combined) can reveal new information (which is not directly accessible) about an entity or a set of entities. The classical situation is when the attacker knows some information about the entity and, using this information, tries to learn something new. Suppose, for example, that the attacker forms a query which gives only one record as a result. Using this query, the attacker can identify one entity. Suppose also that the attacker is not allowed to query some other attributes directly, but if the database is not well secured, he or she can still observe how many results the modified query produces. If the new attribute (e.g. diagnosis=HIV), together with the remaining part of the query, produces one result, the attacker has thus inferred new information – this is the case of positively compromised database. If the number of results is zero, then the database is said to be partially compromised.

Methods that are used for security and privacy protection can be classified into four general groups (Adam and Worthmann, 1989): conceptual, query restriction, data perturbation, and output-perturbation. Two models are based on the conceptual approach – the conceptual model and the lattice model. The conceptual model allows one to identify security-related problems on a conceptual and data layer. The lattice model describes statistical database information in a tabular form at different levels of aggregation. The aim of this approach is to allow for a better understanding of possible aggregation, which may reveal some new or redundant information. Methods that are based on the query restriction approach provide protection through one of the following measures: restricting the

query set size, controlling the overlap between successive queries by keeping an audit trail of all answered queries for each user, or partitioning the statistical databases.

- Conceptual – description and identification of security-related problems
  - Conceptual model
  - Lattice model
- Query restriction – protect the statistical databases from retrieving records about individual entities
  - Query-set-size restriction
  - Query-set-overlap control
  - Auditing
  - Partitioning
- Data perturbation – modification of the original data
  - Probability distribution
  - Fixed-data perturbation
- Output perturbation – modification of the query output
  - Random-sample noise
  - Rounding

Query restriction approach – This method allows for the retrieval of statistical data only if the query size (number of entities involved in the query |C| processing) satisfies the condition $K \leq| C |\leq L - K$, where L is the size of the database (number of entities) and K is a parameter that is set by a database administrator (DBA). This parameter K should satisfy the condition $0 \leq K \leq L/2$. It was shown (Denning and Denning, 1979) that, by using a tool called tracker, it is possible to compromise a database even if K is close to $L/2$. Notice that K cannot exceed L because, otherwise, no statistics would be released.

Query-Set-Overlap Control – Query overlapping is a situation when different queries have many common entities. (Dobkin, Jones and Lipton, 1979) noticed that many compromises involve query sets that have a large number of common entities. This type of control has several disadvantages – cooperation of more users cannot be avoided; there is a need for an up-to-date profile for each user, and database usefulness may be jeopardized by these limitations. A mechanism that performs comparisons between user queries works in O(L) complexity, where L is the size of the statistical database.

Auditing – This is a query restriction method in which a log of queries is saved, and every query is checked for possible data compromise. The given query is allowed or suppressed according to the check result (Chin and Ozsoyoglu, 1982). One problem of this approach is efficiency – the problem of deciding whether a sequence of queries violates privacy was shown to be computationally hard. (Kleinberg et al., 2000) showed that, given a database d and a set of queries, deciding whether an exact answer to these queries leads to the full determination of the value of at least one protected database entry is an NP-hard problem.

Partitioning – The main idea of this method is to group individual entities into mutually exclusive subsets that are called atomic populations (Adam and Worthmann, 1989). These are then available for queries of database users. Authors of the method believe that many ways of compromising databases (like if an attacker has sufficient additional information, such as when entities are inserted / updated / deleted from the database) can be avoided through its use, since atomic population does not contain any information about particular entities. A drawback of this approach, as it was shown in (Schlorer, 1983), however, is that many real databases contain tables with only one entity. If these entities aggregate to a high volume of information, a data loss may occur.

Data perturbation – Data perturbation techniques are divided into two main categories – probability distribution and fixed-data perturbation. The probability distribution approach considers the statistical database as a representative sample of a given population with some given probability distributions. The original database is then replaced by a new sample that has the same probability distributions as the original database. Using this method with dynamic databases is very difficult due to the computational overhead, because some transformation needs to be made in the transformed sample to every data modification in the original database. This, together with possible high inaccuracy (as mentioned below), makes this method not very widely used in statistical databases.

Fixed-data perturbation approach – This approach, on the other hand, changes the values of the attributes, which are to be used for computing statistics, once and for all. This approach often requires another (transformed) database to be created only for statistical purposes. Data is perturbed in a way that some random value is added to the real value. This can suffer from high inaccuracies so, instead of adding a random value, this value is multiplied with the original one. Attributes that have binary representation are perturbed with probabilities (fixed-data perturbation for categorical attributes) of whether the value is true or false. Probability value p that is defined by a database administrator is multiplied by the number of entities that satisfy a particular query, but without the binary attribute. The advantage of the fixed-data perturbation approach is that transformed data can be updated dynamically along with changes to the original data. (Kargupta et al., 2003) discuss the privacy of random-data perturbation techniques and showed that under certain circumstances these techniques can provide a very little data privacy. They also pointed out some possible directions for new privacy-preserving data mining techniques, like exploiting multiplicative and coloured noise.

There is always a problem with the accuracy of results with data perturbation techniques. (Matloff, 1986) showed that, under certain circumstances, 50% bias can occur. (Wilson and Rosen, 2003) provides a study on both the impact of perturbation techniques for protecting databases and the bias problem.

Output perturbation approach – The main difference between this approach and the previous one is that the bias problem here is less severe. This is because the results are based on the original values (not perturbed values), and only the result is perturbed. The first approach is called random-sample noise and was proposed by (Denning, 1980). The idea is very simple. A set of entities that satisfy a requested query is influenced by a probability parameter P that is set by DBA. An entity in the set will be considered in the result with a probability P. The required statistics are computed based on the sample query set. The statistics computed from the sample query set have to be divided by P in order to provide a corresponding unbiased estimator. This method, though, still suffers from the resulting inconsistency. With the varying-data perturbation approach, a random perturbation is added to the query answer, with increasing variance if the query is repeated.

Rounding technique takes the result of the query and rounds it up or down to the nearest multiple of a certain base b. There are three types of rounding techniques – systematic rounding, random rounding and controlled rounding. Systematic and random rounding technique adds some offset to values in the database. Controlled rounding technique affects more values in the row in such a way that the sum of the row equals to the sum of non-rounded values. The problem with rounding is that it is possible to determine the true value by averaging the responses to the same query. In general, rounding techniques are not considered to be effective security-tools, but they can helpful if they are combined with some other approaches.

From the methods that were presented above, the random-sample queries method, the varying-data perturbation method, the fixed-data-perturbation method and the fixed-data-perturbation method for categorical attributes are the most promising security-control methods for online dynamic statistical databases. A very good comparison of all methods mentioned here can be found in (Adam and Worthmann, 1989).

Techniques used in statistical databases to preserve the privacy of individual users can be effectively used to secure information, while still allowing the use of the databases to retrieve some statistical information. In general, databases are used in all three scenarios in PICOS, and these databases will probably contain sensitive material. Therefore, it is clear that special care has to be taken to protect these databases from information leakage while, at the same time, allowing users to use them in order to retrieve desired information. In the following paragraphs, we discuss the relation of statistical databases and related protection mechanisms to all three scenarios in PICOS project.

Let’s discuss the online game community first. It is quite common that almost every online game provides some set of statistics of best players, best attackers/defenders, the level of trust and reliability of players and many other types of information. If there is an access to such a statistical database, it is reasonable to apply some techniques to restrict the type of queries allowed. If the database is “unsecured”, anyone who has access would be able to discover detailed information about individual players. It is obvious that in the case of online gaming, this type of information can be considered as private information. This type of information can be taken into consideration when planning battles, deciding who will be accepted into a community of players, or which players are not reliable, online/offline status, etc. If this type of database is about to be made public, only statistical queries should be allowed. In such a case, no one is able to retrieve any information about an individual player and us it for own profit. But even with restrictions, the database should be usable for retrieving various statistics that provide valuable information.

The case of taxi drivers in relation to statistical databases can be considered as an issue of securing sensitive information about individual journeys and drivers, but still allowing the retrieval of overall

statistical data that can be used for, e.g., planning or reputation calculation. An example of a "statistical query" is a query to discover which days the drivers have to drive more, and to try to find the reasons for this. Statistical information can, e.g., help to organize taxi placement in a more efficient way. Another issue would be the use of personal devices used for passenger/taxi location. These devices may contain very sensitive information about passengers, and if this data is stored in the database it is highly desirable to protect it against unauthorized retrieval. Taxi drivers establish their reputation. The reputation score is based on their past performance. This performance history has to be stored and periodically updated as drivers operate. The only value that the system provides is the reputation score. But the score is likely to rely on many attributes. By application of techniques described above, we can guarantee that those with the access will be able to learn only some statistical values or the reputation score. Requests to obtain an individual driver's details will be strictly prohibited.

In the case of the angling community, the protected assets are the databases containing information about anglers and, e.g., their catch records, photos, interesting places, etc. The use of techniques in statistical databases strongly depends on the kind of data in the system, and the possibility of linking single pieces of data to create a larger view. The angling communities are quite big and there are many sub-communities that actively cooperate, e.g., in hunting trip preparations. These sub-communities share a lot of useful information in the system, but as they do not to have trust in other communities, they do not intend to share their knowledge with others, and are willing to provide only basic information. On the other hand, members of the same sub-community should have access to all information that is being shared. Anglers also build their individual trust which is then used by others to determine, e.g., the reliability of provided information. The factors used to determine the level of trust should also be a subject of restriction if the trust level is the only information provided by the system.

3.1.3.2 k-Anonymity

A model for anonymising personal records in a database has been proposed by Samarati and Sweeney in (Samarati and Sweeney 1998, L. Sweeney, 2002). While anonymity at the communication layer needs to be protected from traffic analysis attacks, anonymized records may be vulnerable to re-identification. Re-identification is the process of relating unique and specific entities to seemingly anonymous data (Malin, 2002), and as such, is an attack on the privacy of a data collection.

When a data holder wants to release anonymized personal records (e.g., for research purposes), it is not enough to remove obvious identifiers such as name, address, or national ID number. Often, some subsets of the data fields constitute a quasi-identifier. For example, ZIP code together with the gender and the birth date may be enough to re-identify a substantial number of anonymized data subjects.

A quasi-identifier is defined as: "Let $RT(A_1, ..., A_n)$ be a table and QI_{RT} be the quasi-identifier associated with it. RT is said to satisfy k-anonymity if and only if each sequence of values in $RT[QI_{RT}]$ appears with at least k occurrences in $RT[QI_{RT}]$".

The k-anonymity model assumes that there is some publicly available database (e.g., the census or voter registration list) that contains certain attributes for each of the data subjects included in it. When a second data set is released, it is often the case that, even if identifiers have been removed, quasi-identifiers can be found, such that re-identification (i.e., linking to the publicly available database in order to find the name, address, etc.) is possible.

k-anonymity is defined as follows (Samarati and Sweeney 1998, Sweeney, 2002): "Let $RT(A_1, \ldots, A_n)$ be a table and QI_{RT} be the quasi-identifier associated with it. RT is said to satisfy k-anonymity if and only if each sequence of values in $RT[QI_{RT}]$ appears with at least k occurrences in $RT[QI_{RT}]$".

In other words, a set of records is k-anonymous if there are at least k records in the anonymity set for each possible quasi-identifier. The techniques proposed to make a set of data k-anonymous are based on suppression and generalization of data fields.

In all three scenarios, special care has to be taken concerning the sets of quasi-identifiers in the database that can be used to significantly decrease the number of final results, and therefore allow for positive re-identification of individual entities that should remain anonymous. In the case of gaming communities, either case can be desired – to allow for re-identification of a single user playing different online games, or to disallow this from happening, because this information can be abused by other players.

In the case of taxi drivers or anglers, the use of k-anonymity is to protect individual entities from being re-identified. Reasons for this are quite obvious; we do not want to provide this kind of private information by default.

3.1.3.3 Mixes

The first proposal for mixes was published by David Chaum in (Chaum, 1981). The system was proposed for sending emails anonymously.

The whole mixing process is very simple – a mix receives some messages from users that want to send messages anonymously. After that, the mix destroys all identifying information from each message and sends all messages onward. One of the basic problems with anonymous communication is the possibility to differentiate one entity (e.g. an email) from others – this is an issue of traffic analysis. Using traffic analysis, an attacker tries to differentiate messages passively just by observing the traffic on the communication channel.

Incoming messages are encrypted with the public key of the mix – to secure the content of the message. The mix, having the corresponding private key, is able to decrypt the message, and then processes the messages and sends them either to the next mix or to the final recipients. Processed messages are typically send onward once some "threshold" condition is fulfilled. This condition directly influences the level of anonymity provided, and there are several types of mixes working with different sending conditions (Wright, 2004) (threshold mix, pool mix, continuous mix, time mix).

Figure 3: Mix node scheme.

There are quite significant delays in message delivery depending on the way a mix processes the message. Processing a message through a set of mixes may even last for some hours. But the primary usage of mixes is in the area of applications that can tolerate some latency (like WWW browsing,

FTP, SSH, etc.) and, therefore, these delays can be accepted in exchange of having the ability to communicate anonymously.

The primary goal of mix technology is to provide an environment for anonymous email communication. Communicating parties can hide their real identity against others that use the same network. If any of the communicating partners wants to reveal the real identity, it should be done via an anonymous channel so that he or she is only the recipient who knows the real identity of a sender. This situation should be quite common in online gaming communities where even the fact that someone sends a message could be valuable information as it reveals his/her online presence as well as relations. Using this technique for, e.g., battle planning will provide a secured and anonymous communication environment, and other players will have little chance of discovering who communicated with whom.

In the case of anglers, anonymous communication can be used for the first contact with an "unknown" angler. There is no initial trust between anglers, so it is not desirable to reveal the real identity upon first contact. And again, if either communication partner wants to reveal his or her real identity, it can be done via an anonymous channel that prevents others from observing this information.

3.1.3.4 Anonymous credentials

A credential system is, in general, a system where users obtain credentials from organizations and then demonstrates their possession. The whole system is anonymous if multiple transactions performed by one user cannot be linked together. The whole system consists of users and organizations. Users have their pseudonyms, which are the only identifying information. Pseudonyms cannot be linked together.

Once an organization issues credentials to a pseudonym, the corresponding user then proves to another organization its possession. The system must guarantee that the only information received by the second organization is that the pseudonym owns the credentials. There may be two basic types of credentials – long-term credentials, which the user can show its possession multiple times; and one-time credentials, which the user demonstrates its possession only once.

Basic properties of anonymous credentials systems are:

- It is impossible to forge a credential even if organizations cooperate.
- Users cannot cooperate to get special credentials that a user alone would not have gotten.
- The system should provide privacy – an organization is not able to find anything specific about a user.

In, e.g., the online gaming community, this kind of technology can be used by players to prove they participated in some online game that allows them to have some benefits in another game. By demonstrating the possession of the credentials in an anonymous way, it would not be possible for online game providers to link different pseudonyms of one user together.

3.1.3.5 Trust

Users are often required to provide some information about them, and with the number of online services they use it is often hard to recall where and to whom they provide such information. Once a user decides to provide some personal information about him or her, he or she is also interested in whether the service is reliable, so that he or she can trust that the data will not be misused. The establishment of trust is essential in any system for anonymous communication. Since we generally do

not know the real identity of a person, but only his or her pseudonym, we need some "extra" information about the user to be able to decide whether to start, e.g., to cooperate in an online game.

A good starting point here would be the PRIME architecture (Andersson et al., 2005). The architecture is, at the highest level, spilt into user and server sides. For users, it offers a central repository for personal data, credentials, and a software layer that protects this data. Users are able to centrally manage their data, and control and track where the data is provided. The service side offers services to interact with users, to provide them with the information that the service side IT environment is trustworthy, and to protect user data. Both the users and services have to respect policies and requirements in the architecture. Policies and requirements are the key aspect for data disclosure and processing.

The PRIME architecture can be applied in all three scenarios for reliable and trustworthy personal data handling. Users will be able to control who has access to their personal data, and to decide whether these services are trustworthy.

3.1.3.6 Protection of user agents in potentially non-trusted environment

The protection of the information and execution integrity of an application executed in a non-trusted environment possibly under attacker control is a notoriously difficult task. The situation is better when secure hardware is available, yet problems related to data presentation to users and secure input remain.

From the PICOS perspective, additional protection for applications might be welcome both on the client and server sides. A client application may contain a user's sensitive data, which should be well protected against compromise, especially when stored on a mobile device that is easy to be lost. Usage scenarios described earlier require, in some cases, some functionality to be available offline without an online connection to the server. Such functionality should be able to manipulate locally stored and potentially sensitive data. Simple encryption of the data can be used to protect it, but as the data should be available offline, a decryption key must be stored in the device as well. Access to the device (e.g., after loss, theft or even the running of a malware program parallel to the PICOS client) therefore allows an attacker to access the local key, and then decrypt data. If the PICOS client is protected by techniques described in this section, local key and function manipulating with sensitive data are better protected than by simple encryption with a key. This is because an attacker is not able (for limited period of time) to extract the key or access the data.

The server side may benefit from increased security against inside attackers, and more trust in technology may be earned if processed data are unavailable to unauthorized yet powerful users like system administrators. All techniques described in this section try to achieve the so-called black box security scenario, where the attacker can manipulate with a program only via its input/outputs. Usually, only limited time protection is possible, resulting in time-limited black box security.

Code obfuscation – Code obfuscation methods use semantically equivalent transformations of the source or executable code and data, and decrease the code's readiness. The aim of such transformations is to harden the creation of a mental model (of what the program is doing), to cover data flow, and to prevent meaningful modification of code by an attacker. Different programming languages have different preconditions for obfuscation. Obfuscation is usually divided into execution, data and preventive transformations.

Execution transformations influence the readability of original code by the insertion of dead (code without effect) or irrelevant code (e.g., tautology conditions in branches), the introduction of

redundant operations, code parallelization, or the removal of standard low-level code patterns resulting from typical high-level programming constructions. Data transformations modify access patterns and the processing of data values by changing data coding, splitting and joining variables, restructuralizing data arrays, transforming static structures to dynamically generated, or modifying inherited relations for object oriented programming. Preventive transformations target known techniques of reverse engineering, decompilators and de-obfuscating tools. Knowledge of the implementation of existing tools is used to prevent their correct functioning. Naturally, such preventive transformations provide only short term protection, but, in combination with the previous techniques, increases the cost for an attacker.

The disadvantages of obfuscation transformations might be increasing the size of compiled code, decreasing the execution speed, and significantly increasing the difficulty of the bug-fixing process when an obfuscated program is issued to customer. A more detailed description of obfuscation techniques and metrics for measuring the obfuscation levels can be found in (Collberg et al., 1997, 1998; Chow, 2001; Nickerson et al., 2001). Several free and commercial tools are available for the obfuscation of most programming languages. Note that obfuscation is not assumed to be a provably secure method of code protection, especially given the existence of large numbers of "de-obfuscators", and even proof of the impossibility of obfuscation for general programs (Barak et al., 2001). Typically, a new obfuscation technique provides protection only for a limited period until the relevant de-obfuscator is produced.

Uninformed agent – Mathematically more robust versions of obfuscation, based on problems with provable non-polynomial complexity were developed for specific classes of programs. Software protection based on the principle of the uninformed agent was introduced in (Riordan, Schneier, 1998), and later extended by (Hacini, 2004; Hacini, Cheribi and Boufaïda, 2006). The basic idea is simple. The sensitive information (code and data) of the agent is typically encrypted with a key that can be derived from specific environmental information. Examples might be the IP address of the target computer where the agent should be executed, a specific string found in database, a specific value published by a trusted third party, or anything else reasonable from the agent usage perspective. An agent systematically queries such environmental characteristics and tries to derive the necessary key. Derivation is successful only when an environmental characteristic matches the pre-specified state from which original key was derived. The agent then decrypts the sensitive part and executes it. Without the correct environmental characteristics, the agent is not able to decrypt the sensitive part, and is therefore "uninformed" and immune against any inspection of the sensitive part by an attacker (if a sufficiently strong encryption algorithm is used), even when the derivation algorithm is known. The main problem with key derivation is the attacker's full control over the execution environment, and therefore the possibility of him or her to manipulate environmental characteristics. The space of all values for queried characteristics must be large enough to prevent brute-force enumeration of all possible values.

A simple example can be the insertion of additional information 'A' into a database only when the database entry with value 'secret0473816' already exists. 'A' is encrypted with key K derived as K := hash(M), where M := hash('secret0473816'). The agent process all entries one by one and computes M' := hash(entry_value). When M == M', the target entry then exists in the database and 'A' can be decrypted, otherwise 'A' will never be revealed.

Mobile cryptography – The mobile cryptography concept was introduced by (Sander and Tschudin, 1998), and further extended by (Xu, 2004; McDonald and Yasinsac, 2007). Some classes of functions

(currently rational and polynomial functions) can be transformed into series of alternative operations that compute same outputs for given sets of inputs as original functions. But it is computationally difficult to compute a reverse transformation or extract used sensitive data without knowledge of the random data used for the original transformation. The protection of sensitive code and data is not dependent on the secrecy of the transformation function (a difference from obfuscation), but only on the secrecy of used data. Still, a transformed function can be directly executed on the same platform as original one. Mobile cryptography provides two basic variants that protect either the processed data or code of the used algorithm. Computation with Encrypted Data (CED) is a process where side B executes function F over data X provided by side A, but B does not obtain any knowledge about data X and A does not obtain any knowledge about function F from the computation. Computing with Encrypted Function (CEF) is a process by which side B executes program P over B's own data X, where P is provided by A and realizes function F. Side B does not obtain any substantial knowledge about F.

A CED variant (Abadi and Feigenbaum, 1990) is suitable for scenarios where an agent executed in potential untrusted environment should be able to use external sensitive data without revealing the data's actual value. A CEF variant is suitable in scenarios where the agent should execute a sensitive algorithm we would like to protect against attack. A function executed with CEF can be currently only be a rational or polynomial function (Sander and Tschudin, 1998). Based on this concept, several practical, usable schemes were proposed, notably the special implementation of DES (Chow et al. 2002; Link and Neumann, 2005) and AES (Chow et al. 2002) encryption algorithms that protect the value of the used key. Such an implementation takes only input data and correctly returns encrypted/decrypted data with the built-in key. However, most of these proposals were shown to be insecure (Link and Neumann, 2005; Wyseur et al. 2007), as a trade-off between code-size and security has to be performed.

Mobile cryptography does not require special hardware, but the protected code is usually larger than the original. Indirect knowledge about function F protected by CEF can be still obtained by the manipulation of inputs, or introduction of random modifications into the CEF protected function (so-called fault analysis) and the observation of output changes. Additionally, an attacker can use a CEF protected function as a black-box "machine" without actually obtaining the function F. To mitigate such attacks, a combination with other techniques like obfuscation must be used.

In the context of the PICOS community scenarios, the protection of user agents providing limited time protection can be used to maintain security of short term information for platforms, where usage of secure hardware (e.g., smartcards, TPM) is not possible or too expensive.

3.1.3.7 Cryptographic smartcards and related standards

The previous techniques do not require use of any special hardware, which decreases implementation costs, but also limits either the duration of the protection or classes of protectable programs. Now we will focus on available hardware support.

Smartcards have developed over the last twenty years into quite powerful devices with the ability to store up to hundreds of kilobytes data, and perform on-card cryptographic operations like hash algorithms (typically MD5 and SHA-x family), symmetric cryptography (DES, AES) and, notably, asymmetric cryptography (RSA, ECC, Diffie-Helmann) with private keys up to 2048 bits long with the possibility of on-card key generation (the private key never leaves the card). Such devices can be readily used to perform critical security tasks on behalf of a user agent, or the user him or herself.

Multi-application programmable smartcards with code portability between different hardware platforms (MULTOS, JavaCard, .net) are now becoming more common.

RSA Laboratories PKCS#11 standard (RSA, 2007) (current version is 2.20) is in widespread use, especially for cryptographic devices with a proprietary communication interface. The set of API functions covers all basic cryptographic functions, data storage and token management. Significant support is also available in existing software products (signature and encryption programs, operating system sign-on, Internet browsers, etc.) and PKCS#11 is the most frequently used standard for accessing the cryptographic capabilities of smartcards/tokens.

Sun Microsystems published the Java Card Platform Specification and the Java Card Development Kit, which includes a reference implementation based on the specification. The aim is to provide the basis for cross-platform and cross-vendor applet interoperability. The current version of the JavaCard specification has recently been released 3.0 (Sun, 2008), however current smartcards usually implement only the 2.2.1 or 2.2.2 version. The JavaCard applet is a Java-like application that is uploaded to a smartcard and is executed by the Java Virtual Machine on the smartcard. Due to limited resources and computing power, Java Cards do not support standard features of Java, like dynamic class loading, security manager, threads and synchronization, garbage collection and object cloning, finalization, large primitive data types (float, double, long and char), and most of the standard classes (most of the java.lang, Object and Throwable classes in limited form).

The main security features of Java Card include all the benefits of the Java language, like data encapsulation, safe memory management and packages. Applet isolation based on the Java Card firewall (applets cannot directly communicate with each other), special interface for sharing objects Shareable must be implemented to allow cross applets interaction. Atomic operations can be enforced via the transaction mode. Data can be declared as transient data, which guarantees that sensitive session data is wiped out when the smartcard is removed from the reader. A rich cryptography API for encryption, digital signatures and message digests is also available.

The MULTOS operating system (http://www.multos.com/) is common in bank issued cards, mainly due to its long existing certification on the Common Criteria EAL 4+ security level (other environments like JavaCard or .net have now achieved the same audit rating). MULTOS applications can be written in an assembler, or compiled from a high level language, typically C or Java.

Publicly available Open Platform specifications (http://www.globalplatform.org/) cover issues of smartcard life cycles, the installation of applets, remote card management, and secure communication channels between smartcards and user applications. Open Platform-enabled smartcards can be remotely administered, and multiple application vendors can independently manage their applications separately from the card issuer.

The lower level communication between PC and smartcard is realized via a PC/SC interface (originally developed for MS Windows, and then ported to other systems) using APDU commands (ISO7816-4). Communication on the physical level between the card reader and the smartcard is defined in ISO 7816-3 (protocols T=0 and T=1).

In the context of the PICOS community scenarios, smartcards can be used to maintain user authentication credentials, securely store sensitive information, and guarantee integrity and secrecy of a communication even when the host computer is compromised, to some extent, by malware. Smartcards can also hold information that is attributed to the user but should not be modifiable by the user itself (e.g., reputation score). A community platform server can then securely and remotely

manage stored information (centralized approach), or cards can communicate directly (with the help of a mediating computer without access to the exchanged communications) and update stored information (decentralized approach). New smartcards can be issued to end users, or already deployed multi-application cards (e.g., loyalty cards) can be used.

3.1.3.8 Hardware security modules

Hardware security modules (HSMs) provide secure key storage and efficient cryptographic processing to facilitate secure electronic transactions. The computation power is significantly higher than that for smartcards. The key feature is that even an operator of the machine where HSM is installed is not able to extract or manipulate stored keys and other sensitive data. A typical example might be an online PIN verification service of a bank, where even a trusted insider is not able to obtain the combination of a user account number and the assigned PIN. The basic architecture of HSMs comes from classical von Neumann architecture, which uses the same building blocks. Moreover, the mechanisms of physical protection, special purpose (co)processors, generators of true random numbers (TRNG), and non-volatile RAM (NVRAM) were added. Physical protection is ensured, for example, by steel shielding surrounding the device, potting in epoxy resin, wired mesh (or alternatively, modern conductive membranes), or various kinds of sensors (e.g., light, power glitch, pressure, thermal, and X-Ray sensors). Detected tampering will immediately result in the erasing of the stored sensitive data. The special-purpose (co)processors are typically used to accelerate symmetric ciphers (mostly DES, 3DES), hash functions (mostly MD5, SHA-1), or modular arithmetic (multiplication, exponentiation) that are used in many asymmetric cryptosystems. Hardware TRNGs are a critical part of all HSMs, necessary for the generation of high-quality (i.e., perfectly random and unpredictable) cryptographic keys, initializing vectors, padding values, and algorithmic counter-measurements against side channel attacks. A battery powered NVRAM then serves as a secure storage location for highly sensitive data (e.g. master keys) – while other keys can be securely stored outside the HSM, protected by master key(s). HSMs are programmable; therefore, part of customized code can be run in a secure environment. HSMs, however, are rather expensive with price around $10 000.

In the context of the PICOS community scenarios, HSM might be used for the manipulation of highly sensitive information – typically, keys on the server side of community platform – to limit the impact of a malicious insider. The limited memory capacity of HSMs does not allow the storage of large amounts of data like a whole database, but database entries can still be encrypted by a key stored only in a HSM. When data manipulation is required, on-demand decryption or processing inside HSM is performed, which involves input and output data outside being in encrypted form only.

3.1.3.9 Trusted platform modules (TPMs)

TPM is the name both for the specification and actual hardware designed to provide a trusted anchor for customer electronics like PCs, mobile phones or PDAs, developed by large group of leading firms in the IT industry under the Trusted Computing Group consortium (https://www.trustedcomputinggroup.org/). In principle, TPM itself is just a variant of smartcards (so far), but built into the device (usually on the motherboard, and planned to be part of the CPU or Southbridge chips) with the ability to securely store hash values (Platforms Configuration Registers – PCR), and perform authentications and variants of key escrow based on RSA. The aim of TCG is to provide:

- A remote attestation feature – trusted measurement is used to build a so-called “chain of trust” from the start up of the device to the full operation of a particular software module. After the device is turned on, the integrity of BIOS is verified against an expected value in PCR, and the

BIOS operations are then executed. The integrity of the operating system loader block is then verified by BIOS against the PCR before the execution is passed to the OS loader. The same process is repeated again and again before execution is passed to another component. When integrity verification fails, the boot process is stopped. If the process successfully finishes, the started application (and its owner) can be reasonably sure that the integrity of all underlying components was not undermined.

- Platform authentication – a 2048-bit RSA private and public 'Endorsement' key placed on the chip during manufacture (TPM v1.1), or possibly later (TPM v 1.2), can be used to uniquely identify and authenticate the target platform. Once generated, the endorsement key cannot be changed.
- Sealed storage – access to private information is bound to a specific combination of hardware and software and cannot be accessed elsewhere. The feature is realised by combination of trusted boot process and additional keys stored in TPM.
- Secure I/O – also known as Trusted path, secure I/O provides a secure path (realized usually via an encrypted channel) between user input (e.g., keyboard) and the output device (e.g., video card) that prevents information being intercepted by an attacker. Both encryption keys and the integrity of the respective module are protected by TPM.

For the PICOS scenarios, TPM can be employed to provide general protection for the user platform against malware (not fully applicable now, as full support for TPM in an operating system is still required), and provide the secure storage of user keys and passwords (directly applicable) and platform authentication via an endorsement key or other keys generated and stored in TPM. Several uses for TPM relevant to PICOS have already proposed. The P2P reputation system with enhanced privacy (Kinateder and Pearson, 2003) utilizes an endorsement key to prevent false reputation claims and remote attestations, and to provide secure storage to protect reputation information on the user platform or when such information is being sent to other user's machine. Such a system can be used to maintain reputation in all three scenarios. This is especially so for the gaming community, where mostly virtual-only contacts are assumed. Robust support for sticky policies (Mont et al., 2003) can be used to bind data and allowed data usages together. Basic protocols for Remote attestation are extended to provide direct anonymous attestations with better privacy protection (Camenisch, 2004). Peer-to-peer access control architecture based on a TPM applied to voice-over-IP (Sandhu and Zhang, 2005) can be used to protect real-time conversations against interception. Note that TPMs are not themselves a panacea, as the communication path between a TPM and the rest of a system must also be protected to prevent the interception and manipulation of data from the TPM (Kursawe et al., 2005). The possibility of exploiting bugs in the programs remains as well. A list of current projects on trust can be found in Annex I.

3.1.4 PETs in mobile environments

Privacy can be established on mobile devices through either native applications, which are installed directly on the device, or through a mediation server somewhere on the Internet or with the mobile operator, which manages and protects the user's resources. In the following chapter, the two categories and some supporting technologies are described in more detail.

High level research on the programmability of mobile devices and supported libraries relevant to the PICOS objectives is examined for common platforms like Java Micro Edition, Windows Mobile and Symbian OS. A special focus was made on software libraries usable for the PICOS scenarios, namely, support for cryptographic functions, communication capabilities, and support for the secure execution of applications. Platform programmability, portability and overall platform security architecture is examined as well.

3.1.4.1 Server side privacy-supporting technologies for mobile devices

In the case when the user resources that need protection are managed by a mediation server on the Internet, the server has to act as policy decision point and has to manage the privacy rules on its site. The T-Mobile Privacy Management Gateway (PMG) follows this approach to protect the user resources' location and identity (MSISDN). If an application provider tries to retrieve the user's location through an enabling service of T-Mobile, the PMG is asked if the AP is allowed to perform this. The user is able to configure privacy rules for each application provider and resource type via either SMS (short message service for mobile) or a WAP/WEB browser. While the SMS interface is a native implementation of proprietary SMS protocols (UCP, SMPP), the WML/(x)HTML content is generated by the Java standard for markup generation, Java Server Faces (JSF). To target the current situation – that the devices in the market understand different web page formats, e.g. WML 1.x, WML 2.x (also known as XHTML-MP) or HTML – the standard implementation of JSF was extended by the mobile faces toolkit from Ericsson. This special extension allows the designing of a browser based on user interface in the form of (JSF) components, which are translated at runtime into different markup languages (WML, XHTML-MP or HTML), depending on the currently connected device. By using this extension library, it is not only possible to generate different content types, but it is also possible to convert images depending on the capability of the target device.

The PMG approach allows the provision of a privacy administration user interface to the customer, without touching or modifying the target devices.

If the resource or content that should be placed under privacy control is on the device, a privacy component must be installed on the device, which is described in the next section.

3.1.4.2 Client side privacy-supporting technologies for mobile devices

Depending on the underlying architecture and operation system of the mobile device, different APIs and SDKs are available for the implementation of custom privacy components or applications. The most popular operation system families are Symbian and Windows Mobile.

While both provide a special SDK for the C/C++ languages, applications for Windows Mobile can also be developed in .NET technologies. By using these proprietary vendor specific interfaces, it is possible to perform very low level device manipulations, but with the drawback that the written application must be adopted/adjusted for each family and/or target device. To give an impression about the possible target configurations, Symbian OS is organized in Series (Series 40, Series 60, Series 80, etc.), each series is subdivided into several Releases (e.g. "Series 60 Release 1"), and finally each release is divided into feature packs (e.g. "Series 60 Release 1 feature pack 2"). Windows Mobile, in contrast, is organized into the main categories "Classic", "Professional" and "Standard".

Portable Digital Assistants (PDA) with an open platform are increasingly dominated by Microsoft Windows Mobile OS, followed by RIM BlackBerry, Palm OS and Symbian. Smart phones are usually shipped with Symbian OS (65% worldwide share, (Canalys research release 2008/021)), Windows

Mobile (12%) or Blackberry RIM (11%) (the situation is different for the North America market, where shipping is usually with RIM (42%), followed by Apple (27%) and Windows Mobile (21%)). Open source operating systems have also started to appear, like Linux-based OpenMoko, Motorola Trolltech and Google's Android platform, but are now mostly incompatible and yet waiting for significant acceptance.

Furthermore, there are not only the two mobile operation systems with an open SDK. A lot of new mobile devices are delivered with proprietary operation systems that do not provide a low level SDK like the two above-mentioned. But nearly every new mobile device provides Java 2 Micro Edition SDK (J2ME). Similar to the Symbian SDK, the J2ME runtime machine is divided into configurations: the Connection Limited Device Configuration (CLDC) and Connected Device Configuration (CDC); and several Profiles, such as the MIDP (Mobile Device Independent Profile), Personal Profile (PP). Each version classified by a configuration and profile could, additionally, implement several optional packages, like crypto API, multi media messaging API, 3D rendering API, Bluetooth API, location API, payment API, etc.

Depending on the supported configuration, profiles and optional packages, the J2ME SDK gives the application control over the graphical display, communication channels (SMS, TCP/UDP, IRDA and Bluetooth), address book, etc. Furthermore, it is possible to register a J2ME application for special events like incoming SMS at a specific SMS-port or incoming HTTP calls. While the former should be supported by nearly every mobile network operator (MNO), the latter is usually restricted by the MNO through firewall rules. These technologies could be used to implement some privacy features on the mobile device. For instance, encrypted communication over SMS can be achieved through an application that combines the messaging API with the crypto API.

As shown in the PRIME research project, T-Mobile has developed a privacy enhanced pollen warning application prototype. Here, a customer could register at an application service provider and subscribe to a notification service for specific pollen penetration levels according to his or her current location. When the customer enters or leaves an area with a high level of pollen he or she has registered for, an information message will appear on his or her mobile device. Both the subscription process and the notification are done anonymously so that no involved party has all information in hand.

One component of this prototype, the "customer console", was implemented using J2ME SDK (here, MIDP 2.1/CLDC 1.1). This application spreads the information about the customer's identity, payment transactions, allergy profile and movements over three independent servers, so that nothing, except the customer console, has more than only a small amount of information on the customer,. The console aggregates all the information together and presents it to the customer in a user friendly way. All communication from and to the mobile device is done anonymously by using pseudonyms, and encrypted through custom encryption on the application level.

The latest noteworthy operation system for mobile devices is Google's Android. The first Android mobile phones were made available in the summer of 2008. Android is based on a Linux kernel and can be programmed through a proprietary java language dialect, which will be translated into byte code for the newly introduced Dalvik virtual machine. Therefore, it is best compared to J2ME DSK. Both J2ME and Android seem to share the same core Java APIs, such as java.util and java.net. But their APIs for graphics, UIs, etc., and the philosophies for developing applications, are very different. Android seems to be more tightly integrated (up to even the OS services provided and how they interact with the APIs), while J2ME is far more liberal in its specifications for the developer and mobile device manufacturer.

As protection against software manipulation, Symbian and J2ME application runtime systems provide verification mechanisms for signed applications during installation and runtime. The signed applications must provide valid information about the software vendor and used capabilities (like read file system, send message, etc.). Especially in J2ME, the user must grant each application access to the Internet, and a messaging system and local storage, except when the J2ME application has been signed by a trusted manufacture certificate like one from the mobile device vendor.

Here, we will focus on the programmability, security models and privacy supporting technologies of the most widespread platforms – Symbian OS, Windows Mobile and JavaME – in more detail.

3.1.4.3 JavaME

Sun's Java Micro Edition is a wide-spread Java-based virtual machine with a limited number of base classes and several additional packages related to mobile devices. General development is possible with several IDEs like Eclipse (Carbide.j, EclipseME plugins), NetBeans and JavaME SDK (http://www.j2meforums.com/wiki/index.php/Development_Tools).

Community development maintains Java Specification Requests (JSR), where specifications of optional extension special-purpose API for JavaME are produced (http://jcp.org/en/jsr/tech?listBy=1&listByType=platform). Several JSRs are interesting from a PICOS point of view. We will discuss selected specifications in more detail here, as similar functionality is usually available for other platforms too. Documents with specifications for each JSR are available at http://jcp.org/en/jsr/detail?id=xxx, where xxx is replaced by the relevant JSR ID number.

The following security and cryptography packages are available:
JSR 177: This security and trust services package provides optional cryptographic packages for the secure storage of sensitive data like a user's private keys, personal information or service credentials. Cryptographic support for payment protocols, data integrity and confidentiality is also provided. Recommended cryptographic algorithms for package implementation are SHA-1 hash algorithm, RSA with SHA-1 for signature, DES, 3DES and AES in ECB or CBC mode for symmetric cryptography with no or PKCS#5 padding. An important feature of the package is the possibility of communication with a JavaCard-based SIM smartcard, and therefore the execution of security-critical features of the JavaME applet on the cryptographic smartcard with additional protection. Implementation of additional algorithms can be obtained from an open source library like BouncyCastle (http://www.bouncycastle.org/).

JSR 229: Payment API provides a mechanism to initiate mobile payment transactions in a secure manner from the JavaME application. The actual payment architecture is hidden from developers, and the specification does not define any concrete implementation of payment architecture nor concrete user interface. Specific payment implementation is left to the API implementator.

JSR 300: DRM API defines the way to access protected content in a secure manner from JavaME, including content rendering, support for identifying and acquiring rights, and handling proprietary properties and rights. An interesting part of the specification from the PICOS point of view is the set of functions for protecting locally created content, as these functions might be usable for the protection of user sensitive information. The final release of the specification is just waiting (08/2008) for approval from all involved parties, and therefore is not implemented by current devices.

The following are the communication and location packages available:
JSR 164 & 165: SIMPLE Presence and Instant Messaging provide an API for instant messaging control, convenient message-based communication with remote users, and presence indication.

JSR 179, 293: Location API 1.0 & 2.0 enable location-based services via API for obtaining current position, and for the management of known landmarks stored in device. Version 2.0 provides additional features like map management, navigation, and the definition of a landmark exchange format for the portability to other devices of landmarks databases.

JSR 256: Mobile Sensor API allows the uniform gathering of data from any measurement data source. Sensors might be physical, like accelerometers, or virtual sensors that process or combine data from other physical sensors like a battery indicator. Sensors can be built-in, wired or wireless, or remotely connected. Besides obvious uses like controlling backlight according to ambient luminance levels, this API can be used to access biometric devices (if present), or aggregate remote information about other community members (e.g., a remote sensor that provides the position of friends).

Both platforms described in next section (Symbian OS and Windows Mobile) usually have support for JavaME execution. We will therefore limit description of the available features to native non-JavaME libraries. JavaME packages can be used if necessary, although usually at the price of performance loss.

3.1.4.4 Symbian

The main programming language for the platform is C++, but other variants are Java (there is an existing Java Midlet profile, see JavaME section), assembler and scripting languages like JavaScript, and WMLScript for browsers. Additional interprets are developed by external parties (e.g., Python interpret).

General development can be done with several IDEs (e.g., Eclipse, MS Visual Studio) with freely available SDK. From our experience, the combination of Visual Studio with the Carbide.vs 3.0.1 plug-in has proved to be the most convenient development platform because of its mature and fast IDE. The new signing process introduced recently (January 2008) makes development difficult for a developer without a PublisherID certificate. The portability of Symbian programs is far from optimal – the specification of a basic API contains several hundred classes, and only a subset of them is usually implemented by a specific device. The set of implemented functions even differ between related families of devices from the same manufacturer (e.g., the Nokia Nxx series).

Symbian version 9 introduced a significantly refactored security model of the platform (Nokia, 2006). The following basic concepts were introduced. 1) Multilayer security via capabilities (rights) to perform certain tasks divided into three main groups: Trusted Computing Base capabilities responsible for most critical tasks (creation of new processes and maintaining its rights), assigned usually only to kernel applications; system capabilities for managing low level device data (network control, file system access); and user capabilities for accessing user level services like voice calls, SMS and data transmissions, or for managing user contacts. 2) An hierarchical directory structure with private folders (so called data caging) to protect data processes without the necessity to implement and maintain ACL (access control list) structure. 3) The mandatory use of digital signatures together with certification of an application when capabilities are required for application execution.

Symbian Cryptographic API allows direct usage of build-in cryptographic mechanisms. The full set of cryptographic API is available only to Symbian consortium partners, but a limited set of functions for certificate management, software installation and secure communication protocols (SSL, TSL, IPSEC) is public (http://developer.symbian.com/main/tools_and_sdks/developer_tools/supported/crypto_api/).

Functions supporting digital rights management are available on most recent devices (OMA DRM 1.0 and 2.0 API). Several modes are available to protect sensitive content. Forward-lock mode is suitable for content that, once purchased, should not be forwarded to others. Combined delivery mode allows

the setting of the rights for a particular media object. A separate delivery mode allows super-distribution, where (encrypted) content itself can be freely distributed, but access (decryption keys) is granted only in a controlled manner. In principle, it is possible to use OMA DRM to protect the distribution of sensitive information about user in a mobile community platform.

Location based services are enabled via a set of basic packages for obtaining current position and the management of stored landmarks (Landmarks API, Location Acquisition API).

3.1.4.5 Windows Mobile

The main programming languages here are C++ as the native language, and C# and Visual Basic .NET as managed languages with an intermediate interpretation layer (.NET framework). JavaScript is also supported. Interprets for additional languages are available from third parties.

The basic development settings for Windows Mobile 5 and higher requires Visual Studio IDE (2003 or higher), Microsoft .NET Compact Framework v2 SP2, and the Windows Mobile 6 Software Development Kits. The development process is more mature than for Symbian OS, and does not require the developer to undertake an inconvenient signing process in the default settings of a client device.

Windows security model (http://technet.microsoft.com/en-us/library/cc182298.aspx) is less restrictive by default than that of Symbian OS, but can be set to several levels with respect to the installation of (signed) applications ranging from open platform, where all applications can be installed without user intervention, to closed platform, where only signed applications can be installed.

Depending on the chosen language, several cryptographic libraries are available. Microsoft cryptographic API (CAPI), as well as the desktop platform (Cryptxxx functions) are available for C++. If the .NET framework is used (C#, Visual Basic) then the System.Security.Cryptography library, with support for all common cryptography primitives, is available.

Windows Mobile has similar support for smartcards as the desktop platform, realized via the set of SCardxxx functions (winscard.dll). Programmable smartcards with JavaCard, .net, or cards compliant with PKCS#11 specifications can be used as secure storage, and secure execution environments for sensitive parts of the code can also be used.

The Windows Media digital rights management platform is supported and implemented through Windows Media Player Mobile. This protection framework is heavily concentrated on the protection of media content, and has limited usability for protection of user personal data (contrary to the JavaME and Symbian DRM libraries). Still, JavaME JSR 177 or JSR 300 might be used if the JavaME virtual machine is implemented.

Native API is available for communication with GPS modules, but no universal landmark management functions yet exist.

3.1.4.6 Mobile platforms development overview

The overall conclusion is that, today, mobile devices are generally well programmable and contain build-in support for cryptographic operations, or allow the adding of such support from existing open source libraries. An additional advantage is the possible support for specialized cryptographic hardware and secure execution environments realized via smartcards or build-in TPM devices. Sensitive user information can be encrypted, stored in secure hardware or, additionally, protected by a system of access rights.

Considering the inspected platforms, the performance of JavaME programs is significantly lower than that of native applications written for Symbian OS or Windows Mobile, but JavaME provides better portability, as it can be usually executed in a Java virtual machine on other platforms. The availability of a package with fast cryptographic support (like JSR 177) is vital for JavaME, especially for asymmetric cryptography. The other inspected platforms allow one to implement cryptographic mechanisms independently (if necessary, some cryptographic support is usually available) with reasonable speed.

3.1.5 Anonymity and pseudonymity

In remote transactions, there is a transfer of information between involved parties, which may affect their respective privacy, since the transferred information is now under the control of the other party. The European directive 95/46/CE, on the protection of individuals with regard to the processing of personal data, specifies in section 28 and in Article 6.1.c that:

"personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

Taking this directive into account, remote transactions can be classified into two large groups. On the one hand, those for which the client does not need to provide any sensitive information with respect to her privacy. On the other hand, those ones for which the client has to provide some sensitive information in order to be accepted as a valid party in the transaction.

3.1.5.1 Anonymity at the communication level

Based on the aforementioned principle of disclosing the minimal amount of information necessary to perform a given transaction, in open transactions the client should disclose neither any sensitive information that could reveal his or her identity, nor other information related to the transaction performed. However, due to the nature of remote Internet communications, both communicating parties are identified by their IP address, and it is usually easy to correlate an IP address with an identified entity. Therefore, even in open transactions, an individual's privacy is affected, and it is usually possible to correlate the client's identity with the performed transaction. Likewise, an external entity is also able to correlate both communicating entities in a remote transaction after analyzing the IP packets travelling through the network.

In open transactions, the client does not need to disclose any sensitive information; hence, protecting the individual's privacy is (simply) a matter of preventing any entity from correlating a given transaction with the IP address of the client involved. In other words, protecting individual's privacy consists on keeping the client's IP address from the server or any other external observer, but at the same time allowing the communication and transfer of information.

Chaum discussed the problem as well as the basis for its solution in (Chaum, 1981). Subsequent works evolved into diverse solutions based on the same principle, which involves avoiding a direct connection between the client and the server. Instead, a virtual path is established between several routers that are responsible for transferring the information between both communicating parties, but at the same time, such correlation remains hidden to all the entities involved except for the initiator of the transaction. Each router is only able to correlate incoming messages with outgoing messages, but it knows neither the origin of the message nor the final recipient. For the external observer, incoming and outgoing messages are encrypted, and therefore they can not be correlated with each other.

Consequently, the external observer cannot guess the route followed by each message. A rough survey of the main proposals follows:

As already discussed under 3.1.3.3 ***Mixnets***, (Chaum, 1981) was the first proposal to make the communication endpoints anonymous in such a way that neither the recipient nor the intermediate routers are able to correlate a given message with its originator. The system defines several intermediate nodes, or mixes, with public keys known to involved parties. When an intermediate node (mix) receives a message, it then deciphers and stores it until it reaches a specified threshold, or it reaches some specified deadline. In either case, it intermixes in time and sends the stored messages to the specified recipients. For example, when Alice wants to send an anonymous message to Eve, she encrypts the message with Eve's public key, adds the recipient and encrypts everything with the public key of a specified mix node. This process is repeated for each mix node in the path to Eve and the message is then sent to the mix node used for the last encryption. Each mix node decrypts the message, and after temporal mixing with other messages, it sends it to the specified recipient, and so on until the message reaches its destination. This scheme also allows an anonymous message to be replied to. The encryption primitive adds some random bits to preclude the possibility of an encrypted message being correlated with a decrypted one. Moreover, messages are divided into chunks and padded so that outgoing messages are the same length and can not be related to the incoming ones. The security of the scheme resides in the fact that it is necessary to corrupt all the mix nodes in the path in order to be able to break the anonymity of the message sender. If any of the mixes in the path remains honest, then the sender's anonymity is preserved.

Onion routing (Syverson, Goldschlag and Reed, 1997) is quite similar to Mixnets, but it is connection oriented, as opposed to mixnets, which were originally designed for connectionless communications. In this scheme, a routing network exists, composed of onion routers with known public keys, and onion proxies responsible for establishing an anonymous path from origin to destination. An application proxy is responsible for filtering outgoing messages in order to remove sensitive personal information. The onion routers in the same network are all permanently connected, multiplexing data transmissions, and the path followed by a given message is kept open for a while to allow bidirectional communication. For example, when Alice sends a message to Eve, the application proxy filters it and removes any sensitive information from the message, and sends it to the onion proxy, which establishes a communication path, through several onion routers, to carry an anonymous message from origin to destination. It then encrypts the recipient and message in a multi-layer structure encrypted for each router in a similar way to that done in mixnets. When a router receives a message, it peels off the outer layer and sends the result to the next router in the path until the destination is reached. As this scheme is oriented towards real-time connections, it does not enjoy the flexibility that mixnets have to perform temporal mixes, and therefore its security against external observers is diminished. Additionally, the application proxy as well as the onion proxy both know the origin and recipient of the message, and therefore they both must be under the sender's control. **Tor** (Dingledine, Mathewson and Syverson, 2004) is a second-generation onion router.

Crowds (Reiter and Rubin, 1998) is based on the idea of melting into the crowd to achieve anonymity. Senders compose a network or a crowd by means of a system module, a jondo, in such a way that they send their own messages as well as randomly routing the incoming messages. When a jondo receives a message, it does not know its origin, but only knows the recipient and the node where it came from; therefore, it cannot distinguish if such a node is its original sender or if it simply routed the message. Messages are encrypted by means of keys shared between each pair of jondos. An external observer can distinguish neither the initiators of messages nor the paths followed by them, which are merged

with the messages sent by the crowd. The scheme is oriented towards bidirectional communication with web servers, where each message between two jondos is attached with an identifier that allows a communication path to be established for delivering messages and replies. This identifier is transformed along the way. For example, when Alice wants to request a resource from a web server, Alice's jondo decides to route it through another (Bob's) jondo in the crowd, and therefore the message is encrypted with the key shared by both jondos, and sent to the intermediary jondo. At that moment, Bob decides to request a resource from another web server, which means that Bob's jondo must send two messages: the local message is routed through another intermediary jondo, and the message received from Alice's jondo is routed through another intermediary jondo after transforming the message identifier, and so on until some jondo randomly decides to send the message to the recipient. The path followed is stored locally for a while to allow the back-routing of any reply message.

Hordes (Shields and Levine, 2000) is based on the crowds system with some minor differences, the most important one being the way in which the reply messages are back-routed to their destination. These messages are broadcast from a router to all members of a given group in which the anonymous initiator of the message resides. The scheme offers features similar to the crowds system, but claims better efficiency.

These schemes, though suitable in practice for making communications anonymous, are not robust enough against attacks from a global observer capable of analyzing the network traffic over a long period of time, though the more distant the routers are, the more robust the system is against these kinds of attacks. These schemes exhibit similar features, except that mixnets are connectionless oriented. They can be sorted based on robustness as follows: mixnets, onion routing, crowds and hordes, with mixnets being the most robust, and hordes the least so. However, if they are sorted based on efficiency, then the order would be reversed.

3.1.5.2 Anonymity and pseudonymity in authorization based on privileges

In those scenarios where all potential users enjoy the same privileges to perform remote transactions, the aforementioned mechanisms which anonymize the client's communication endpoint are enough to protect client privacy. However, there exist many scenarios where the client must prove that he or she owns enough privileges to access some remote resources offered by a given server. In these cases, such privileges are normally to do with the possession of some features, properties, attributes, etc., which grant the owner the right to enjoy the corresponding privileges.

In these kinds of scenarios, usually the client is identified and then reveals the required features and properties by means of credentials so that they can subsequently enjoy the corresponding privileges. This scheme is an important violation of individuals' privacy, since a large amount of sensitive information about individuals is collected and correlated with the transactions performed.

The European directive 95/46/CE, on the protection of individuals with regard to the processing of personal data,[4] specifies in section 26 and in Article 2.a:

- "the principles of protection must apply to any information concerning an identified or identifiable person";

[4] A more extensive discussion of the data protection principles can be found in section 4.

- "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person";
- "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable";
- "personal data shall mean any information relating to an identified or identifiable natural person (data subject)".

Therefore, anonymity is a cornerstone in protecting individuals' privacy in those scenarios where the client must prove that he or she owns enough privileges to access a remote resource. Anonymity can be understood as a mechanism to preclude the possibility of an identified individual's being correlated with a set of privileges and transactions.

Likewise, based on the principle of disclosing the minimum amount of information necessary to perform a given transaction, there are scenarios where it is appropriate and sufficient that the client proves that he or she owns enough privileges, but at the same time does not disclose any sensitive information allowing such privileges and transactions to be directly correlated with him or her.

This interaction model allows for privacy protection, as well as precludes unprivileged users from accessing resources for which they do not have enough rights. In this way, it guarantees the rights of both parties: the server restricts access to those entities with enough privileges, and at the same time guarantees clients' privacy while allowing them to prove their privileges.

However, it is important to note that, in these types of environments, absolute anonymity does not exist, that is, when anonymous clients prove that they hold certain privileges, they are only anonymous with respect to the set of potential clients that also hold such privileges, the anonymity set.

Anonymous Credentials

Credentials provide a suitable mechanism to convey diverse information, which makes them very appropriate for systems where entities own privileges, whereas anonymity is a cornerstone in protecting individuals' privacy in those environments where the user must prove possession of certain privileges. Therefore, anonymous credential systems form the fundamental basis for privilege environments where individual's privacy is a concern.

In anonymous credential systems, entities prove possession of some credentials without needing to reveal their identities, protecting in this way their privacy by means of anonymity. These credentials enable entities to enjoy the corresponding privileges without compromising their privacy.

The concept of credential was introduced by Chaum in (Chaum, 1985), where it was defined in an abstract and general manner, though it was applied in a context where individuals' identities are protected by means of pseudonyms, defining in this way the first anonymous credential system, based on pseudonyms.

Chaum's pseudonym credentials (Chaum, 1985) is a pioneering work that defines the problem and the application scenario for anonymous credential systems. It had a major influence on all subsequent studies on the topic. This work focuses on pseudonyms as a means of providing anonymity to users. Thus, organizations issue credentials to anonymous users based on their pseudonyms, and the user can

transform such credentials so as to be able to show it to another organization under a different pseudonym, thereby achieving "unlinkability" between organizations. The proposal is based on blind signatures (Chaum, 1983), a cryptographic scheme proposed by the same author.

Chaum and Evertse developed the original idea and proposed a more elaborate formal model of the system (Chaum and Evertse, 1986). In this work, the mathematical model supporting the system is refined and detailed, and defines a formal framework to analyze the main properties of the system. However, the system needs a central authority involved in most of the processes, which means it is of little practical interest.

Brands' digital credentials (Brands, 2000) are based on credentials that convey multiple attributes relating to an individual. However, the user is able to selectively reveal only those attributes that her or she wants to show, concealing the others. Likewise, it is also possible to prove logical relationships about the attributes encoded in the credentials without the need to show them. The issuing organization is not able to correlate a credential issued with the fact of showing attributes from that one. However, it has the drawback that each use of a credential can be correlated with another use of the same one, a fact that diminishes the degree of anonymity provided by the system.

With **Camenish and Lysyanskaya's anonymous credentials** (Camenisch and Lysyanskaya, 2001), organizations register users by means of pseudonyms, different ones for each organization. These pseudonyms are used by users to apply for credentials. These are statements that issuing organizations guarantee to be true about the holder. By means of a zero-knowledge protocol, the user is able to prove that he or she owns a given credential relating to a specified pseudonym. The organization is not able to extract any additional information other than that the condition is satisfied. An organization issues credentials to a given pseudonym acting on the user's behalf. The user is able to show this credential to another organization under a different pseudonym by which the latter knows the user. Because of the nature of zero-knowledge protocols, the showing of a credential to an organization is anonymous and non-linkable to other showings, even for the issuing organization. Moreover, the system provides some mechanisms to dissuade users from sharing credentials. However, all shown actions from a given user before the same organization are correlated, since all of them are shown under the same pseudonym. This fact has a major impact on the degree of anonymity that a user may obtain. Nevertheless, although users are anonymous, in some circumstances, it is possible for an organization with special privileges to ascertain which user has performed a given anonymous transaction. **Idemix** (Camenisch and van Herreweghen, 2002) is a prototype implementation of this anonymous credential system, which is part of the European PRIME project, and provides the core support for an anonymous credential system to be used in different scenarios.

Verheul's self-blindable credential certificates (Verheul, 2001) are based on credential certificates with pseudonyms, but in this case the user is able to transform such credentials into different pseudonyms with the purpose of concealing his or her identity, and also making his or her connections untraceable. The system provides mechanisms to support certificate revocation as well as mechanisms to dissuade users from sharing credentials.

In **Persiano and Visconti's anonymous credential system** (Persiano and Visconti, 2003), an individual obtains master credentials from organizations, and is subsequently able to transform them and prove that the attributes specified in such credentials fulfil certain properties in such a way that is not possible to correlate different users of such slave credentials. Moreover the system incorporates some mechanisms to dissuade users from sharing credentials. This approach is only interesting from a theoretical point of view, since it is not efficient in practice. However, in (Persiano and Visconti,

2004), an efficient system, based on computational assumptions derived from group signatures, is defined where users are able to prove logical relationships regarding attributes encoded in credentials, but with no need to reveal them. Unlike Brands' scheme, such proofs are non-linkable, which allows multiple proofs to be possible. It also incorporates some mechanisms to dissuade users from sharing their credentials.

Digital signatures for anonymity

With the work by Chaum and van Heyst (Chaum and van Heyst, 1991), a new kind of signature scheme was developed. They introduced a different approach where the correlation between a public and a private key is broken. In these signature schemes, many different private keys correspond with one public key in a one to many relationship, and even in some of them, many different private keys correspond with many public keys in a many to many relationship. These signature schemes allow us to focus on anonymity from different points of views with many interesting features. Group signatures (Chaum and van Heyst, 1991, Ateniese et al., 2000, Dodis et al., 2004), ring signatures (Rivest, Shamir, Tauman, 2001, Dodis et al., 2004), traceable signatures (Kiayias, Tsiounis and Yung, 2004, Nguyen and Safavi-Naini, 2004, Choi, Park and Yung, 2006), and fair traceable multi-group signatures (Benjumea et al., 2008), among others, are included within these new signature schemes. They share the interesting property that many different entities own different private keys, which enables them to issue signatures that can be verified with a single public key. Nevertheless, the verifier entity is unable to distinguish which entity, from the set of possible issuers, did actually issue a given signature. Additionally, it is not possible to link different signatures, even if they have been issued by the same entity. Therefore, these signature schemes provide two very important properties: anonymity within a set of possible entities, and non-linkability between issued signatures. Additionally, they have their own properties, which makes them very interesting in themselves.

With **group signatures** (Chaum and van Heyst, 1991, Ateniese et al., 2000) (GS), a group public key defines a group. A designated group manager, who owns the group private key, is responsible for joining new members to the group on demand. Whenever a new member is added to the group, the new member receives his or her own unique private membership key allowing him or her to sign on behalf of the group. The issued signature can be verified with the group public key, and it is neither possible to distinguish which member of the group issued the signature, nor even to link the signature with any other one issued by a particular member. However, the group manager has the special ability to identify which member of the group has issued a given signature, providing in this way reversible anonymity, in the sense that if a member abuses his or her anonymity, the group manager can open the signature and disclose the identity of its issuer. Another proposal for group signatures (Nguyen and Safavi-Naini, 2004) adds a fairness authority to provide support to the open primitive, which is only performed if there are enough conditions. This proposal adds fairness to the main scheme.

With **ring signatures** (Rivest, Shamir and Tauman 2001, Dodis et al., 2004) (RS), a ring is made up of the public keys of the entities that comprise the ring. These entities do not need to be aware of the existence of the ring, since their public keys are freely available. Any entity in a ring is able to produce a signature that can be verified with the ring public key, but no one is able to distinguish which entity issued the signature, or even to link it with any other signature produced by any entity in the ring. They provide similar features as those provided by group signatures, but ring signatures cannot be opened to disclose the identity of their issuer, which thus provides irreversible anonymity.

Traceable signatures (Kiayias, Tsiounis and Yung, 2004, Nguyen and Safavi-Naini, 2004, Choi, Park and Yung, 2006) (TS) are group signature schemes with additional tracing capabilities, which makes them very suitable for real-world applications. In addition to group signature properties such as indistinguishability and the untraceablilty of signatures from among any other one issued by a group member, and the ability of the group manager to open a signature issued by any member of the group, a user can claim that a given signature has been issued by him or herself. It is also possible, with the help of the group manager who provides members with a trapdoor, to identify which signatures from within a set were issued by a given member, without disclosing any other information. These additional capabilities make this scheme very suitable for real world applications, since the tracing capability is necessary in many real situations. This tracing facility enhances the anonymity features, since it allows the signatures issued by a given user to be traced without needing to open them. Otherwise, if tracing is not provided, it is then necessary to open all the signatures, and break their anonymity, in order to identify which ones were issued by a given user.

The **fair traceable multi-group signature** scheme (Benjumea et al., 2008) (FTMGS) is a modification of the traceable signature scheme with the aim to increase the fairness of the original scheme. With the modification, users get private membership keys after joining a group, which entitles them to issue signatures on behalf of that group. These signatures can be verified with the group public key, but they are anonymous in the sense that they are indistinguishable, and it is not possible to identify which member actually issued them. Moreover, in addition to the group manager, who is mainly responsible for joining new members to the group, the fairness authorities, based on non-repudiatable proofs, are responsible for opening a signature and for providing a member tracing trapdoor from information gathered from the group manager. If the fairness authorities do not collaborate (because the required conditions are not met), then the gathering and disclosure of restricted information becomes impossible. This splitting of duties between the group manager and the fairness authorities increases the privacy guarantees of users, since in many scenarios the group manager is trusted with respect to the joining of new members, but cannot be trusted with respect to the privacy of members. Additionally, this scheme offers some features to discourage the members of the group from sharing their private membership keys with other entities. This feature is very interesting since it prevents entities that do not belong to the group from cheating and obtaining benefits as if they belonged to the group. It also offers a primitive that allows a user to prove that two signatures are linked, i.e. that they were issued by the same user, while maintaining anonymity and non-linkability with other ones. In many authorization scenarios, a user has to prove that fulfils several conditions in order to be authorized, which in turn sometimes implies the proof that the user simultaneously belongs to several groups. In this scenario, linking signatures from different groups proves to the verifier that they have indeed been issued by the same user, and prevents an authorization proof from being composed of proofs from different users. In this context, a linked-signature is a signature attached with a linking-proof.

An interesting benefit of the approach based on digital signatures, apart from the ones provided by the scheme itself, is the fact that it can be transparently integrated into the standard frameworks (Benjumea et al., 2007) such as the X.509 and SPKI, which provide very interesting features regarding interoperability and heterogeneity.

3.1.5.3 Anonymity and pseudonymity in the context of the PICOS project

As it has been seen, privacy issues in the PICOS project have to be focussed by two complementary technical approaches. At the communication level, a communication of a community member (possibly using a mobile device such as a mobile smart phone) with a community server, or even with

another community member (in a P2P connection), entails that each communicating peer is able to identify in a unique manner the other peer in the communication, which would break any other privacy efforts that could be achieved in upper layers; it is therefore necessary to introduce an anonymizer layer (such as tor, crowds, etc.) at the communication level.

On the other hand, at the user's privilege level, clients have to be "identified" as members of the community, and possibly belonging to some sub-communities (or subgroups), in order to be accepted as a valid party in most of transactions, such as accessing community forums and databases, posting articles, establishing P2P connections, etc. Privacy in this model of interaction has to be focussed using a complementary approach that takes into account the privileges of users in authorization scenarios, but at the same time protects their privacy by means of anonymous (or pseudonymous) proofs of privileges. This approach can follow two different paths based on the aforementioned schemes, one based on anonymous credentials, and a different one based on group signatures (or derived ones). In this new privacy-aware scenario, users prove that they are members of the community (and possibly of some sub-community), but these proofs cannot be linked with the users' real identities (nor even with some previous transactions), which enable them to anonymously (or pseudonymously) carry out the transactions allowed to the members of the community. A second level of trust within the members of the community can be enforced by means of a reputation management system in concordance with the privacy supporting technology.

3.1.5.4 Interoperability, standard frameworks

One of the main concerns of the PICOS project is interoperability between different communities, as well as the provision of suitable support for communication using heterogeneous networks and devices such as servers, laptops, PDAs, mobile phones, etc. In these heterogeneous scenarios, standards play a fundamental role. This section briefly presents an overview of one of the most widely used standards in the field of security, as well as some proposed extensions to cope with privacy issues.

There are several standardization efforts to facilitate the interconnection of remote information systems, such as the X.509 (ITU, 1997; ITU, 2000) and SPKI (Ellison, 1999; Ellison et al., 1999) frameworks. The X.509 framework defines, among other things, the format for authentication credentials, that is, the public key certificates, as well as the format for authorization credentials, known as attribute certificates. These standard certificates convey relevant authentication and authorization information, which allows interoperability between heterogeneous systems.

The X.509 Framework

X.509 public key certificates (PKC) (ITU, 1997, Housley et al., 2002) have been designed to bind a public key to a subject under the consideration that such a subject is the only one that knows the associated private key. With these certificates, the certification authority (CA), i.e. the entity that certifies the binding, is equally important. Any entity using the public key certificate will trust the binding of the subject and the public key if it trusts the entity that issued the certificate. These certificates have proved to be a very useful tool for providing authentication in many different contexts, such as electronic mail, the World Wide Web, user authentication, and IPsec. In particular, the TLS (and SSL) transport layer protocol uses X.509 public key certificates to provide an authenticated secure communication channel to application layers.

X.509 attribute certificates (AC) (ITU, 2000, Farrel; Housley, 2002) bind a holder to a set of attributes, and at the same time can be linked with a X.509 PKC. The attribute authority (AA) is the entity that certifies such bindings. These attributes can be used for authorization in many different ways, providing a flexible approach. The holder of the AC is authenticated, by means of the linked PKC, to enjoy the privileges associated with the specified attribute. Here again, the authorization verifier needs to trust the certificate issuers in order to trust the bindings that they state.

The standard specifies two models for using X.509 attribute certificates in authorization processes: the push model, where the user, after being authenticated, sends the required attribute certificates to the server; and the pull model, where the user is authenticated and the server gets the required attribute certificates from some public certificate repository.

X.509 certificates are valid for a limited period of time specified in their fields. However, under certain circumstances, the binding can be revoked, e.g., if the private key is compromised or if the specified attribute no longer relates with the holder. If a certificate is revoked, then such a fact is made public by means of a public certificate revocation list (CRL) (Housley, 2002; Farrel and Housley, 2002). Additionally, OCSP (Myers et al., 1999) provides an interactive way to check if a given certificate has been revoked.

Standard frameworks and anonymity: The X.509 Semantic Extension

A recent work (Benjumea et al., 2007) proposes a semantic extension to X.509 certificates to allow new signature schemes, such as ring signatures, group signatures, traceable signatures, fair traceable multi-group signatures and others, to be incorporated into public key certificates as public key algorithms. This semantic extension makes it possible for the X.509 framework to enjoy the interesting features that these signature schemes provide, especially in the field of anonymous authentication. Additionally, the reverse also holds, that is, the semantic extension allows applications using these signature schemes to enjoy the features and facilities that the X.509 framework provides. Moreover, the semantic extension can also be applied in a similar way to other frameworks, such as SPKI (Ellison, 1999; Ellison et al., 1999), and others.

In this semantic extension, several entities can own different private keys that correspond to only one common public key certificate. Any of these entities can be authenticated as the right holder of the certificate, if he or she proves ownership of a private key that can be verified with the public key specified in the certificate. It must be pointed out that, because entities have different private keys corresponding to the one specified in a public key certificate, they can be authenticated as the right holders of the certificate and can enjoy the benefits that such authentication entails.

The properties of the aforementioned authentication process mainly depend on the public key algorithm used. These algorithms mainly provide anonymity and some other related properties to the authentication process. In these signature schemes, the signature issued by a member of a group (or ring) cannot be related to the entity that indeed issued the signature, nor can it be linked with any other signature; in this way, anonymity is thus provided to the signature issuer. Additionally, related properties are also offered such as reversibility, traceability and others. Thus, the semantic extension entails a subdivision of the entity authentication concept, which now may refer to identification and to anonymous authentication, depending on the properties of the signature scheme used. These properties are specified in the public key certificate itself, which allows the certificates to be properly used in the scenarios where they are required. Note that these signature schemes support anonymous

authentication by allowing a given member to sign a random challenge on behalf of the group, which can be verified by an authenticator with the corresponding group public key.

3.1.5.5 Conclusion

Anonymity and pseudonymity are very important technological means to protect users' privacy in many different scenarios. The state of the technology at three different and complementary levels have been examined: (i) the communication level, (ii) the user's privilege level, and (iii) the standardization level. These technological approaches have an important influence on the design of privacy concerned architecture supporting the PICOS mobile community system.

3.1.6 The assurance process

Since we have proposed the use of assurance cases for PICOS, we will concentrate here on state-of-the-art security assurance methodology.

The goal of software assurance is to provide credible evidence that software meets its required properties. The usage of the term varies, but always refers to a reduction in the level of uncertainty concerning issues such as the achievement of a goal, prediction, inferences, etc. This is achieved basically by adopting a specification mechanism for asserting the desired security properties of a system, planning, and assuring compliance with the requirements.

Security assurance concerns the required security properties of a system, including privacy requirements. Assurance must provide evidence that the number of vulnerabilities in a piece of software, including the presence of features that may be intentionally exploited by malicious agents, are reduced to such a degree that it justifies a certain amount of confidence that the security properties of the software meet the established security requirements, and that the degree of uncertainty involved has been reduced.

The state-of-the-art in software security assurance is much less mature than in other disciplines such as quality and safety assurance (Software, 2007). Security testing methods are immature, and testing by itself cannot gauge security, since security is not a functional property of the system, but often the absence of certain functional properties that are undesired but not totally definable in the presence of malicious or unintended behaviour. However, software assurance has been a very active area of research: some advances have been made over the last 10 years, and a high number of standards, techniques, methodologies, tools and initiatives have seen the light of day during this period.

It is widely recognized now that security is best assured if it is addressed holistically, systematically, and from the very beginning of the software's development process. We focus here mainly on the stat-of-the-art tools, processes, methodologies and techniques that follow this approach to software assurance.

3.1.6.1 Security engineering

No mature software engineering methodology today exists that integrates large scale system development methodologies with security issues (Mouratidis and Giorgini, 2007). However, there is widespread agreement among researchers today that security considerations should be introduced early in the system development life cycle. In this approach, system security issues must already be identified during the requirements phase of system development, and security requirements should be considered together with other kinds of requirements.

Several approaches have been proposed for developing system security requirements: fault tree analysis for security, Failure Modes and Effect Analysis (FMEA), threat modelling, misuse and abuse cases, and attack tree analyses, among others. Security requirements often conflict with other requirements, and adding security as an afterthought at a late stage of development may seriously impair the required functionality of the system. Many projects have failed because the security requirements were not clearly understood or were considered only at a late stage of software development, resulting in poor design choices and inadequate architectures from the point of view of security.

There is a bias in available software engineering techniques towards aspects of functionality, quality, and reliability. Security is, however, basically anti-functional, establishing what should not happen rather than what should happen. Nevertheless, many proposals have been made to extend system engineering processes such as ISO/IEC 15288 (ISO, 2008) and SEI CMMI (CMMI, 2002) to address security issues.

Attempts have been made to define a capability maturity model including security features, e.g., the Systems Security Engineering Capability Maturity Model (SSE-CMM), which add security activities to the Systems Engineering Capability Maturity Model (SE-CMM) (SSE-CMM, the Federal Aviation Administration (FAA)/DoD Proposed Safety and Security Extensions to Integrated Capability Maturity Model (iCMM), and the Capability Maturity Model Integration (CMMI)) (Pitblado, 2000).

The SSE-CMM is now an international standard (IDSO/IEC21827), and is intended to enable the addition of security practices into systems engineering to help improve an organization's security engineering practices, and to serve as a standard mechanism of evaluation and certification.

The FAA approach is an alternative to the SSE-CMM, but adds security activities to the iCMM and CMMI process areas instead of the SE-CMM.

There is, nevertheless, little empirical evidence to show the success of these methods and techniques (Software, 2007).

3.1.6.2 Assurance Based Development (ABD) and Software Security Assurance Cases

ABD (Strunk and Knight, 2006) has been recently proposed as an approach by which assurance is created throughout a system's development process, which thus integrates the development of a system with its assurance arguments. Criteria for the confidence of a development choice are thus provided at the time of choice, and not after, which facilitates detection of potential security assurance difficulties at an early stage of system development, and not after development when they are harder to address. In this way, security considerations can inform the requirements, design, architectural and implementation choices of system development.

The central concept of ABD is the *assurance case*. An assurance case may be defined as "a documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system's properties are adequately justified for a given application in a given environment" (Ankrum and Kromholz, 2006).

A security assurance case is a structured collection of security-related claims, arguments, and evidence, and presents arguments showing how a top-level claim is supported by objective evidence, while considering people, processes, and technology. An assurance case may also require taking into account non-technical issues such as legal and economic requirements.

The consequences of a security breach will affect how much effort is put into developing arguments and claims, and some cases may therefore require a higher standard of evidence and argumentation than others. Evidence supporting assurance cases may include testing, code review, formal mathematical proofs, arguments about the nature of the development process, the reputation of the development organization, and the trustworthiness of the developers, among others.

Early development of an assurance case can improve the development process by establishing the assurance and evidence requirements needed in every stage of the software development life cycle, as it may be very hard and costly to generate the required security case evidence once development is complete.

Assurance cases were first developed for safety requirements, where they have been successful. However, there is currently very little empirical evidence that assurance cases improve the security of software. Efforts are currently underway to standardize the content and structure of assurance case artefacts, as well as making software assurance processes an integral part of the system development process.

3.1.6.3 Assurance cases: Initiatives

The most mature software security assurance case standard is *SafSec* (SafSec, 2006), which has been tested on only a few case studies. SafSec is an assurance methodology developed by Praxis High Integrity Systems and sponsored by the UK Ministry of Defence (MOD). SafSec is intended to provide an integrated view of assurance, and a standard structure for producing and evaluating a combined assurance case for safety and security. Other goals are to ensure completeness, to minimize overlap and duplication of evidence, and to provide a single methodology and framework for safety and security certification and accreditation of products and systems. Assurance activities in SafSec are initiated at the earliest phases of a system development life cycle.

Another effort at standardizing security assurance processes is the *ISO/IEC* and *IEEE 15026, System and Software Engineering – System and Software Assurance*. The software assurance case has been proposed within ISO 15026. The ISO 15026 proposes the assurance case as the central artefact for establishing confidence in the security of system. The standard describes an assurance process that provides evidence that critical requirements are satisfied throughout the life cycle of a system. It consists of an *assurance plan* establishing the objectives, activities, resources and responsibilities for safety/security/dependability during the system life cycle, as well as an assurance case. The latter consists of a set of structured assurance claims with arguments and evidence that show how assurance requirements have been satisfied. The arguments and claims will be built and maintained throughout the life of the system, and be derived from sources such as artefacts generated from other application practices.

The standardization process of the IEEE 15026 has now been taken over by the Institute of Electrical and Electronic Engineers (IEEE) and its initiated project P15026 (System and Software Engineering – System and Software Assurance) (Hampton, 2006). P15026 was approved on 22 August 2007 by the IEEE-SA Standards Board until 31 December 2010.

The *International Working Group on Assurance Cases* (for Security) (Bloomfield at al., 2006a) was formed to work on assurance cases for security. Its point of departure was a workshop organized in June 2004 in Florence, Italy, and entitled “Assurance Cases: Best Practices, Possible Obstacles, and Future Opportunities”. Thereafter, in order to promote communication between groups working in the area of assurance cases, a new workshop focusing on assurance cases for security was hosted by the

Workshop on Assurance Cases for Security in June 2005 in Washington (Bloomfield at al., 2006b). This workshop expressed the need to support the communication of risks between stakeholders in critical infrastructure, and advanced the idea that assurance cases could be suitable for this purpose because of their modularity and flexibility, since they could be applied to whole systems, components, processes or organizations. It was concluded that it should be possible to develop a single methodological framework for assurance cases.

In March 2006, a new workshop, titled "Assurance Cases for Security: Communicating Risks in Infrastructures" followed, which was hosted by the European Commission's Joint Research Centre in Ispra, Italy. The workshop concluded that assurance cases were a viable way of supporting the communication of risks between the different stakeholders involved in critical infrastructure.

A fourth workshop was held in Edinburgh, Scotland on June 27, 2007 and titled "Assurance Cases for Security – The Metrics Challenge". The purpose of this workshop was to investigate the state of practice in metrics for assurance cases in the context of security, and to identify research directions in the area.

Many problems associated with assurance cases were highlighted in (Ankrum and Kromholz, 2006). These problems include: the volume and nature of the required evidence; the lack of explicit relationships between assurance claims, arguments, and the supporting evidence; the lack of support for structuring the information; the lack of a standard set of rules of evidence; the lack of guidance on how to gather, merge and review arguments and evidence; the lack of guidance for weighing conflicting or inconsistent evidence; and the difficulty in comprehending the impact of changes because of the huge volume of information. There is hope, however, that these problems may be mitigated by the development of tools supporting assurance cases.

3.1.6.4 Conclusions

One of the objectives of the PICOS project is to evaluate the effectiveness of the PICOS platform through the application of state-of-the-art assurance methods. In Annex 1, p.35, it is stated that "Assurance must be an integral constituent of the PICOS solution, and we do believe that it should be pursued in a holistic manner". However, no mature assurance technology which is integrated with system development and adopts a holistic approach seems to be available today. We consider that security assurance cases seem to be a promising methodology and to fit well into the assurance objectives of PICOS, not least from the research point of view. Particularly, the development of privacy assurance case patterns for particular security privacy laws and regulations could be an important research result of the PICOS project.

3.2 Overview of community platforms and of mobile technologies

3.2.1 Community platforms

Over the past three years, the biggest thing which has happened on the Internet is the rocket-speed growth in the usage of social networks and community services.

The latest available statistics speak for themselves:

For the month of June 2008, the Internet has a whole received 860 millions visitors. Among those, 580 millions visited social networks! (http://www.comscore.com/)

While the social networking services domain has two large players, *Facebook* and *Myspace*, the landscape appears as very segmented when analyzed from several perspectives:

- Service Providers.
- Technology providers.
- Consumers/end-users.

This segmentation is complex because of the business model and associated players of the domain.

The following figure (Figure 4) highlights the players in this business along with their inter-relationships.

A central role is played by the **Community Service providers**. These provide a set of services to well targeted communities. Services include information publishing and sharing, community oriented communication services, and the creation of direct connections between members.

Community service platform operators: these players usually operate service platforms for a number of service providers, and have lower costs of operation through economies of scale.

Community software vendors: there are a large number of specialised software vendors, with a large majority of them selling the software "as a service" (SaaS).

Advertisers: these players are make the business of community services a reality through linking commercial goods vendors to the relevant consumer communities.

Community members: by joining online communities and participating through the sharing of information and user generated content, these players help the online community to develop and grow. They hence become an attractive target for advertisers, and help generate more money for developing the community service.

Mobile and Convergent Operators: these players deliver the basic communication services that are key to supporting communication services within the communities (voice communication, messaging, mail, multimedia).

The PICOS project receives research funding from the Community's Seventh Framework Programme.

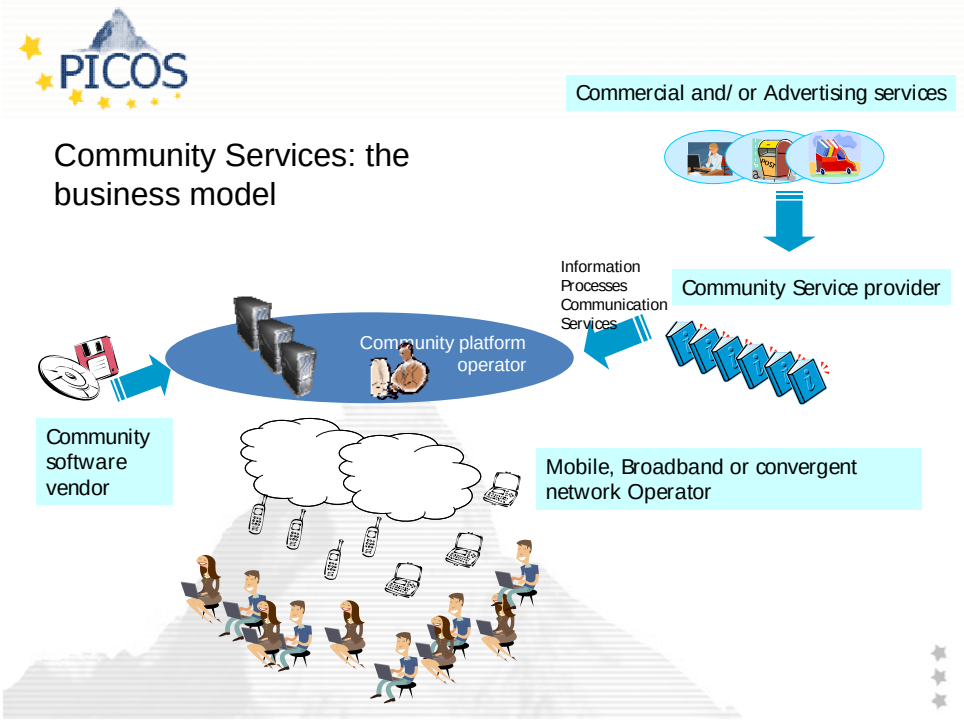

Figure 4: PICOS Community Services: the business model.

Membership to social networks is generally expected to be free of charge for the end users, qith subscription fees being a possible and acceptable option for either professional networks or highly value added “centre of interest” types of communities.

Deploying and operating a social network service has costs (such as the computer based platform, the development and support of software components, site administration, etc.), so advertisement-based revenue is the general business model for service providers in this domain.

Community services are a very attractive target for advertisers, since the members gather together because of shared centres of interests, which hence makes them an efficient channel for targeted advertisements:

- Advertisers know the profile of the community
- Community members are receptive to advertisements linked to their centres of interest(s)

Analysts are still cautious about the market opportunities for advertising linked to community services. The eMarketer company forecasts US advertisement spending on social networking sites to reach US$ 2.5 billion by 2011, which is approximately 6% of the total anticipated US online advertising spending for the same period.

Several reasons make this outlook uncertain; a paper from Technology Review, an MIT publication (July/August 2008), comments that, "the problems with social-network advertising revolve around three main issues: attention, privacy and content".

While members tend to share private information within their communities, they are very concerned about the management of such private data, and in particular when making this information available to advertisement companies. As an example of this, the attempt made by FaceBook (November 2007) to track users' purchases on commercial websites and display them to their friends was badly received and had to be scaled down to an "opt-in" option only.

3.2.1.1 Insight from the consumer/end-user side

Analysis of the services/features offered by the social networks and community services tells that, besides a set of atomic functionalities common to almost all the services, these services can be divided according to the specific functions each delivers to the targeted types of communities.

- Bookmarking and news (*Technorati, Del.icio.us* ...).
- Consuming (*eBay, Like* ...).
- Events and trips (*Travellerspoint, Virtual tourist, I'm in* ...).
- Entertainment (*Habbo, Second Life, Cyworld* …).
- Location spotting (*Wayn*..).
- Media sharing (*Last fun, Tabblo, Flickr, Youtube* ...).
- Micro blogging (*Jaiku, Twitter, LiveJournal, Plurk* ...).
- Searching / Organizing (*Spock, Yelp* …).
- Social networking (*Myspace, Facebook, LinkedIn, Bebo, Orkut, Mixi* ....).
- Interest groups (*Catster, Care2, Lifeknot* ...).
- Calendars and lists (*Plaxo, Meetup* …).
- Group innovation (*Scispace, Storymash* …).

The functionalities presented in the following Table are the "core" features that are available on almost all social networking/community services.

User/member authentication	Authentication mechanisms are very simple and almost always based on a login/password mechanism.

Ability to create personal profile	A personal profile is a set of attributes which describes a community member as he or she is or, as he or she wants to look like within the network or the community. Profile attributes may be flagged as private or public, so they can be seen by everybody, by the community members or only subgroups within the community. Members can also be allowed to create multiple profiles such as, for example, a "business" profile and "private" profile.
Upload / download of pictures, audio, video files	Each member has the ability to upload a certain amount of personal data onto the community platform and has the ability to download an unlimited volume of data from the same platform (downloaded data can be either user-generated or commercial data). Uploads/downloads are performed from/to a personal computer device. Some community services offer the ability to upload multimedia documents directly from a mobile device (PDA or mobile phone) using various mechanisms (SMS or by a specific application installed on the handset).
Document storage and management	Members are offered a data storage capacity on the community service platform along with related management tools.
Tools for building communities (Networking, groups, communities)	These tools offer key capabilities for members so they can build groups within the community, or develop networks (friends, business relations) or communities based on specific centres of interests. Such tools include the ability for members to discover/browse other member profiles, to invite people and manage groups.
Creation and management of forums, message boards or wikis (including moderation functions)	Each community member is offered the possibility to create and manage his or her own discussion board(s) or forum(s), along with, optionally, some moderation capabilities once the forums are opened to the public (non-community members or non sub-groups members).
Document sharing (including profile)	Sharing information is the key reason for an individual joining a community. A sharing capability applies to all content a member has uploaded on the community platform, including his or her profile attributes.
Search tools	This function is of importance for large communities where large quantities of information are shared by the community members.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Recommendations/rating/feedbacks	This function can be implemented as a standalone feature, or embedded with the content sharing function, depending on the structure of the community platform and the community objective. This function allows members to evaluate and comment on content/information placed by other members.
Document tagging	This function is usually linked to search tools, since tagging helps structured searching.
Communication functions (IM, e-mail, voice, video communication)	The basic communication function offered on all social network/community platforms is the text chat, which is a real-time text conversation. This function, called "instant messaging" is coupled with Presence/availability, indicating the dynamic availability status of the community members. Additional communication functions can be offered, such as e-mail, SMS (to connect with mobile members), and voice or video telephony (mostly using the voice or video over Internet). The communication function supports one to one interactions, but is often extended to group chats.
Presence management	This function is tightly coupled to the communication text chat function, and indicates a member's availability for conversations with other members. Members can set their presence status according to a variety of flavours (textual information), and can control who can access this information.
Notifications (e-mail, SMS)	Notification about "events" happening within the community or within a sub group is a key capability which makes members feeling "connected" to the community. A member posting a new document, a new sub group being created, and a new member joining a sub group are examples of events for which a member may want to receive a specific notification, instead of just simply discovering it when he or she connects to the community service. E-mail is the most popular notification mechanism, SMS being only offered in very few community services (for the obvious cost reason).

The PICOS project receives research funding from the Community's Seventh Framework Programme.

RSS imports and/or exports	RSS (Really Simple Syndication) protocol is a standard Internet protocol allowing users to get updates about information located on different places on the web. This mechanism is very useful within communities for both export and import functions. Community or sub group members can be easily updated on information of interest for the group located outside the community platform, and can be offered an update mechanism for information available to external world.

Table 3: Common functionalities offered to end users.

3.2.1.2 Insight from the Service Provider side

Service providers are the people who offer the social networks/community services to the end users.

Offering a community service means performing the following functions:

Building the service platform, including software development

Only a few social networks have developed their own service platform. The market has rapidly become structured with specialized actors. A few companies are designing and selling software platforms for communities. Software design ranges from a full custom design tailored to very specific community service requirements, to a generic platform software which can get customized (to a limited extent) by the service provider or by the software vendor (we will go into more detail in the "technology" section later).

Social Platform (now *OneSite*) is an example of fully customizable software platform.

PhPFox, *ELGG*, *Drupal* and *Joomla* are examples of downloadable software platforms.

Operating the service platform

Specialized companies offer to operate community service platforms in "hosted" models. Operation includes maintaining and running the hardware and software elements, keeping the platform connected to the Internet, and ensuring the smooth growth of the platform elements so as to adapt to the volume of community members.

Companies hosting social networks/community services are mostly also developing the software components. On a single physical platform, they can host multiple social networks/community services. This is called "white labelling".

Examples of these companies are *Ning*, *KickApps*, *Prospero Technologies*, *CollectiveX*, *Broadband Mechanics* and *AffinityCircles*, just to name a few.

Managing relationships with service users

This is definitely the role of the community/social network service provider. While most of the services are offered for free to their members (no subscription fee), the relationship with the service

users focuses on the "brand" of the service, including its ethics and culture. This covers aspects related to community profiles, and handling legal aspects (copyrights, defamation, privacy, child protection, etc.)

Managing the service revenue streams

Service providers offer social networks/community services according to basically three business models.

Revenues from advertising

This is the far most frequent business model. Here, service providers sell their "community members" as targets for advertising. The more members the community has, the more valuable it is for advertising companies. Hence, the race to grow community/social network size.

Selling the member profiles (preferences) as valuable information to advertising companies can also generate revenues. However, such a business model is very risky since members can quickly run away from the community because of privacy abuse, if not informed beforehand about the commercial usage of their personal information.

Revenues from goods sales

This business model is common for community services built on "centres of interest" or "consuming" types of communities. Managing a community in this case is done as a sales tool, so members are encouraged to buy goods, through easy discussions, evaluations, and rankings from other members.

Advertising is obviously implicitly coupled as a revenue stream with this model.

Revenues from subscription

In this case, service providers generate revenues through subscription fees paid by each community member. The fee may correspond to subscription to a physical community, where the online service is provided as a free service to the members or the community can be purely "online".

Such a business model mostly applies to professional communities, where community services like information sharing and searching, and discussion forums, bring significant value for members in their professional activities (e.g. *XING*).

Platform functionalities offered to service providers

Community service creation

- Ease of platform set-up.
- Capabilities for customization of the service user interface and inclusion of specific service branding.
- Capability of including third party advertising or own advertising on the service platform, and flexibility for advertising types and placement.
- Creation of custom domain names.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

- Presence of application programming interfaces for integration of additional functions to the service platform. Integration of applications can be done by the service provider, but can also be done by the service members (widgets, mash-ups).
- Multilanguage support.

Community service operation

- Content moderation: a content moderation system enables network administrators to review and approve submissions (such as photos and videos) before they are displayed.
- Network and usage statistics collection and management tools.
- Network and user limits configuration tools.
- Advertisement management systems.
- Member administration systems, including provisioning and deletion functions.

3.2.1.3 Insight from the technology side

As community services are at the heart of Web 2.0, all service platforms are developed using web technologies, protocols and software development tools.

The buzzwords for software developers are *simplicity*, *lightweight* and *flexibility*.

The architecture model is client-server, where the community service users are using their favourite web client software browsers to access the services.

The big innovation that social network services bring to end users is the concept of mash-up, which allows the end users, the Service Providers or Independent Software Vendors (ISV) to develop their own applications through the combining of information coming from different sites or different providers.

These capabilities rely on community services and application providers offering open API (Application Programming Interfaces) that can be used by external applications developers to access information programmatically. A well-known example is *GoogleMaps API*, which allows one to embed a Google map within –for example– a location spotting service.

This mash-up concept is the key support of the collaborative capabilities of Web 2.0.

Mash-up applications can be integrated as additional services within a given community service platform; in this case they are presented to the end-users as “widgets”. For example, mashing-up a Google map with the address of your Facebook friends could be presented as a “where are you” widget on the Facebook UI.

Server side technologies

Because of the very rapid development of social network services, all service platforms have been developed using proprietary architectures and programming interfaces. This direction has also been

strongly influenced by the business models, where the goal was/is not interoperation with other networks, but rather capturing the largest number of community members.

The situation is not changing significantly, even though a couple of initiatives have emerged that encourage more openness and standardization between community services.

This trend for standardization/openness is being pushed by the end users and the applications developers.

- End users need to belong to multiple communities, and want to have their personal information, including their profile information, accessible from all their communities, rather than having to duplicate them in each. End users also look for a unique/common authentication/login mechanism, so they do not have to remember multiple logins to their various community services.
- Application developers are delivering key added value to the community service platforms, which allows Service Providers to offer better capabilities to their end users. However, in this very competitive environment, application developers do not want to have to develop several times the same application to deal with various proprietary interfaces.

OpenSocial Initiative

OpenSocial is an initiative launched by Google in 2007. Acknowledging the fact that social networks /community platforms offer proprietary, heterogeneous and incompatible APIs for applications and mash-ups services developers, the OpenSocial objective is to standardize the APIs so an application can interact with a single design on multiple community platforms.

All documentation and code is available at (http://code.google.com/apis/opensocial/).

At the moment, a number of social networks platforms and/or services have endorsed the OpenSocial specification, among which Engage.com, Friendster, hi5, Hyves, imeem, LinkedIn, MySpace, Ning, Oracle, orkut, Plaxo, Salesforce.com, Six Apart, Tianji, Viadeo and XING.

Open ID initiative

Open ID is a project initiated by a non commercial organization (http://openid.net/foundation). Its objective is to offer web users an easy and secure way of logging on to multiple web sites by using a single identifier, profile and password.

This identification mechanism is based on a 3-parties process:

- The end user.
- The Identifier Provider.
- The Service Provider.

The Identifier provider role is to host the end user profile information, identifier and associated password.

When the end user logs on to a web service, he or she just provides his or her “openID” identifier. With this information, the Service provider queries the Identifier provider, who then prompts the end user for the password and agreement to log on to the service. Depending on the end user response, the Identifier Provider will accept the log-in to the service.

Authentication is not included in the OpenID function. OpenID is designed so the end user can select his or her authentication mechanism of choice.

Open ID is developed as an open standard, and an open source software license model. It is developed using web technologies.

Although it is still in its adoption phase, a number of big service providers have already adopted the system. According to the OpenID foundation, there are currently approximately 10 000 sites supporting the OpenID login and approximately 160 million OpenID-enabled URIs.

Client side technologies

Community services do not bring new technologies to the client side. Initially targeting access through broadband devices (PCs, PDA, laptops) and Internet connections, the de facto technology for clients is the web browser. Enriched with additional technologies like Flash or Ajax, web browsers offer end users advanced capabilities for the easy handling of multimedia content, and flexible design for flashy, customizable User Interfaces.

Mobile phones have started to be considered as relevant end devices for accessing social networks/ community services. However, no specific technologies have been developed for them at the present time.

Connecting to social networks from mobile phones can be done using several technologies:

- SMS/MMS connectivity: this capability is either available on any device (SMS), or on a large number of devices (MMS). Connectivity allows the uploading of text messages, pictures, and audio/video clips.
- WAP/Web connectivity: such connectivity allows simple access to the service, in browser mode, with no custom client software to be installed on the mobile phone. This connectivity offers downlink communications from the service to the end user (e.g., reading posts and messages). However, WAP/Web connectivity offers a mediocre user experience and slow performance.
- IP access over GPRS/CDMA/EDGE/3G: data connectivity offered by mobile network operators that brings better performance when connecting mobile phones to the Internet. However, the web UI still does not deliver an acceptable user experience, so the need for using dedicated software clients on mobile devices still remains.

Handset manufacturers have started to “factory install” client software on some devices for accessing selected leading social networks/community sites. Independent software vendors (ISVs) are also developing mobile clients for accessing some leading community services.

However, the development of mobile access for community services is hindered by the need for specific clients on handsets, for which installation and operation is far less usable than is the case for the laptop/desktop computer environment.

The development of mobile client software is also complex because of the number of different operating environments on mobile equipments. When developing client software, ISVs have to generate multiple versions to be able to support a significant number of mobile phones.

3.2.1.4 Insights from privacy, ID management and trust management

Identity management

Almost all social networks/community services platforms implement an identity management mechanism based on a simple login/password. Pseudonymity is possible through usage of pseudonyms, which can be attached to a user ID.

The Open ID initiative (see above) – which is not specific to community services – has the goal of simplifying the login mechanism for users who are accessing multiple web sites. With OpenID, the end user can enforce the authentication mechanism.

Privacy

Even though management of private, personal information is of great concern when joining communities and sharing information, current social networks/community services only offer some basic capabilities to end users with regards to privacy:

- the ability to appear on the network through a pseudonym;
- the ability to restrict profile information access (e.g. “my friends”);
- the ability to split profile data into public and private parts, or into private and business parts;
- the ability to expose “my presence” status information to a limited audience.

Some services provide advance notification on the usage of private information on the network.

Trust management

This is a really weak area, even if trust is of significant value within community services.

Current implementations are limited to rating/feedbacks/recommendation methods for shared information.

3.2.2 Mobile technologies

Mobile communications and services provided to mobile devices such as mobile phones or notebooks are based on a number of protocols and technologies. This section will present the most important of them from a mobile operator’s point of view. The technologies are categorised as “communication technologies”, “enabling services” and “customer services”. These communication technologies have the basic functionality to support voice and data transmission. The enabling services provide general functions that are used by one or many customer services. The customer services are built on top of the communication technologies and the enabling service. They are targeted directly at the customers.

The aforementioned categories will now be presented in turn.

3.2.2.1 Communication technologies

A large number of communication technologies exist for digital communication between devices (and through these devices, between people as well). In the following list, we will focus on wireless communications, and present the most important technologies and standards.

- **GSM**: The most widespread wireless communication technology worldwide is the Global System for Mobile Communication, which was first standardized in 1990 by the Groupe Spécial Mobile of the European Telecommunications Standards Institute (ETSI). The standard describes different layers of (cable based and wireless) communication and call signalling, as well as a distributed architecture with well defined responsibilities. The standard also contains specifications on management functionality, such as customer device subscriptions, handovers between cells, paging on incoming calls, etc. This so-called 2nd generation network is circuit switched, meaning that each partner that is willing to communicate has to allocate a specific bandwidth whether he or she uses it or not. To protect customer communications, different privacy features have been implemented. First of all, the customer identifier is only sent over the wireless link during the subscription phase. From that moment on, a so-called Temporary Mobile Subscriber Identity (TMSI) is used for communication. Additionally, the wireless link between the mobile phone and the base station is encrypted. A set of different encryption algorithms is available. The one to be used is negotiated at subscription, but this may be re-negotiated later on. However, all encryption algorithms of the standard have proven to be (relatively easily) breakable, so one should not rely on them for highly confidential content. It also turns out to be a problem that the encryption is only performed between the base transceiver station and the mobile device, as the transceiver station often sends its content to the core network through (wireless) directed microwave radio transmission. An additional security risk comes from the authentication being unidirectional. As the base station does not authenticate to the user device, man-in-the-middle attacks can be performed with fake base stations. Some mobile phones with additional end-to-end encryption to remedy these problems are available from different providers.
- **(E)GPRS**: The (Enhanced) General Packet Radio Service is an extension of GSM for data packet transmissions, which was standardized in 1998 by the Standard Mobile Group (SMG), a successor to the Groupe Spécial Mobile. The packet switching on top of a circuit switched network is simulated by the use of virtual channels. Such a channel can be reserved by various devices simultaneously, and is used only when data is actually transmitted. This technology is known as 2.5th generation networks as it is an intermediate between circuit and packet switching. GPRS is mainly used for Web- and WAP-Browsing, as well as for MMS transmission. In terms of privacy, the technology relies on the mechanisms of the underlying GSM protocols.
- **UMTS** (**Universal Mobile Telecommunication System**): This 3rd generation network is the successor to GSM technology. It was standardized in 1998 by the ETSI, and the first national services have been available since 2002. The code division multiple access technology used for wireless transmission here has a higher robustness against interference than the time division multiple access of GSM. UMTS is packet switched from the ground up, and provides a much higher bandwidth per device compared to its predecessor. The technology is targeted at general data communication, including World Wide Web, notification services, chatting, mobile-TV and voice transmission. The privacy features of UMTS are much more elaborate than those of its predecessor. So, the subscription at a base station now includes a mutual authentication procedure to prevent false base station attacks. The standard also provides a default authentication algorithm that can be used. However, the standard does not mandate how authentication is to be performed. The cryptographic

protocol has been improved and uses a 128 bit key (in contrast to GSM, where the key size was 54 bits), and the encryption extends to the core network.

- **W-LAN** (**Wireless Local Area Network**): This usually describes radio technology for locally bounded data transmission (up to a few hundred metres) that works on license-free frequency bands. The most widespread standards in this area are the Institute for Electrical and Electronics Engineers (IEEE) 802.11b and 802.11g, which were adopted in 1999 and 2003 respectively. Both standards provide transmission at the moderate rates of 11MBit/s and 54MBit/s. These standards have received some criticism because of their low level of privacy protection: by default, data is transmitted without encryption and the defined Wired Equivalent Privacy (WEP) algorithm, which is specified for protected traffic and is based upon the RC4 encryption algorithm, turned out to have serious security flaws. Since 2007, the new IEEE 802.11i specifies new authorization and encryption mechanisms, also known as Wi-Fi Protected Access (WPA). With WPA, authorization is performed by the use of a pre-shared key, or through the Extensible Authentication Protocol (EAP).
- **Bluetooth**: Designed for local communication between battery powered devices, version 1 of this standard was published in 1999 by the Bluetooth Special Interest Group. The second version was published in 2004. The field of application is local wireless communication at a range of 10m to 100m, mainly between mobile phones and between mobile phones and their accessories. It uses the same frequencies as the previously presented W-LAN technologies. Interference between devices is reduced by using frequency hopping during communication. Bluetooth specifies a number of pre-defined service profiles (these are sub-protocols that act at the higher protocol layers) for different tasks. Some of the most commonly used ones are: the Object Push Profile for file transfer, the Dial Up Networking Profile for use of a mobile phone as an Internet gateway, the Advanced Audio Distribution Profile for transmission of audio data, etc. Privacy is provided by link layer encryption, and authentication material is exchanged in a pairing phase when two devices first meet. It has been noted that the pairing process is vulnerable to attacks if the human-selected password is weak (which is rather obvious).

3.2.2.2 Enabling services

The implementation of the protocols that have been described in the last section gives the end user access to the communication infrastructure and permits basic data exchange services. However, the availability of a general communication infrastructure also spawns commercial and non-commercial providers that operate services. As, by itself, the infrastructure provides no support to third party providers for additional services, there are different (standardized and proprietary) solutions for external providers to get access to the system services. In the following, we will give a short overview of these so-called enabling services.

- **SMS-Gateway**: An enabler that provides an interface between IP-based services and the SMS-Subsystem of GSM. After authentication, a subscriber to the gateway service can send messages to mobile phones or receive messages. Often, the account of the subscriber is connected to a short code. This is a short phone number without area code that is only valid within one operator's infrastructure.
- **IN/SCP** (**Intelligent Networks/Service Control Point**): The IN permits for defining rules that are executed at different points of a phone call. These actions may consist of presenting

a voice recording to the caller when he or she picks up, letting him or her go through a voice dialog to set some call parameters, or having an external application perform call signalling.

- **IP Multimedia Subsystem** (**IMS**): A collection of services that provide multimedia to phone users. The system is IP based. However, it has also been integrated into existing GSM and MSISDN networks. The IMS provides ways to transfer multimedia content from and to different parties, to perform special billing, provide presence information, etc.
- **Location Server**: In location based services, the content provider has to access the location information of the end user. The location server is an enabler at a mobile network operator that provides information on the whereabouts of the logged in customers of the operator. The location information can be requested by MSISDN or by the IP of the end user, and is delivered in different location formats. The location is usually retrieved based on the radio-cell in which the customer is logged. The precision of this method ranges from 100 metres to 15 kilometres in GSM, but is somewhat higher for UMTS as these cells tend to be smaller.
- **Payment Server**: Many services provided in the GSM environment are charged services. However, as there is no direct relation between the provider and the consumer of a service, payment has to be performed by other means. One way to ease the process is by using a payment server. This has an interface to the content providers that enables them to bill the customer for their service usage. In this case, the payment server provider (usually the MNO) handles the collection.
- **Identity Management**: Due to the lack of ID information on the Internet, personalized services can be cumbersome to use. The customer has to create some kind of account for each service with personal information and leave authentication credentials. In the worst case, these credentials have to be entered each time the site is visited. An identity management service is a remedy for this. The customer can perform a single-sign-on operation with the service (this may also happen automatically), which means that he or she is then authenticated for all services that use the identity management service.
- **Privacy Management**: The goal of privacy management is to provide a data security layer for such services as identity management and location servers. It gives the customer the possibility to control which of his or her personal data that is stored in one of the aforementioned services may be disclosed to external service providers. The restriction is performed on a per-provider-basis, and granularity may be increased by specifying time restrictions.
- **Age Verification System**: This service has been thought of to permit the commercial exploitation of rated content in the Internet. As the name suggests, it is a system that enables the reliable verification of a service user's age of majority. The general task can be solved by different means. Of those the most reliable ones are the use of special smart-cards (as the German GeldKarte) and the use of an AVS-Server. For the latter, the user has to register at the service. His or her identity is usually verified once face-to-face in combination with his or her identity card or by Post-ID. If the customer wants to access rated content over the Internet, he or she is then redirected to the AVS-Server, where he or she has to confirm his or her authenticity by entering a PIN. In succeeding to do so, majority is assumed and the desired content is delivered. Another common AVS procedure (especially in the UK) is based on requesting the customer's credit card data prior to the access of the rated content.

3.2.2.3 Customer services

The enabling services that have been presented in the previous section are not of value to the customer in themselves. Most of them cannot even be used directly by customers. Those services that are to be used directly by the customer usually place a strong focus on being easy to use and available with standard hard- and software. This comes down to relying mainly on WML, (X)HTML or SMTP for IP-Services, and on SMS and voice for GSM-Services. However, there are obviously exceptions to this where the customer has to install some special software.

In the following, we classify customer services into single user and peer-to-peer services on the one hand, and community services on the other.

3.2.2.3.1 Single user and peer-to-peer services

- **Voice Call**: From the mobile operator's perspective, this is where it all began, and is still the work-horse for mobile communication. Aside from customer to customer communication, a number of providers for voice services exist. Some examples are service hotlines, counselling and erotic content. Most of these services are reachable through special numbers or short codes, and have an altered billing. This ranges from toll-free numbers over per-call billing to high rate calls. To protect their privacy, customers are able to suppress the transmission of their phone number for outgoing calls. If activated, the caller MSISDN is only transmitted until the last switching centre. However, this restriction can be overruled by the recipient for some special phone connections. So, police and emergency call lines always get the calling party ID. In addition, to get rid of unsolicited calls in Germany, there is a list of numbers that do not accept these kinds of calls. However, this is an anti-harassment measure rather than for privacy protection.
- **Short Message Service** (**SMS**): In Europe, this was one of the most significant applications of the 1990s and the beginning of the 21st century. They were initially conceived to transmit administrative content from the network operators to the customer, and were to be provided free of charge. However, when the popularity of this service became clear, the transmission type was promoted to a normal telecommunication service. One peculiarity of SMS is that each customer to customer message is sent through a short message service centre (SMSC), which forwards it to the final destination. This is either by forwarding it to the SMSC of another mobile operator, or by sending it to the destination directly. Similar to voice calls, SMS has been established as an enabler for services with alternate pricing schemes. Nowadays, mainly multimedia content downloads and chatting are provided for payment. There is no privacy feature, such as the calling line identification restriction for voice calls. However, there are SMS-Gateways in the Internet that let the customer to freely set the sender ID.
- **E-Mail Push**: E-mail is certainly one of the most widespread communication systems on the Internet. With the evolution of modern mobile devices in terms of display quality and connectivity, it is a natural step to have e-mails accessible on mobile phones. However, E-Mail Push goes a step further than most PC-based e-mail clients in that the customer does not have to regularly pull for his or her messages, but instead simply has new messages "pushed" to him or her, similar to an SMS.
- **Location Based Services** (**LBS**): This is a class of services that have some kind of localized model, and compute their results taking the location of one or many customers

into account. The location is usually provided through a location server, as presented earlier. LBS are usually divided into pull- and push-services. In the former, the localization is performed on demand when the customer requests the service, as in a pharmacy-finder scenario. The latter are activated once and perform localizations in the background to provide some kind of continuous service. So, for example, the customer can be notified by SMS in case he or she enters some region of interest. As location information is generally seen as highly privacy relevant, access to it can be restricted (see Privacy Management). However, there is an ongoing dialogue between data protection officers and emergency/police forces regarding the circumstances on which disclosure should be possible without customer authorization or consent.

- **Content Download** and **Media Service**: As the capacity of modern mobile transport channels is increasing continuously, it is possible to transmit all kinds of multimedia content over a wireless link. Available services range from Multimedia Messaging Service (MMS), over transmitting bounded content (pictures, sound files) to TV-Streaming over UMTS. These services usually identify the customer for billing purposes. Anonymous usage is thus not possible in this case.

3.2.2.3.2 Community services

- **Conference Calls**: This service gives a group of customers the possibility to perform a voice call with more than two involved parties. This kind of service can be implemented at different locations. A company can host a conference-bridge that accepts the incoming calls of conference participants and performs the authorization. Another possibility is MNO-operated conference calls that are provided directly by the telecommunication providers. Conference calls can be provided for business and, also, for leisure, e.g., in flirt-lines where each caller can talk to a group of unknown people through the phone. From a privacy point of view, these are similar to voice calls.
- **Instant Messaging** (**IM**): This technology originates from the Internet. A user can specify a buddy list (a list of acquaintances) for whom he or she receives so-called presence information, and with whom he can start a text based chat communication. The presence information is usually displayed in the list of buddies in the form of an icon that changes depending on the buddy state (online, away, busy, etc.). With the convergence of the Internet and initially circuit switched communication systems (e.g. GSM), these instant messaging systems are now also available on mobile phones. From a privacy perspective, most services are not optimal as all messages are sent without encryption and pass over a relay. However, some systems support end to end encryption. Protection against other customers is usually achieved only by accepting messages from and sending presence information to the customers on the buddy list.
- **Push-to-Talk** (**PTT**) or **Push-to-Talk over Cellular** (**PoC**) is a community service where walky-talky style messages can be sent to defined by activating a special key on the phone. This message will then be propagated to all logged in customers. The content of the message can also be stored if a group member is not available at the time. It will be sent to him or her on log in. Privacy is protected through a group metaphor: only members of a group can participate in the group communication.

- **MyFaves** is a service of T-Mobile that provides easy access to and management of five phone numbers. Calls to these numbers have a special, lower, rate. The special contacts are displayed with an icon on the main display of the phone. Changes in the special contact information can simply be transmitted to the peers.
- **Web2.0** (**Flickr**, **Wikipedia**, **MySpace**): Participative web sites are commonly known as Web 2.0. They present a new trend in Web pages, where the users are those who provide the content of the page. The types of services range from centrally managed software projects as in Sourceforge, over online auction applications as eBay, to public video hosting as in YouTube. Modern mobile communication devices with high bandwidth Internet connections and sufficient computing power to watch movie clips have made these services available pervasively. The privacy threat stemming from this kind of application is potentially huge, as users often partially publish highly personal information (e.g., hosting of a personal photo album in "Kodak Gallery") with only restricted control over who gets access to this data. In most systems in which some kind of access control exists, this is based on invitations. These are usually presented as a link that can later be found in the invitee's browser history. However, this is not that much of a problem in mobile environments, where the device is usually not shared between customers.

3.2.2.4 Conclusion

It can be seen that services in a mobile environment consist of a large variety of technologies. The used protocols are now rapidly shifting from circuit switched to package switched communication. Most of these technologies have some kind of privacy feature. However, they are usually not tuned to each other. Ironically, in the "old" circuit switched world, the handling of privacy relevant information is much easier due to the relatively closed environment (but with the drawback that few companies have full control over all subsystems).

3.3 Business aspects of trust, IdM and privacy

The collection, processing and exchange of information are a key economical success factor on the Internet. The question who has access to what kind of information is therefore becoming more and more important. This is especially the case in environments that contain large amounts of personal information. Online and mobile communities represent such an environment.

Trust, privacy and identity management (IdM) address the question of information access. Thus, when talking about the influence of trust, privacy and IdM on the frameworks of online and mobile communities, different perspectives have to be taken into account. Besides the technological and design perspective, legal, social and economical or business aspects are also of relevance.

The following sections are intended to describe a business perspective on trust, privacy and IdM with special regard to communities. They first start with an overview of the context of business aspects. Then, general aspects with respect to online services (**Error! Reference source not found.**), and more detailed aspects regarding mobile communities are discussed (**Error! Reference source not found.**). This discussion then finally leads to an examination of specific aspects of marketing in such communities (**Error! Reference source not found.**).

3.3.1 Context of business aspects

Trust, privacy and IdM are broad expressions that are widely used and which comprise of different, and also interdependent, aspects. For instance, trust may relate to trust between community members, but it may also mean the trust of a community member in the community provider. In the latter case, the willingness to disclose personal data, which is an aspect of privacy, depends significantly on the degree of trust a user has in a service provider.

Likewise, trust, privacy and IdM affect various aspects of information systems. These are aspects that have an impact on the various elements (e.g. technology, design, etc.) of information systems, software applications and services. An IdM system, for example, is at first a technical mechanism that allows a user to handle personal information. Such a system has to be compliant with legal frameworks and constraints (e.g., regulations on how information may be processed). It furthermore has impacts on the design of an application (e.g., which specific features implement the functionalities of the IdM system), and it thereby also influences how a service might be advertised and sold (i.e., IdM related features may represent an added value which can be specifically advertised as a service or product feature).

3.3.2 General business aspects

From a business perspective, mobile Internet access in general allows the ubiquitous provision of various kinds of existing (online) services (e.g., payment services,[5] advertising,[6] searching and communities[7]). Moreover, mobile devices are location independent, in the sense that they can be used at different locations, and that their location can change during the time of usage, instead of being associated with just one specific location (like, e.g., a personal computer usually is). Such locations have to fulfil certain requirements (e.g., network access). With the location independence, associated with mobile devices, new services and features have emerged, such as context based services (e.g., weather information depending on the current location of a user).

When designing, deploying and providing such services, different requirements regarding trust, privacy and IdM have to be considered. They can at first be regarded as requirements of many such services. Thus, for example, a payment service is required to ensure the privacy of user data, whereas community services such as a personal profile or content sharing have some kind of trust and IdM requirements regarding the amount of personal information they deal with. These requirements can be fulfilled by particular features of the respective service. For example, a payment service could use encryption mechanisms to ensure the privacy of users and their data. If we consider a service as something that is provided by a service provider to a service requestor (using information technologies) who requests and uses the service (as a “user”), this provision may also include any kind of financing model (e.g., service fee, advertising). For example, users would usually require a payment service to ensure a certain degree of privacy and protection of their data (e.g. bank account). Such a requirement might be taken into consideration by users when they decide whether to use (and possibly pay for) the service. This makes the trust privacy and IdM aspects a part of a service and outlines their economic influence.

[5] E.g., worldpay, Paynova.
[6] E.g., Google Ads, wunderloop.com, admob.
[7] E.g., Loopt, Facebook Mobile, yahoo one connect, youtube mobile.

The PICOS project receives research funding from the Community’s Seventh Framework Programme.

However, the value of these aspects is hard to quantify. Trust and privacy do not provide such an obvious benefit for users as other features do. In other words, referring to the aforementioned example, the usage of an encryption mechanism in a payment service to ensure privacy and to protect user data would normally only be recognized by users if something goes wrong and actual harm to the users takes place. In contrast, if the payment service supports different ways of paying (e.g. different credit cards, paying per bank account, etc.), this benefit – that a user can directly choose between these options – is more obvious. The situation regarding Identity Management and trust is similar. Trust is especially something implicit that may be supported by features of a service (e.g. the possibility of rating other users as it is used on eBay), but which is not a feature itself. IdM might also rather just be supported by a service than a feature whose benefit is obvious to a user. Hence, aspects like privacy and IdM are not as attractive in a marketing sense, as other product features and attributes are, because their benefits are not as obvious.

Nevertheless from a business perspective, Privacy and IdM have to be seriously considered, due to the fact that personal user data are a valuable resource, and that a misuse of these data can lead to serious consequences not only for individual or whole groups of users (e.g. financial losses or loss of reputation, if private information is disclosed), but also for those service providers who are not able to avoid such a misuse. From this point of view, technologies which enhance Privacy and IdM – so-called Privacy enhancing technologies (PET) – also provide a benefit because they may avoid the consequences of data misuse (Ribbers, 2008).

Trust in the context of mobile services can especially be found with regard to the relation between a service provider and a service user (service customer). Like in usual customer relationships in the real world, trust is an important part of this relationship (McKnight and Chervany 2002). Further, trust can be seen as a characteristic of the customer relationship and as a competitive advantage. This is because trust is build over time, and a trusted relationship between customer and service provider is something that cannot be offered easily by another service provider. Therefore, trust can help to build customer loyalty in order to prevent customers from changing a service provider.

In online communities and especially social networks, personal user data and the users' identity is of even more relevance, as it is an essential element of the nature of social networks to share and exchange such data with other users. Personal data is not only provided to a service provider in order to use a specific service, but it is also provided to other users (Gross and Acquisti, 2005). The benefit that is simply obtained by using a service (e.g. weather information) is obtained in communities by the exchange of information. Such information can comprise of content such as photos and videos (e.g. flickr, youtube), but also personal user information (e.g. Facebook, myspace). Personal information is, additionally, of interest for third parties, like companies, in for personalised advertisements or similar activities. Considering this and the resulting increase in the importance of personal information in comparison to other online services, the importance of trust, privacy and IdM is increasing as well.

3.3.3 Business aspects of mobile communities

The outlined economical relevance of trust, privacy and IdM becomes more important in a mobile usage context. This is firstly because many online services are now also provided and used in a mobile environment. At the same time, however, the personal data which they use (such as credit card information, information about a users' personality, interests, behaviour, etc.), are enriched by information about the context of a user (e.g., his or her location). Such information often serves as a

The PICOS project receives research funding from the Community's Seventh Framework Programme.

foundation for context based adaptations of services, for example, for mobile marketing purposes (Albers and Kahl, 2008) or other new services which make use of such context information.

As one kind of service, communities reflect this ongoing trend by also becoming more mobile (Fremuth and Tasch, 2005). Mobile Communities represent an aggregated service, composed of various smaller (mobile) services. For example, a community could make use of an advertising service like Google Ads to place advertisements. Another example could be the use of a positioning service to identify the position of single community members, in order to display them on a map. Such a map is provided by loopt[8] and plazes.[9] These examples show how mobility has extended the spatial freedom of users, which leads to larger user flexibility, regarding the access to digital information and services. Coevally, information about the current context (location, time, used device, etc.) becomes more important for the providers of such services, as context information may be used to improve existing services and to enable the introduction of new ones.

The relevance of mobility for communities is underlined by the amount of personal user data that is provided, stored, processed and exchanged, and that may be used in any kind of services. From a business perspective, the combination of personal information that is available in communities and information about a users' current context creates a large potential for personalised services, marketing and advertising activities.

However, a user may not always be aware that his or her personal and contextual data is used, or how it is used or distributed, although he or she should have control over it (Royer, 2007). Following this, and due to the information availability in mobile communities and their possible usage options from a business perspective, aspects of trust, privacy and IdM have to be considered. This is particularly the case because communities need business models to finance themselves, and their access to large quantities of information about users – including aspects about their personality, interests and relationships – offers extensive marketing possibilities for them (Huberman et al., 1999). These diverging interests of users, advertisers and community providers are discussed in more detail in the following subsection.

3.3.4 Marketing and advertising in mobile communities

Online communities and social networks provide a platform for huge masses of people, and usually contain detailed data about their members. The amount of personal data that is provided, stored and shared between users in communities makes them attractive for various kinds of marketing activities. For instance, Microsoft bought 1.6 percent of the shares of Facebook in 2008, for about US$ 240 million, to improve their position in the online advertising market, currently dominated by Google. Facebook is one of the platforms with the most members, currently more than 120 million, besides MySpace (245 million), hi5 (80 million) and friendster (80 million).

One of the main reasons behind the interest of companies such as Microsoft is not only the huge group of people who are organised in communities, but also the trend that advertising and other marketing efforts on the Internet have became subject to personalization over the last few years. For example, personal recommendations on Amazon.com could be mentioned here, as well as personalized advertisements on Google, which are based on a user's search term. Such personalizations, which

[8] www.loopt.com.
[9] www.plazes.com.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

represent forms of one-to-one marketing, have the potential to be more appropriate to the user's actual interests and needs (Koch and Schubert 2002). They could thereby make a user feel more special compared to traditional, target group based marketing. However, platforms such as Facebook or friendster contain a lot more information about their individual users than what a user bought or what he or she was searching for. Therefore, from an advertiser's point of view, communities represent an ideal place for personalized marketing and targeted advertising.

For the communities themselves, marketing and advertising means a possibility to generate revenues and to finance their services. This certainly holds for communities organized by commercial organisations, e.g. Facebook. It also holds for many communities organized by volunteers, and also has a long tradition in the "real" world; e.g., newsletters of sports clubs were and often are made possible by the advertisements of shops or other services that may appeal to the members of the club, or whose owners and operators are merely members of the club.

However, if such marketing activities become personalized, based on user data, this implies that users are willing to share their personal information and to let it be used for marketing purposes. That this is often not the case has been shown by several marketing related activities by online communities in the recent past. For example, Facebook[10] and the German community StudiVZ wanted to enable advertisements based on personal user data, which in both cases lead to heavy protests by their users. After these protests, the activities were either cancelled (Facebook) or at least attenuated (StudiVZ). Furthermore, to restrict the quantity and quality of information that is accessible by other users, a number of communities started to integrate different privacy settings (e.g. Facebook, LinkedIn, MySpace). These communities now allow users, in a more or less detailed way, to specify which information can be seen by whom. Such mechanisms represent a form of identity management, which is used to improve the protection of personal user data.

The aspect of privacy in communities becomes even more relevant, for advertisers as well as for users, when these communities make use of context information that is available in a mobile usage context. In particular, location information may be used in mobile communities for location based community services, as is the case, e.g., with loopt. Location information means further opportunities for advertisers, because advertisements and other marketing activities could be presented to a user not only based on his or her user profile, but also based on current location. On the other hand, the fact that, besides the characteristics of a user, information about his or her location is also available makes the question of who has access to this information also more important.

The area of conflict between the need for privacy of individual community users on one hand, and the opportunities of personalized marketing on the other, demonstrates the relevance of privacy issues for communities, especially in a mobile usage context. In fact, a balance between all involved parties (User, Advertisers and Community Provider) has to be found, as all of their interests matter to a certain degree. That does not necessarily mean that it is a fixed balance between privacy and marketing. The mentioned mechanisms of identity management, recently integrated by various communities, give users the opportunity to specify a particular degree of privacy, and show that the importance of privacy for the users is recognized.

Against this background, other forms of marketing activities could be of interest for communities as well. Viral Marketing is based on the assumption that it is not only important if someone buys a

[10] http://www.guardian.co.uk/technology/blog/2007/nov/07/facebookssocialadvertisings.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

product or a service, but also whether he or she influences others. Viral marketing activities are already used in various forms. For example, Apple has established an "Apple Group" on Facebook,[11] which is used to get and share the latest information about Apple products. Other examples are music labels and music artists on MySpace. The customers of their music can directly add them as friends and integrate their songs into their own profiles. But in such forms of marketing, privacy concerns have to be also considered and new challenges have to be managed; for instance, the question of how long information provided by users in product or company related groups should be stored within communities, and who has access to it.

3.3.5 Conclusion

To reveal the relationship between trust, privacy and IdM, and business aspects of mobile communities, the previous sections first described the context of such business aspects. It was shown that trust, privacy and IdM can be regarded from different perspectives that are related to each other and that have an influence on these aspects. From the business perspective, the discussion of trust, privacy and IdM on a general level showed that they affect business aspects of online services, even though their benefit is not clearly measurable. In any case, they have to be taken into account from the perspective of service providers. This is especially so now given that services are using an increasing amount of personal user data combined with information about their context, like in mobile communities. Finally, as the main focus of this chapter, trust, privacy and IdM were discussed in the context of mobile communities and the emerging opportunities for marketing and advertising in such communities.

3.4 HCI and security, privacy, trust and IdM issues

Issues of human computer interaction and security are frequently influencing each other. Consider, for example, the case of a safe that is locked with numerous different locks and placed in the basement of a building. This might be a very secure way of storing valuables, but it is also very inconvenient and cumbersome to use if you want to access them and wear, e.g., your jewellery on a regular basis.

This example clearly illustrates that, frequently, there is a tension between security requirements and usability requirements. Typically, the user just wants to log on to the system and does not want to be bothered with any authentication issues, security requests, etc., but rather just wants to get his or her work done. The people in charge of the security of a system, on the other hand, want tight security solutions, e.g., passwords of arbitrary design (and therefore hard to remember) with a minimum of 20 characters.

This tension between security and usability needs has important consequences for the actual security of a system (as opposed to the theoretical security). Technically, it is easily feasible to require and force people to use the most theoretically secure measures, but if one wants to achieve actual security, the capabilities and habits of the people using the systems on a day-to-day basis need to be considered.

If these users' needs are not considered, people will find ways around the intended security system and exhibit behaviours very much not wanted due to their unsecure nature. For example, it is very common

[11] http://www.facebook.com/pages/Apple-Students/11147074409.

for users to write down passwords, share passwords with other users or choose passwords that are easily memorised – practices not very much liked by people concerned with security issues. Sasse et al. addressed the motivation of people for such behaviour and identified seven main issues that lead to undesirable password behaviour (Sasse et al., 2001):

- Identity issues: People who exhibit good password behaviour are often described as 'paranoid', 'pedantic' or 'the kind of person who doesn't trust anybody'.
- Social issues: Sharing your password is considered by many users to be a sign of trust in their colleagues.
- 'Nobody will target me': Most users think the data stored on their system is not important enough to become the target of a hacker or industrial spy.
- 'They could not do much damage anyway': Most users do not think that somebody getting into their account could cause any serious harm to them or their organisation.
- Informal work procedures: Current password mechanisms and regulations often clash with formal or informal work procedures.
- Accountability: Most users are aware that their behaviour does not fully comply with security regulations. However, they do not expect to be made accountable because they regard the regulations as 'unrealistic', and their behaviour as 'common practice'.
- Double-binds: If a computer system has strong security mechanisms, it is more likely to come under attack from hackers who want to prove themselves, and who will, in the end, find a way to get in.

The results of this study clearly show that human factors need to be addressed to achieve systems that are actually, and not only theoretically, secure. To address this problem, Saltzer and Schroeder introduced the principle of psychological acceptability (Saltzer and Schroeder, 1975):

"It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the users' mental image of this protection goal matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors".

Similarly, Whitten and Tygar (Whitten and Tygar, 1999) state that user should:

- be reliably made aware of the security tasks they need to perform;
- be able to figure out how to successfully perform these tasks;
- not make dangerous errors; and
- be sufficiently comfortable with the interface to continue using it.

If these principles are not met, severe consequences following users insecure behaviour have to be expected.

To design successful (usable and secure) interfaces in this context, some unique aspects of HCI and usability in the domain of security and privacy, need to be understood.

Security and privacy are secondary goals
Human behaviour is essentially goal driven. To achieve successful systems it therefore essential to design systems in a way that support the user in his or her tasks in an effective and efficient way. Task are differentiated as either production tasks or supporting tasks.

Production tasks are those that are required to achieve a desired result. Supporting tasks enable production tasks to be carried out in the long run, but are not necessarily required to achieve the immediate goal.

Security and privacy are typically supporting tasks and not the users' main goals. If the supporting task gets in the way of the main task, chances are that users will find a way around it to achieve their main goal.

Diverse users
Another challenge for the design of interfaces in the privacy and security domain is the diversity of users. Security applications have historically been designed with a highly trained and specialised user in mind. However, because of the broadening application of software for (critical) business processes, more and more users without a technological background have to use these systems. With the PICOS objectives in mind, we thus have to deal with even broader and less-defined user groups.

Complexity
Security and privacy solutions typically have to function in a very complex environment and consider many different factors. But complexity is also one of the big enemies of usability. In their classic study, "Why Johnny Can't Encrypt", Whitten and Tygar have shown how difficult it can be to communicate complex concepts such as PGP successfully to users (Whitten and Tygar, 1999).

Perception of risks
In a recent article, Bruce Schneier focuses on the user's perception of risks (Schneier, 2008). The prospect theory states that humans – according to survival theory – tend to accept risks for large losses rather than the sure risk for a small loss. This also explains why users do not want to pay for security – the buyers prefer to take the chance of a loss than paying for security. Therefore, the sellers of security software can either increase the user's fear, or include security software in more general software products.

3.4.1 Example studies with special relevance for PICOS

3.4.1.1 Dhamija & Dusseault 2008
In their work about identity management, Dhamija and Dusseault have discovered what they call the seven flaws of identity management (Dhamija and Dusseault, 2008). According to them, the complex combination of privacy, security and identity management is the cause of vast challenges for usability. It is obligatory for identity management systems to obtain the trust of the users as well as the trust of

the relying parties. A truly user-centred approach is needed to overcome the seven flaws of identity management:

Identity management is not a goal in itself: Users do not focus on identity management; for them this is secondary and they are not willing to invest time in this area.

Users follow the path of least resistance: If a system is too complex, the users tend to take shortcuts and avoid security measures. The easier to use a system is, the more appreciated it will be.

Cognitive scalability is as important as technical scalability: Each user has on average about 25 accounts with passwords. Because of the enormous cognitive load that is required for remembering these passwords, users tend to use one password for several accounts.

User consent could lead to maximum information disclosure: Users are used to warning messages and tend to click on them without really reading or understanding them. Users might thus assume that this is the most convenient way to reach their goal.

We need mutual authentication (not just user authentication): Phishing attacks illustrate the necessity of mutual authentication. The user does not only have to authenticate the relying party, but also the identity provider.

Relying parties want to control the customer experience: The combination of relying parties and identity providers introduces additional complexity for the users who now have to handle two bodies that might even require the user to visit another website.

Trust must be earned (and is hard for users to evaluate): The decision of trust involves risk management, which is very hard to do in the online world.

3.4.1.2 Bratus et al. 2008

The difference in online and offline security behaviour is one of the basic topics of Bratus et al., 2008. They investigate why people that are perfectly capable of making security decisions in real life fail to do so in the online world. Therefore, they propose interface design principles for designers in order to facilitate the user's trust decisions. According to them, current interfaces mislead users in their decisions because they train the user away from applying real-world trust functionalities. Therefore, the users do not know the possible risks and implications. This applies, for example, to the paper-icons frequently used in current applications. The user does not suspect active data, such as macros behind this information, and is therefore completely unsuspicious. Another example is trust mechanisms. In real life, people have different mechanisms to distinguish whether one is trustworthy or not. In the online world, these mechanisms do not apply and the users have to rely on different aspects such as digital identities. This also applies to phishing attacks. Answering these problems, the authors propose an interface design whose operations distinguish between the different implications and also the required user interactions. According to Bratus et al., future environments could be divided into private, work and public zones, where the user can adapt the already known offline security mechanisms to the online interactions.

4 Regulatory framework on privacy and IdM

4.1 Introduction

The principle aim of PICOS is to research, develop, build, trial and evaluate an open, privacy-respecting, trust-enabling identity management platform that supports the provision of community services by mobile communication service providers. The successful functionality of the PICOS platform will only be achieved when the proposed solutions will fit into the existing legal framework. More specifically, the processing of the information about the users (or other entities) for the ends of PICOS will respect the rules contained in the European legal framework on data protection. Furthermore, specific obligations that relate to the processing of personal data in the field of electronic communications will also be respected, as well as the obligations regarding the retention of specific categories of data. The European legal framework for data protection and privacy will be carefully examined from the very early stages of the project in order to achieve the development of a privacy-compliant identity management platform. Besides the relevant legal framework on privacy and data protection, it is crucial to take into account some other relevant legislation that is of great importance for the PICOS Platform. In particular, laws and regulations concerning the provision of Information Society Services – focusing mainly on the provisions on liability – will be analysed in this chapter.

This chapter provides a general overview of the relevant legal and regulatory framework that will be respected during the development of a fully compliant PICOS platform. More specifically, the following directives will be examined: Data Protection Directive (1995/46/EC), ePrivacy Directive (2002/58/EC), Data Retention Directive (2006/24/EC) and some provisions of the eCommerce Directive (2000/31/EC). Various principles analysed here are translated into specific legal requirements and are included in the PICOS D2.4 Requirements Deliverable. In that deliverable, more requirements tackling specific legal issues related to online and mobile communities, such as anonymity, IP addresses and targeted advertising are analysed.

4.2 Data Protection Directive (1995/46/EC)

The Data Protection Directive[12] aims to lay down specific rights of the individual on his personal data, while ensuring that such data can move freely within the single market created between the Member States of the European Union. In this subchapter, we are going to give a general overview of the Data Protection Directive, and focus on the principles of legitimate processing of personal data that will be respected in the development phase of an Identity Management platform, such as PICOS.

4.2.1 Introductory terms for data protection

Article 2(a) of the Data Protection Directive (DPD) defines 'personal data' as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental economic, cultural or social identity". Although the Data Protection Directive tried to harmonise the processing of personal data

[12] Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, L 281, p. 31-50 (23.11.1995).

The PICOS project receives research funding from the Community's Seventh Framework Programme.

with the free movement of such data, there are still many differences between the Member States with regard to the term 'personal data', and especially when it refers to an 'identified of identifiable natural person'. Moreover, recital 26 DPD reads that, in deciding whether data can be used to identify a particular person, "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Moreover, the term 'personal data' should include all data about a person (including economic, professional, etc. data), and not only data about the person's personal life (Dammann and Simitis, 1997, p.109). This breadth of the conception of personal data means that data is usually presumed to be 'personal', unless it can be clearly shown that it would be impossible to tie the data to an identifiable person (that is, unless the data is truly anonymous) (Kuner, 2008, p.51).

Article 8 of the DPD describes special categories of data, i.e., "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life", commonly known as sensitive data. The processing of the aforementioned data is prohibited, unless one of the specific grounds described in the same Article is fulfilled.

According to Article 2 (b) of the DPD, "data processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". It follows that the definition of processing is extraordinarily broad, which means that it is difficult to conceive any operation performed on personal data which would not be covered by it. It is important to note that mere storage of personal data by the providers of publicly available electronic communications services or of a public communications network constitutes 'data processing', so that simply storing data on a server or other medium is deemed to be processing, even if nothing else is being done with it.

In the context of processing of personal data, three distinctive categories of parties are recognised:

- Data subject: the individual who is the subject of the personal data.
- Data controller: a person (natural or legal) who alone or jointly with others "determines the purposes and means of the processing of personal data" (Art. 2(d) DPD).
- Data processor: a third party who simply processes personal data on behalf of the data controller without controlling the contents or use of the data (Art. 2(e) DPD).

The classification of a natural/legal person as "data controller" or "data processor" is of great importance, for several issues, such as who will carry the obligations appointed to the 'data controller' by the Data Protection Directive, and who is to define the details of the data processing. As a rule of thumb, it can be said that the data controller is liable for violations of the Data Protection legislation, while the responsibility of the data processor is reduced (Kuner, 2003, p. 62).

Under the regime established by the Data Protection Directive, a key concept is that of the 'data subject's consent'. If the data controller obtains the data subject's consent, then he or she is broadly free to process the personal data. The Directive states that a 'data subjects' consent' must be freely given, specific and informed (Art. 2 (h) DPD).

4.2.2 Basic principles in data processing

The European legal framework on data protection contains some basic principles for the processing of personal data. These principles are intended to be good practices that data controllers should comply with in order to protect the data they hold, reflecting both their interests and those of the data subjects (Walden, 2003, p. 432). The first of these principles requires fair and lawful processing (Art. 6(a) DPD). In determining whether any processing of personal data is 'fair', particular regard must be paid to the method by which data were obtained. Under the second principle, data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes (Art. 6(b) DPD). This principle thus has two components: (1) the data controller must specifically inform the data subject of the purposes for which data has been collected; and (2) once data has been properly collected, it must not be used for further purposes incompatible with the original purposes. The third principle requires a data controller to hold only personal data that is "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Art. 6(dc) DPD). Data controllers are therefore obliged to store only a bare minimum of data that will suffice for the running of their services. In the same context, the design and technical devices of the data processing systems must be oriented towards collecting, processing and using either no personal data or as little as possible ('data avoidance') (Holznagel and Sonntag, 2003).

The fourth principle stipulates that all personal data "shall be accurate and, where necessary, kept up to date" (Art. 6(d) DPD). The specific legislative provision creates an obligation for the data controllers to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, are either erased or rectified. In practice, a data subject is likely to complain of a breach of this principle in cases where there has been some detriment to the individual as the result of the information being incorrect. It is therefore advised that the data controllers set up a mechanism whereby the data subjects are able to update their personal data or notify the data controller about the inaccuracies of the present information. This mechanism could be set up either within the network platform (by using the network's interface), or outside the platform (e.g. by the use of a 'hotline'). The fifth principle reads that personal data must not be kept for longer than what is necessary for the purposes for which this data were collected (Art. 6(e) DPD). This implies that data should be destroyed or rendered anonymous when the specified purpose for which they were collected has been achieved. The sixth principle requires processing to be carried out in accordance with the rights of the data subjects. More precisely, Article 12 of the DPD grants data subjects the right to obtain certain basic information from the data controller about the processing of their personal data. While Article 12 explicitly requires only that exercise of the rights contained in subparagraph (a)[13] be "without constraint at reasonable intervals and without excessive delay or expense", it is generally accepted that these conditions apply to the exercise of the rights contained in

[13] According to article 12 (a) of the Data Protection Directive, every data subject has the right to obtain from the controller "[…] i) confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of processing, the categories of data concerned, and the recipients to whom the data are disclosed, ii) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, iii) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in article 15 (1)".

The PICOS project receives research funding from the Community's Seventh Framework Programme.

sections subparagraphs (b)[14] and (c)[15] as well (Dammann and Simitis, 1997), i.e. the right to rectify, erase or block the data, as well as the right of notification to third parties of any rectification, erasure of blocking of the data.[16]

The seventh principle addresses the issue of data security: it requires data controllers to take 'appropriate technical and organizational measures' (Art. 17.1 DPD) against unauthorized or unlawful processing, and accidental loss, destruction or damage to the data. To the extent that this principle covers the security requirements and robustness of the network itself, this principle overlaps with the security and confidentiality requirements laid down in Articles 4 and 5 of the e-Privacy Directive. Taken as a whole, this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that the data controllers must consider the state of technological development and the cost of the implementation of any security measures. Finally, the last principle is the notification to the supervisory authority in order to ensure the supervision of the data processing. The data controller must notify (Art. 18,19 DPD) the supervisory authority about the processing, an mention among other matters the name of the controller, the purpose of the processing, the categories of data subjects, the categories of data processed, as well as the recipients to whom the data might be disclosed.

The Data Protection Directive also contains a liability provision. Pursuant to Article 23, any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national data protection legislation is entitled to compensation from the controller for the damage suffered. The controller may be exempted from liability, in whole or in part, if he or she proves that he or she is not responsible for the event giving rise to the damage.

4.3 ePrivacy Directive (2002/58/EC)

The ePrivacy Directive[17] translates the data protection principles of the general Data Protection Directive into specific rules for the electronic communications sector, regardless of the medium used. This directive regulates issues such as the confidentiality of communications, the status of traffic and location data, itemised billing, and unsolicited communications and, therefore, it should be taken into consideration, along with the relevant working documents and opinions of the Data Protection Working Party of Article 29 of the Data Protection Directive.

In the general frame of mobile communities, the term communication is very important. "Communication means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic

[14] "[…] the data subject has the right to obtain from the controller […] as appropriate the rectification, erasure or blocking of the data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".
[15] "[…] the data subject has the right to obtain from the controller […] notification to the third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate".
[16] The rights of the data subject are presented more extensively in the PICOS D2.4 Requirements document.
[17] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), Official Journal L 201, pp. 37-47 (12.07.2002).

The PICOS project receives research funding from the Community's Seventh Framework Programme.

communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information" (Art. 2 (d) ePrivacy Directive).

Article 4 of the ePrivacy Directive stipulates that the providers of publicly available electronic communications services must take appropriate technical and organizational measures to safeguard the security of their services, if necessary in conjunction with the providers of the public communications networks with respect to network security. Having regard to the state-of-the-art and the cost of their implementation, these measures have to ensure a level of security appropriate to the risk presented. This provision extends the security obligation that was already included in the general data protection directive of 1995. Security is thus no longer only legally required for the processing of personal data, but also for electronic communications in the framework of publicly available services on public networks.

The ePrivacy Directive further aims to protect the confidentiality of communications. Member States must, through national legislation, ensure the confidentiality of communications (and the relevant traffic data) by means of a public communications network and publicly available electronic communication services. In particular, listening, tapping, storage and other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, and except when legally authorized to do so, are prohibited. However, the Directive provides for an important exception to the principle: legal authorization for the monitoring of electronic communications is possible when it constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the communications system.[18]

According to Article 2(b) of the ePrivacy Directive, traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Such data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Traffic data that is needed for billing and interconnection payments may be processed until the end of the period during which the bill may be lawfully challenged or payment pursued (Art. 6(2) ePrivacy Directive). The Working Party 29 stipulated that this should ordinarily involve a routine storage period for billing of of maximum 3-6 months, with the exception of particular cases of dispute where the data may be processed for a longer period.[19] Processing of traffic data is also allowed for the purposes of marketing electronic communications services or for the provision of value added services if the subscriber or user to whom the data relate has given consent (Art. 6(3) ePrivacy Directive). However, any natural/legal person that already has the e-mail addresses (traffic data)[20] of its customers may use them for direct marketing of its own similar products or services, without the consent of the customer. It suffices to say that the customer may withdraw his or her consent at any time. As it will be further analysed (Section 4.4), the

18Article 5(1) in conjunction with Article 15(1) of the Directive 2002/58/EC.

[19] Art. 29 Working Party, WP 69, Opinion 1/2003 on the storage of traffic data for billing purposes (29 January 2003) available online at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp69_en.pdf .

[20] Art. 29 Working Party, WP 37, Working document: Privacy on the Internet- An integrated EU Approach to On-line Data Protection. (21 November 2000) available online at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Data Retention Directive contains specific provisions regarding the retention of some types of traffic (and location) data for law enforcement purposes.

According to Article 2(c) of the ePrivacy Directive, location data means any data processed in an electronic communications network that indicates the geographic position of the terminal equipment of a user of a publicly available electronic communications service. The ePrivacy Directive does not make use of the term 'Location Based Services'. However, Article 2(g) of the Directive defines the term 'value added service' as "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof". Thus, we could say that a Location Based Service (LBS) is a value added service which processes location data other than traffic data for purposes other than what is necessary for the transmission of a communication or the billing thereof.

The ePrivacy Directive also introduces an Article on unsolicited communications. The aim of the regulation is to protect subscribers from intrusions to their privacy by any form of spam, which may impose a burden and/or cost on the recipient. Article 13(1) of the ePrivacy Directive stipulates that "the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent" (i.e., it stipulates an opt-in rule). Thus, the practice of sending electronic mail for the purposes of direct marketing, while disguising or concealing the identity of the sender on whose behalf the communication is made, or without giving a valid address to which the recipient may send a request that such communications cease, is prohibited. These provisions apply to subscribers who are natural persons, as explicitly mentioned in Article 13(5) of the ePrivacy Directive. However, Member States must ensure that the legitimate rights of legal persons are also sufficiently protected. Paragraph 2 of the same Article, though, provides an exception to this rule for existing customers. More specifically, it sets out an opt-out system: if a person or a company receives electronic mail contact details from it own customers (whether they be natural or legal persons) in the context of the sale of a product or a service, then direct marketing for its own similar products or services is allowed unless the customer explicitly opts out.

4.4 Data Retention Directive (2006/24/EC)

The Data Retention Directive[21] aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (Art. 1(1) DRD). The crimes for which the retained data are to be used are not explicitly mentioned in the Directive, and should therefore be defined by each Member upon the implementation of the Directive into national law. In order to prevent vastly diverging interpretations of the term 'serious crime' by the various Member States, the Council of the European Union urged the Member States to have due

[21] Directive 2006/24/EC of the European Parliament and of the Council 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, Official Journal L105, pp. 54–63 (15.03.2006).

regard to the crimes listed in Article 2(2) of the Framework Decision on the European Arrest Warrant,[22] and crimes involving telecommunications.[23]

The Directive aims at the harmonisation of the obligations of providers of publicly available communications services or public communication networks. The terms "electronic communications network" and "electronic communications service" are defined respectively in Article 2 (a) and (c) of the Framework Directive.[24] Moreover, the term public communications network is defined in Article 2(d) of the Framework Directive, and the term "provision of an electronic communications network" is defined in Article 2(m) of the same Directive. However, it is not always easy to determine whether a service qualifies as an electronic communications service and, consequently, whether the providers of such a service fall under the scope of application of the Data Retention Directive. Furthermore, the wording of the definitions can lead to a very broad interpretation of the terms, and thus to a very broad group of providers that qualify as "providers of public communications networks or services".

The Data Retention Directive includes a detailed list, in Article 5, of the categories of data to be retained, and the main categories read as follows:

a) Data necessary to trace and identify the source of a communication.

b) Data necessary to identify the destination of a communication.

c) Data necessary to identify the date, time and duration of a communication.

d) Data necessary to identify the type of communication.

e) Data necessary to identify users' communication equipment or what purports to be their equipment.

f) Data necessary to identify the location of mobile equipment.

The providers of publicly available electronic communications services or of public communications networks need to be very careful about the types of data they need to retain. The Data Retention Directive provides for retention periods of not less than six months and for a maximum of two years from the day of the communication. Article 15 (3) of the Directive allows the Member States to postpone the application of the Directive "to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail" until 36 months after the date of adoption of the Directive.

The Data Retention Directive does not provide for the reimbursement of the providers of publicly available electronic communication services or of a public communication network for demonstrated additional costs they incur in order to comply with obligations imposed on them as a consequence of the Data Retention Directive. However, the European Commission has recognised the opinion that "reimbursement by Member States of demonstrated additional costs incurred by undertakings for the sole purpose of complying with requirements imposed by national measures implementing this

[22] Council Framework Decision on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) (13.06.2002).
[23] Council of the European Union, Statements, Council doc. 5777/06 ADD 1 (10.02.2006) available at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf.
[24] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108 , pp. 33-50 (24 April 2002).

Directive for the purposes as set out in the Directive may be necessary".[25] Although such reimbursement could thus be granted as legitimate state aid, the Member States are not obliged by the Data Retention Directive to reimburse such costs.[26]

Security obligations that are imposed on the providers in the Data Retention Directive are very rigorous. To be retained, the data do not need to be of evidential quality, but they should be of the same quality and subject to the same security and protection as those data on the network. Moreover, the data shall be subject to appropriate technical and organizational measures to protect them against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure. Additionally, appropriate measures shall be taken in purpose of ensuring that they can be accessed solely by specially authorized personnel. Finally all other data shall be destroyed at the end of the period of retention; except, of course, those that have been accessed and preserved. The deletion of data should occur upon expiration of the retention period chosen in the national legislation. It is clear that the data should be stored in such a way that will allow their transmission upon request to the competent authorities, without delay.

4.5 eCommerce Directive (2000/31/EC), with focus on liability of Internet Service Providers

A crucial issue that will arise after the actual implementation of the PICOS platform is the issue of liability of the various actors that are involved in the PICOS identity management system. In principle, liability is a matter of national law. However, the European legal instruments contain certain provisions concerning, among others, liability of Internet Service Providers.

Liability of Internet Service Providers is regulated in Articles 12-14 of the eCommerce Directive.[27] The Directive takes a horizontal approach to liability, i.e. it concerns liability for all types of illegal activities initiated by third parties on-line (e.g. copyright piracy, unfair competition practices, misleading advertising, etc.). It establishes a number of limitations on the liability, which are based on the specific types of activities undertaken by operators, as opposed to different categories of operators.

The providers do not have a general obligation to monitor the information that is being transmitted or stored (Art. 15 eCommerce Directive). They also have no obligation to actively seek facts or circumstances indicating illegal activity. This means that no cyber-patrolling is required from the service providers. However, Member States may impose on information society service providers the obligation to promptly inform public authorities of allegedly illegal activities undertaken by recipients of their services. Furthermore, the limitation of liability for intermediary service providers regarding the transmitted information does not affect the possibility of injunctions of different kinds, such as

[25] Council of Europe, Statements, Council doc. 5777/06 ADD 1 (10 February 2006) available online at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf.

[26] Problems have already arisen in Czech Republic, where the police authorities don't reimburse the telecommunications companies within a small period of time, causing huge financial problems especially to SMEs. For more information see http://www.edri.org/edrigram/number4.3/czechdataretention (accessed 16 February 2006).

[27] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), L178, 01-16 (17.07.2000).

The PICOS project receives research funding from the Community's Seventh Framework Programme.

orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information (Recital 45).

As already mentioned above, the eCommerce Directive distinguishes between levels of liability basing on the type of the service that is being provided. In the case of mere conduit, where the role of the provider is solely the passive transmission of the information, or provision of access to a communication network, the provider is not held liable if he or she does not initiate the transmission, does not select the receiver of the transmission and, additionally, does not select or modify the information contained in the transmission (Art. 12 eCommerce Directive). It is clarified that the abovementioned acts consist of automatic, intermediate and transient storage, which means that the information cannot be stored for longer than what is reasonably necessary for the transmission. Therefore, from the side of the provider of the service, there is neither knowledge nor control over the transmitted or stored information. Article 13 of the eCommerce Directive addresses the case of providers of a caching service. It exempts them from liability regarding copies that are stored only temporarily and, in the same way as in the case of mere conduit, in an automatic, intermediate and a transient way. “Hosting” activities are exempted from liability as long as the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances by which the illegal activity or information is made apparent. Upon obtaining knowledge or awareness, the hosting provider has to expeditiously remove or disable access to the information (Art. 14 eCommerce Directive).

4.6 Interim conclusions

The successful functionality of the PICOS platform will only be achieved when the proposed solutions fit into the existing legal framework. The description of the legal framework in this chapter, complemented with the specific requirements contained in PICOS Deliverable D2.4 “Requirements”, will assist the developers in creating a fully legally compliant platform. The processing of personal data in the PICOS platform needs to comply with the legal principles contained in the Data Protection Directive and the more specific provisions of the ePrivacy Directive. The obligations of the parties involved in the processing of data within PICOS will be clarified in detail, based on the relevant legal documents.

5 PICOS Vision and mission statement

With European citizens increasingly demanding community-related services and subscribing to a greater number of these communities, inter-disciplinary solutions for identity, trust and privacy management will be increasingly seen as a cornerstone for the success of online communities, and especially in mobile-based usage contexts. PICOS specifically addresses these types of contexts, and addresses a number of privacy, identity and trust-related requirements of online mobile communities. The spread of mobile cellular technology to consumer devices and the availability of diverse location-based services and technologies, combined with increasingly powerful methods of pervasive computing, are enabling ubiquitous interaction with all types of online communities for professional and non-professional users alike. Handheld devices are no longer just about personal digital assistants (PDAs) or cell phones; they are no longer only used to keep calendars or receive e-mail, but also to access favourite online communities and store sensitive information. Increasing capabilities make handheld devices extensions of the desktop computer, suitable for all manner of professional and

leisure applications within rich community contexts. With increased processing power, storage, and both local and wide area connectivity, these devices are providing new means of accessing and using community-related services with increased convenience for different types of users. Users also now generally expect to be able to use their preferred devices and applications to boost their communications, productivity, connectivity and/or leisure activities in different contexts of sophisticated real-time interactions, including information sharing and different forms of collaboration, with device independence and the rich integration of media (text, voice, video and others). Understanding the intended uses of mobile devices and the environment in which they will function (i.e. online community interactions) will be of paramount importance in the PICOS approach.

Within PICOS, the latest technologies in the mobile context will be evaluated in order to enhance customer privacy in community services. Specific requirements for the PICOS concepts and architecture, derived from available technologies and from the specific point of view of a mobile operator serving a large number of customers world wide, will be elaborated, and a variety of open issues will be further addressed within the project life, such as new client technologies (Android, MIDP3.0), encrypted communication (SMS, voice), fine grained policies on bodies, managing of resource quality in privacy rules (e.g., accuracy of location data), new enabling services, identity management (single sign on), Hybrid LBS technologies (GPS, WLAN, Cellinfo), etc.

PICOS adopts a holistic approach to the central issues at stake, involving cross-disciplinary legal, social, cultural, organisational and economic/business aspects, by trying to provide a thorough and sound understanding of the complex interrelationships and dependencies involved and developing the appropriate technical expertise and solutions to support the communities' needs for privacy, IdM and trust. Provision of adequate procedural and organisational measures is critical for the security aspects involved, and these are also points of interest for PICOS, taking into account the range of potential organisations which may benefit from advances in the context of the project. Integration with the standard legacy IT infrastructure of existing communities and upgrading existing online networks to leverage them with PICOS specific technologies and approaches is another fundamental goal, as is the understanding of the structuring of social networks and how complex relationship dynamics influences not only different requirements and usage habits, but also the possible business models and opportunities for the different stakeholders involved.

PICOS also aims to analyse tradeoffs for seemingly irreconcilable dichotomies between privacy and other important societal values (i.e. privacy vs convenience/profitability/accountability/efficiency, etc.) towards leveraging community win-win scenarios which could simultaneously protect privacy, foster trust, securely manage identities and satisfy alleged antithetical interests.

Promoting a proper adoption of standards and conformity to established assurance and certification criteria is advisable in IT projects intended to support or build secure social networks and other types of online communities, in combination with well-focused, objective-aligned and consistent architectural, design and development activities reliant upon industry-respected best practices. Regulatory architectural patterns are emerging and could soon be advanced through standards bodies, which will establish a repository of compliance architectural patterns that address diverse compliance requirements. Continued advances, mapping, and relating contextual requirements to contextual solutions via frameworks will be necessary to advance privacy assurance infrastructure. Research is needed for (among others): the development of new approaches to embedding privacy and trust/reputation features early on in the software lifecycle within system architectures (which are increasingly adopting either the Service Oriented Architecture paradigm, or are at least service-based); balancing community-specific requirements and exhaustively analysing user interaction habits;

implementing usability guidelines; the comprehensive understanding of mobile environment ecosystems (including devices, operating systems, operators, network standards, software development kits and runtimes, server-side software, simulators, tools, etc.); and leveraging rich mobile application capabilities (including dimensions for interoperability, security, pervasiveness, application management, data persistence, platform integration support, etc.). PICOS can thus help the software industry to begin to develop safe and reliable services that protect personal information in online communities. In PICOS, frameworks, architectures, use-case models, and taxonomies represent an emerging set of tools necessary to convincingly address many competing forces affecting information privacy.

Disjointed forms of personal communications are likely to rapidly converge into unified applications that combine voice, instant messaging (IM), video, collaboration and presence, and thus provide richer community experiences. The result will improve organizational efficiency, and thus allow individuals or groups to communicate directly with each other through a common system, regardless of device or application. Converged client applications are taking advantage of the concept of presence, enabling users to discover in real-time not only the availability of other users, but even their current activity and also their availability for communication, including forms and methods at a given point in time (i.e., mobile phone, IM, audio phone, or desktop videoconference). However, privacy implications in each scenario need to be thoroughly assessed and addressed (i.e., how will the location information be used? who has access to location information? when is the information legally discoverable? how long will location information be stored?) with proper policies. Finally, mechanisms need to be provided for fine-grained control (i.e., determining if presence information refers to general location or a more specific or even exact location as made possible by GPS technology).

The realities of a hostile digital ecosystem are becoming visible to the public. Critical infrastructures that run the global digital ecosystem are vulnerable, and fail to protect valuable personal information. Multilateral security based on classical and new security technologies is needed to ensure a reliable and trustworthy context for the complex interactions between all stakeholders involved. New identity technologies are emerging to support online reputation systems. Blogs, social network, and digital passports are driving innovation and contributing to the emerging spectrum of relation-enabling infrastructure required for systems that function on a societal scale. Communities flourish or falter largely based on their ability to establish, maintain, and exit numerous relationships. The need to relate is an inherent societal requirement, and enabling people and resources to readily come together, relate for a time, and then disperse peacefully should be the primary goal of IdM and privacy-respecting systems; this will foster the conditions that allow cooperation to emerge and to reduce frictions and cognitive costs associated with relationships. PICOS can support such a philosophy by providing the necessary trust in well-designed supporting IT infrastructures for online communities.

The availability of secure hardware on both client and server side can be beneficial for improved security of the PICOS prototype, but the need for additional hardware might become a limitation. Usage of secure hardware can be limited to a small number places in the architecture (servers) for more expensive hardware like Hardware Security Modules (HSM), or relatively cheap smartcards can be used, ideally from already existing infrastructure like GSM SIM, loyalty cards or DRM enabled mobile devices.

Trusted Platform Modules (TPM) can be employed to provide secure storage of user keys, and passwords and platform authentication, via endorsement keys or other keys generated and stored in the TPM. Several uses of TPMs relevant for PICOS have already been proposed. The P2P reputation system with enhanced privacy utilizes endorsement keys to prevent false reputation claims, and remote

attestation and secure storage to protect reputation information on user platforms or when sent to other user's machine. Such a system can be used to maintain reputation in all three scenarios, especially for the gaming community, where mostly virtual-only contacts are assumed. Due to the currently rather immature but expanding state of TPM technology, the PICOS prototype will at least be given the possibility to employ additional protection mechanisms, butit should not rely exclusively on them, so as to provide better portability to non-TPM systems.

An open issue and potential PICOS objective is the creation of a multiplatform reputation system with the possibility for interconnection between different community platforms. Such a multiplatform system would enable the user to carry his or her own reputation status between different systems, and build persistent reputation traces without the necessity of rebuilding reputation from scratch in every new system. Secure hardware can be used to maintain the integrity of reputation values.

Portability of applications is necessary for particular PICOS usage scenarios and should therefore be of high priority, especially for broader scenarios, like the gaming community, with a high number of involved parties, where diverse execution platforms are to be expected. The inspected mobile platforms offer more or less the same functionality, but differ in execution speed and support given for cryptographic mechanisms. The PICOS architecture should provide some kind of platform abstraction with specific implementation for widespread platforms like JavaME, Windows Mobile and Symbian OS.

Many IdM related challenges have to do with membership to diversified communities. Claims-based products, next-generation federation solutions, and user-centric identity can all help alleviate IdM needs in cross-domain environments, and thus provide community stakeholders with a consistent and convenient identification experience that effectively allows them to manage their identity across different types of communities. IdM technology must become more sophisticated and distributed (i.e., user-centric, and more like an identity meta-system) to enable communities and individuals to collaborate efficiently over distributed systems with diversified user populations, i.e., IdM technology must enable people to establish community relationships with whomever they choose and with a reasonable assurance of safety and a tolerable level of convenience. But difficult problems remain for this new generation of technologies. The trust model for distributed systems is particularly difficult to work out. Issuing information cards and exchanging personal attributes only have meaning when parties can rely on the information these artefacts contain. Approaches where individuals have to fully manage their own identities pose a challenge in that they impose too much of a burden on individuals, many of whom are not identity-savvy. However, other approaches involving commercial consumer identity providers (IDPs) as businesses that act in the interests of individuals are still lacking clear business models. IdM vendors are adding technologies and integrating with partners that provide transaction monitoring, behavioural analysis, user risk analytics, log management, and activity monitoring functionality. These technologies can allow communities to verify the effectiveness of controls, identify risks, and monitor high-risk users and behaviours. Research and development into IdM technologies will be core to the strategies of PICOS.

Similarly, authentication is too closely aligned with centralized administrative models. The need to authenticate users across domain contexts is reaching a critical point. It seems that the industry desperately needs a workable, scalable approach to distributed authentication. User-centric approaches such as OpenID and information cards aspire to offer universal identification, but so far these technologies remain unproven in mainstream use. Conversely, role management and privilege management products cast a ray of hope on the complex issues of cross-domain authorization. Support for identity-themed standards that are well suited to SOA environments (i.e. information cards,

SAML, WS-Trust, and XACML) is a point to consider; however, none of these standards – or even the collection of them – constitutes a generic infrastructure service for, say, authentication, authorization, or role management, given the fact that the industry has not arrived at standards for basic identity services.

Identity and access management are fundamentals of community building, but they are only the beginning. Networks still lack many crucial features that promote the social cohesion necessary to ensure the longevity, and preserve the value, of networked resources. A new generation of technologies must emerge to foster pro-social behaviours by supporting natural processes of recognition, reciprocity, and community awareness. Most people typically do not consider the value of the information that they supply to a website when registering on a community. It is also extremely difficult to assess the potential for negative consequences that could arise as a result of the identity information they provide being leveraged for marketing (including for unsolicited e-mail messages); even sites with strong privacy policies can inadvertently expose customer information to resourceful attackers. Amid rising anxiety over identity theft and privacy invasion, communities often look to improving the accuracy of identification technology in the hope of improving security. But the impulse to rely on identification systems, though a natural response to such social dilemmas, also substantially increases societal risks, often without materially improving security. Identity systems are a means of establishing social order and regulating the use of shared resources. New technologies must support natural processes of recognition, community awareness, and reciprocity that promote pro-social behaviours. Understanding these social aspects and coupling them with regulatory and technological approaches will also be central to the PICOS vision.

Trust, privacy and identity management also present some economic considerations. Based on advanced information and communication technologies, information has become a valuable, tradable good. Information about individuals (personal information) especially has an economic value for companies and service providers, as it allows a personalised addressing of these individuals, e.g., for marketing and service provision purposes, in order to reach their limited attentiveness. From the point of view of these individual users, this raises the question of which information is accessible for whom, and in which form. Therefore it becomes of major importance that users are given the possibility to manage their personal information and to keep control over their publication and distribution. This is particularly the case within the context of online communities and social networks, since the publishing and sharing of personal information with others is an integral part of their concept. Considering the fact that communities are increasingly used in a mobile environment, the relevance of these aspects is additionally emphasized.

To address such aspects and set up a basis for this on a technical, conceptual and organizational level should be one of the fundamental goals of PICOS. PICOS should intend to demonstrate how trust, privacy and IdM could be introduced in the context of mobile communities and the respective services, and how they could be integrated within their social, technical and economic context, consistent with the partially diverging perspectives, interests and goals of the parties concerned. The balancing of the perspectives can be regarded as one of the major challenges of the project. Among the concerned parties, besides community users, PICOS further has to consider the community providers and potential third parties, such as, e.g., service providers and advertisers. Hence, the research work in PICOS needs to consider not only aspects of trust, privacy and IdM, but also aspects of business, marketing, personalisation and usability, which are of relevance during the entire process of collecting, analysing, using and distributing personal information.

The principle aim of PICOS is to research, develop, build, trial and evaluate an open, privacy-respecting, trust-enabling identity management platform that supports the provision of community services by mobile communication service providers. The aforementioned functionalities will be implemented in a successful way into the PICOS platform only when the proposed solutions fit into the existing legal framework. PICOS finds the translation of privacy principles and varied legal-regulatory instantiations to operational infrastructure to be central to the difficulties associated with addressing privacy. Some assistance is available in the form of privacy impact assessments and questionnaires; however, more elaborate "toolsets" could be devised in the context of PICOS to help bridge the gap between disparate disciplines of law, policy, technology, security, society and business. A unified toolset would help reduce the dissonance centred on concepts and a vocabulary that often thwarts understanding, communicating, and addressing privacy requirements.

A framework may help establish a common model and perspective that stakeholders (i.e., legal, regulatory, marketing, audit, security, operations, IT architects, and engineering professionals) can use to communicate with each other. Different privacy aspects (access, agent, audit, certification, control, enforcement, interaction, negotiation, usage, and validation) could help architects organize and classify a set of privacy compliance services in the framework, and could later be used to instantiate privacy policies. These services can be mapped to specific implementation details, but could initially be purposely abstract to avoid forcing the introduction of a particular technology, process or mechanism. These privacy services establish a reference architecture that empowers diverse constituents to address the problem of deciphering and translating legal code into infrastructure code. With a framework's privacy services layer, engineers, policy makers, and compliance professionals can better understand, translate, and trace legal requirements to services, and then to specific implementation details. By utilizing compliance service abstractions, IT infrastructure designers and builders can better understand and address complex privacy issues, and break complex and often ambiguous legal requirements into a more definitive and manageable set of services that can be traced and mapped to detailed infrastructure implementations. PICOS can study specific frameworks (i.e., the ISTPA Privacy Framework) to gain a comprehensive view of compliance knowing that such frameworks do not yet provide a granular means of mapping and relating regulatory requirements to solutions, while taking into account liaisons with other FP7 projects (i.e. PRIME-Life) and standardisation bodies (i.e. SC 27 of ISO/IEC JTC 1 SC 27) to define its strategic approach to privacy and identity management.

The choice of representative scenarios related to the PICOS-chosen communities will enable the consortium to model the most urgent needs related to the above mentioned open issues, and couple them with appropriate solutions and generalized architectural and design principles expressed both in a common generic platform (that can be potentially adopted as a basis by different types of communities), and in platform and community application prototypes.

Bibliography & References

[1] Abadi, M., Feigenbaum, J., 'Secure circuit evaluation', *Journal of Cryptology*, 2, 1, 1990, s. 1-12.

[2] Adam N. R., Worthmann J. C., 'Security-control methods for statistical databases: a comparative study', *ACM Computing Surveys*, 21(4):515-556, 1989.

[3] Albers A., Kahl C., 'Prototypical Implementation of an Intermediary Platform for Context-sensitive Mobile Marketing Applications', In: *Proceedings of the 14th Americas Conference on Information Systems (AMCIS)*, August 14th-17th 2008; Toronto, Canada, 2008.

[4] Andersson Ch., Camenisch J., Crane St., Fischer-Hübner S., Leenes R., Pearson S., Sören Pettersson J., and Sommer D., 'Trust in PRIME', *International Symposium on Signal Processing and Information Technology*, IEEE, 2005.

[5] Ankrum T. Scott, Kromholz Alfred H. (The MITRE Corporation), 'Structured Assurance Cases: Three Common Standards' (slides presented at the Association for Software Quality [ASQ] Section 509 Software Special Interest Group meeting, McLean, VA, January 23, 2006), available online at http://www.asq509.org/ht/action/GetDocumentAction/id/2132.

[6] Arlinghaus, R., 'Recreational fisheries in Germany: a social and economic analysis', Report of the IGB, Department of Biology and Ecology of Fishes, Leibniz Institute of Freshwater, Berlin, Germany, 2004.

[7] Arlinghaus, R, Mehner, T, Cowx, IG, 'Reconciling traditional inland fisheries management and sustainability in industrialized countries, with emphasis on Europe', *Fish and Fisheries* 3 (4), 2002, 261-316.

[8] Ateniese G, Camenisch J., Joye M., Tsudik G., 'A practical and provably secure coalition-resistant group signature scheme', in *CRYPTO 2000: Advances in Cryptology*, volume 1880 of Lecture Notes in Computer Science, pp. 255-270. Springer-Verlag, 2000.

[9] Bailey W.A., Clark T.D., 'A simulation analysis of demand and fleet size effects on taxicab service rates', in *Proceedings of the 19th Conference on Winter Simulation* (Atlanta, Georgia, United States, December 14-16, 1987). A. Thesen, H. Grant, and W. D. Kelton, Eds. WSC '87. ACM, New York, NY, 838-844, DOI= http://doi.acm.org/10.1145/318371.318705. 1987.

[10] Bailey W.A., Clark T.D., 'Taxi management and route control: a systems study and simulation experiment', in *Proceedings of the 24th Conference on Winter Simulation* (Arlington, Virginia, United States, December 13-16, 1992). WSC '92. ACM, New York, NY, 1217-1222. DOI= http://doi.acm.org/10.1145/167293.167897. 1992.

[11] Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan S., Yan, K., 'On the (Im)possibility of Obfuscating Programs', *Crypto 2001*.

[12] Benjumea, V., Geol Choi S., Lopez J., Yung M, 'Anonymity 2.0: X.509 extensions supporting privacy-friendly authentication', in *CANS'07: 6th. Intl. Conf. on Cryptology and Network Security*, volume 4856 of Lecture Notes in Computer Science, pp. 265-281. Springer-Verlag, December 2007.

[13] Benjumea, V., Geol Choi S., Lopez J., Yung M, 'Fair Traceable Multi-Group Signatures', in *FC'08: 12th. Intl. Conf. on Financial Cryptography and Data Security*, Lecture Notes in Computer Science. Springer-Verlag, January 2008 (also http://eprint.iacr.org/2008/047).

[14] Blaze M., Feigenbaum J., Lacy J., ,Decentralized Trust Management', in *Proceedings of the 17th Symposium on Security and Privacy*, IEEE Computer Society Press, 1996, pp. 164-173.

[15] Bloomfield R. E., Guerra S., Masera M., Miller A., Weinstock Ch.B., 'International Working Group on Assurance Cases (for Security)', *IEEE Security & Privacy* 4, 3 (May-June 2006): 66-68 [BLO06a].

[16] Bloomfield R. E., Guerra S., Masera M., Miller A., Sami O.S., 'Assurance Cases for Security Workshop Report', Version 01c, *Workshop on Assurance Cases for Security*, Arlington, VA, June 13-15, 2005 (2006) [BLO06b].

[17] Brands, S.A., *Rethinking Public Key Infrastructures and Digital Certificates Building in Privacy*, The MIT Press, August 2000.

[18] Camenisch J., Van Herreweghen E.v., 'Design and implementation of the idemix anonymous credential system', in *Proceedings of 9th ACM Conference on Computer and Communications Security (CCS)*, Washington D.C., November 2002. ACM, Academic Press.

[19] Camenisch, J., Lysyanskaya, A., 'Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation', in *EUROCRYPT 2001: Advances in Cryptology*, volume 2045 of Lecture Notes in Computer Science, Springer-Verlag, 2001, pp. 93-118.

[20] Camenisch, J., 'Better Privacy for Trusted Computing Platforms', *ESORICS 2004*, LNCS 3193, 2004.

[21] Camenisch, J., Shelat A., Sommer D., Fischer-Hübner S., Hansen M., Krasemann H., Lacoste G., Leenes R., Tseng J., 'Privacy and Identity Management for Everyone', in *ACM DIM*, 2005.

[22] Canalys research release 2008/021 – http://www.canalys.com/pr/2008/r2008021.pdf [Last Access: 2008-08-16].

[23] Carlsson Ch., Havnen A., Walden P., Making the Fun of Fishing Legal with Mobile Value Services, Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences, 2008, p. 86.

[24] Chaum, D., Evertse, J.H., 'A secure and privacy-protecting protocol for transmitting personal information between organizations', in *CRYPTO'86: Advances in Cryptology*, volume 263 of Lecture Notes in Computer Science, Berlin 1986, Springer-Verlag, pp. 118-170.

[25] Chaum, D., van Heyst, E., 'Group signatures', in *EUROCRYPT'91: Advances in Cryptology*, volume 547 of Lecture Notes in Computer Science, Berlin, 1991, Springer-Verlag, pp. 257-265.

[26] Chaum, D., 'Blind signatures for untraceable payments', in *CRYPTO'82: Advances in Cryptology*, Santa Barbara, CA USA, Aug. 1983, Plenum Press, pp. 199-203.

[27] Chaum, D., 'Security without identification: Transaction systems to make big brother obsolete', *Communications of the ACM*, 28(10):1030-1044, October 1985.

[28] Chaum, D., 'Untraceable electronic mail, return addresses, and digital pseudonyms', *Communications of the ACM*, 24(2):84-88, February 1981.

[29] Chaum, D., 'Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms' *Communication of the ACM*, Volume 4, number 2, February 1981.

[30] Chawla S., Dwork C., Mcsherry F., Smith A., Wee H., 'Toward privacy in public databases', in Joe Kilian, editor, *Proceedings of the 2nd Theory of Cryptography Conference* (TCC'05), Volume 3378, pp. 363-385. Springer-Verlag, February 2005.

[31] Chin F. Y. L., Ozsoyoglu G., 'Auditing and inference control in statistical databases', *IEEE Transactions on Software Engineering (TSE)*, 8(6):574-582, 1982.

[32] Choi, S.G., Park, K. and Yung, M., 'Short traceable signatures based on bilinear pairings', in *IWSEC 2006: Advances in Information and Computer Security*, First International Workshop on Security, volume 4266 of Lecture Notes in Computer Science, Springer-Verlag, Oct. 2006 pp. 88-103.

[33] Chow S., Eisen P., Johnson. H., Van Oorschot, P. C., 'A white-box DES implementation for DRM applications', in *Proceedings of ACM CCS-9 Workshop DRM*, 2002.

[34] Chow S., Gu Y., Johnson H., Zakharov V. A., 'An Aproach to the Obsfucation of Control-Flow of Sequential Computer Programs', *Springer LNCS 2200*, Berlin, pp. 144-155, 2001.

[35] CMMI for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing, Version 1.1 (CMMI-SE/SW/IPPD/SS, V1.1), Carnegie Mellon University, March 2002.

[36] Collberg Ch., Thomborson C., Low, D., 'A Taxonomy Of Obfuscating Transformations', University Of Auckland, New Zealand, 1997 http://www.cs.arizona.edu/~collberg/Research/Publications/CollbergThomborsonLow97a/A4.pdf [Last Access: 2008-08-16].

[37] Collberg Ch., Thomborson C., Low D., 'Breaking Abstraction and Unstructuring Data Structures', University Of Auckland, New Zealand, 1998 http://www.cs.arizona.edu/~collberg/Research/Publications/CollbergThomborsonLow97d/A4.ps.gz [Last Access: 2008-08-16].

[38] Dammann, U., Simitis, Sp., *EG-Datenschutzrichtlinie*, Nomos Verlagsgesellschaft, 1997.

[39] Denning D. E., 'Secure statistical databases with random sample queries', *ACM Transactions on* Database *Systems (TODS)*, v.5 n.3, p.291-315, 1980.

[40] Denning D. E., Denning P. J., 'The tracker: a threat to statistical database security', *ACM Trans. Database Systems*, 4(1):76-96, March 1979.

[41] Dingledine R., Mathewson N., and Syverson P.F, 'Tor: The second-generation onion router', in *Proceedings of the 13th. USENIX Security Symposium*, August 2004.

[42] Dobbing B., Lautieri S., 'SafSec: Integration of Safety & Security Certification SafSec Methodology: Standard', November 2nd, 2006.

[43] Dobkin D., Jones A. K., Lipton R. J., 'Secure databases: protection against user influence', *ACM Trans. Database Systems*, 4(1):97–106, 1979.

[44] Dodis, Y., Kiayias A., Nicolosi A., Shoup, 'Anonymous identification in Ad Hoc groups', in *EUROCRYPT 2004: Advances in Cryptology*, volume 3027 of Lecture Notes in Computer Science, pages 609-626. Springer-Verlag, 2004.

[45] Ellison C., Frantz B., Lampson B., Rivest R., Thomas B., Yionen T., RFC-2693. SPKI certificate theory. IETF SPKI Working Group, September 1999.

[46] Ellison, C., RFC-2692, SPKI requirements. IETF SPKI Working Group, Sept. 1999.

[47] European Commission, Privacy Enhancing Technologies: How to create a trusted information society, A Fine Balance Conference 2007, London, 2007, http://www.petsfinebalance.com/docrepo/Fine%20Balance%20London%20FinalReport%20FINAL%20VERSION.pdf.

[48] Farrel S., Housley R., RFC-3281, An Internet Attribute Certificate Profile for Authorization, The Internet Society, April 2002.

[49] Fleming Seay A., Jerome W., Sang Lee K. & Kraut R., 'Project massive – A study of online gaming communities', *Proceedings of CHI 2004*, ACM Publishing, Vienna, Austria, 2004.

[50] Fremuth N., Tasch A., 'Mobile Communities – new business opportunities for mobile network operators?', in: *Paper submitted to the 8th Intl Workshop on Mobile Multimedia Communications MOMUC*, München, Germany, 2003.

[51] Froese, R; Pauly, D, *Fishbase version* (02/2008), http://fishbase.org/search.php.

[52] Goodenough J., Lipson H., and Weinstock Ch., 'Arguing Security – Creating Security Assurance Cases', available online at https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/assurance/643-BSI.html.

[53] Gross R., Acquisti A., 'Information Revelation and Privacy in Online Social Networks (The Facebook Case)', in: *Proceedings of ACM Workshop on Privacy in the Electronic Society (WPES)*, ACM, Alexandria, United States, 2005.

[54] Hacini S., Cheribi H., Boufaïda Z., 'Dynamic Adaptability using Reflexivity for Mobile Agent Protection', *Proceedings of World academy of science, engineering and technology*, Volume 17, ISSN 1307-6884, 2006.

[55] Hacini S., 'Using dynamic adaptability to protect mobile agents code', *Information Technology: Coding and Computing*, 2005.

[56] Hampton Sh., New York, letter to Paul Croll, King George, VA, June 8, 2006 (approval by IEEE Standards Board of new Project P15026). Available from: http://standards.ieee.org/board/nes/projects/15026.pdf.

[57] Hogben G., 'Security Issues and Recommendations for Online Social Networks', ENISA, October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

[58] Holznagel, B., Sonntag, M., 'A Case Study: The JANUS Project' in Nicoll, C., et al (eds.), *Digital Anonymity and the Law – Tensions and Dimensions*, TMC Asser Press, The Hague, 2003.

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

[60] Huberman B., Franklin M., Hogg T. 'Enhancing Trust and Privacy in Electronic Communities', in *Proceedings of the 1st ACM conference on Electronic commerce*, Denver, Colorado, United States, 1999, pp. 78-86.

[61] International Security Trist and Privacy Association (ISTPA), *Analysis of Privacy Principles: Making Privacy Operational*, Version 2.0, May 2007.

[62] ISO, ISO/IEC 15288:2008. Systems and software engineering - System life cycle processes. 2nd International Organization for Standardization/International Electrotechnical Commission, 18th March 2008.

[63] ITU-T Recommendation X.509, Information Technology – Open systems interconnection – The Directory: Authentication Framework, June 1997.

[64] ITU-T Recommendation X.509, Information Technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, March 2000.

[65] Jøsang A., Ismail R., and Boyd C., 'A survey of trust and reputation systems for online service provision', *Decision Support Systems*, 43, 2 (March 2007), pp. 618-644. DOI= http://dx.doi.org/10.1016/j.dss.2005.05.019.

[66] Kargupta H., Datta S., Wang Q., Sivakumar K., 'On the privacy preserving properties of random data perturbation techniques', in *ICDM '03: Proceedings of the Third IEEE International Conference on Data Mining*, Washington, DC, USA, 2003. IEEE Computer Society, 2003.

[67] Kiayias A., Tsiounis Y., Yung M. 'Traceable signatures', in *EUROCRYPT 2004: Advances in Cryptology*, volume 3027 of Lecture Notes in Computer Science, pp. 571-589. Springer-Verlag, 2004.

[68] Kinateder M., Pearson S., 'A Privacy-Enhanced Peer-to-Peer Reputation System', *LNCS* Volume 2738, 2003.

[69] Kleinberg J. M., Papadimitriou C. H., Raghavan P., 'Auditing boolean attributes', *PODS*, pp. 86-91, 2000.

[70] Koorn Ronald (ed.), *Privacy Enhancing Technologies: White Paper for Decisions-Makers*, Ministry of the Interior and Kindom relations, the Netherlands, 2004.

[71] Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, 2003.

[72] Kursawe K., Schellekens D., Preneel B., 'Analyzing trusted platform communication', *ECRYPT Workshop*, 2005.

[73] Liao Z., 'Real-time taxi dispatching using Global Positioning Systems', *Communications of the ACM* 46, 5 (May. 2003), 81-83. DOI= http://doi.acm.org/10.1145/769800.769806. 2003.

[74] Link H.E., Neumann W.D., 'Clarifying obfuscation: improving the security of white-box DES', *Information Technology: Coding and Computing*, 2005.

[75] Malin, B., 'Compromising privacy with trail reidentification: The reidit algorithms', *Technical Report CMUCALD-02-108*, Carnegie Mellon University, 2002.

[76] Marsh S., Brown I., 'Privacy Engineering Whitepaper', *A Report from the Special Interest Group of the Cyber Security KTN*, 2008,

http://www.petsfinebalance.com/docrepo/Privacy%20engineering%20whitepaper%20FINAL.pdf.

[77] Massively.com, http://www.massively.com/2007/12/04/japanese-media-company-launches-mobile-mmog/, Access: 2008-05-23.

[78] Matloff, N. S., 'Another look at the use of noise addition for database security', in *IEEE Symposium on Security and Privacy*, p. 173-181, 1986.

[79] McDonald, J. T., Yasinsac, A., 'Towards Working With Small Atomic Functions', *Security Protocols Workshop*, Brno, 2007.

[80] MMOGCHART.COM, http://www.mmogchart.com, Accessed: 2008-05-20.

[81] Mont M.C., Pearson S., Bramhall P., 'Towards accountable management of identity and privacy: sticky policies and enforceable tracing services', *Database and Expert Systems Applications*, 2003.

[82] Mouratidis H., Giorgini P., 'Integrating Security and Software Engineering: an Introduction', chap. I in *Integrating Security and Software Engineering*, H. Mouratidis and P. Giorgini, eds., Hershey, PA: Idea.

[83] Myers, M., Ankney R., Malpani A., Galperin S., Adams C., RFC-2560. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, The Internet Society, June 1999.

[84] Nardi B., Harris J., 'Strangers and friends – collaborative play in World of Warcraft', *CSCW06 Proceedings*, Banff, Canada, 2006.

[85] Nguyen L., Safavi-Naini R., 'Efficient and provably secure trapdoorfree group signature schemes from bilinear pairings', in *ASIACRYPT 2004: Advances in Cryptology*, volume 3329 of Lecture Notes in Computer Science, pp. 372-386. Springer-Verlag, 2004.

[86] Nickerson J., Chow S., Johnson H., 'Tamper Resistant Software: Extending Trust in Hostile Environment', *Proceedings of the 2001 workshop on Multimedia and security*, ACM. 2001.

[87] Nokia Corporation, 'Symbian OS Overview to security', v1.1. http://forum.nokia.com/main/platforms/s60/security.html, 2006 [Last Access: 2008-08-16].

[88] Outdoorfoundation 2007: State-Level Economic Contributions of Active Outdoor Recreation – Technical Report on Methods and Findings. April 2007, http://www.outdoorfoundation.org/pdf/ResearchRecreationEconomyStateTechnicalReport.pdf.

[89] Persiano P., Visconti I., 'An anonymous credential system and a privacy-aware PKI', in *ACISP 2003: Proc. 8th Australasian Conf. on Information Security and Privacy*, volume 2727 of Lecture Notes in Computer Science, pp. 27-38. Springer-Verlag, 2003.

[90] Persiano P., Visconti, I., 'An efficient and usable multi-show nontransferable anonymous credential system', in *FC 2004: Financial Cryptography: 8th Intl. Conf.*, volume 3110 of Lecture Notes in Computer Science, pp. 196-211. Springer-Verlag, 2004.

[91] Pitblado R. and Smith E. (DNV London), 'Safety Cases for Aviation. Lessons from Other Industries', in *Proceedings of the International Symposium on Precision Approach and Automatic Landing*, 2000.

[92] Pocketgamer.co.uk, http://www.pocketgamer.co.uk/r/Mobile/Vivendi+Games+Mobile+News/feature.asp?c=5520, Acessed: 2008-05-21.

[93] Reiter M., Rubin A., 'Crowds: Anonymity for Web Transactions', *ACM Transactions on Information and System Security*, 1(1):66-92, November 1998.

[94] Resnick P., Kuwabara K., Zeckhauser R., Friedman E., 'Reputation systems', *Communications of the ACM*, v.43 n.12, p.45-48, December 2000 [doi>10.1145/355112.355122].

[95] Ribbers P., 'Privacy Risks, Benefits and Costs', in: PRIME 'F' Series of Deliverables – Business Processes and Business Case, *PRIME Project Deliverable*, Rotterdam, The Netherlands, 2008, pp. 167-200.

[96] Riordan J., Schneier B., 'Environmental Key Generation Towards Clueless Agents', *Springer LNCS 1419*, Berlin, 1998, s. 15-24.

[97] Rivest R., Shamir A., Tauman Y., 'How to leak a secret', in *ASIACRYPT 2001: Advances in Cryptology*, volume 2248 of Lecture Notes in Computer Science, pp. 552-565, Springer-Verlag, 2001.

[98] Royer D., 'FIDIS D11.3: Economic aspects of mobility and identity', *FIDIS Project Deliverable*, Frankfurt, Germany, 2007.

[99] RSA Laboratories, PKCS #11: Cryptographic Token Interface Standard v2.20, http://www.rsa.com/rsalabs/node.asp?id=2133, 2007. [Last Access: 2008-08-16].

[100] SafSec , webpage, Bath, Somerset, UK: Praxis High Integrity Systems Ltd., Available from: http://www.praxis-his.com/safsec/index.asp.

[101] Samarati P., Sweeney L., 'Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression', *Technical Report SRICSL-98-04*, SRI Computer Science Laboratory, 1998.

[102] Sander T., Tschudin Ch., 'Protecting Agents From Malicious Hosts', *Springer LNCS 1419*, Berlin, 1998, s. 44-60.

[103] Sandhu R., Zhang X., 'Peer-to-Peer Access Control Architecture Using Trusted Computing Technology', *SACMAT'05*, ACM 2005.

[104] Scherner, T., Privacy as an enabler for new communities – an example of a leisure-time community, *3rd FIDIS Doctoral Consortium: Identity Management & Mobility in Practice*, 2006, Stockholm, Sweden.

[105] Schlorer J., 'Information loss in partitioned statistical databases', *Computer Journal*, 26(3):218-223, 1983.

[106] Shields C., Levine B., 'A Protocol for Anonymous Communication over the Internet', in *Proceedings 7th ACM Conference on Computer and Communication Security*, Nov. 2000.

[107] Silva A.P., Mateus G.R., 'Location-Based Taxi Service in Wireless Communication Environment', in *Proceedings of the 36th Annual Symposium on Simulation* (March 30 – April 02, 2003), IEEE Computer Society, Washington, DC, 47. 2003.

[108] Software Security Assurance: A State-of-the-Art Report (SOAR) July 31, 2007.

[109] SSE-CMM: Systems Security Engineering – Capability Maturity Model, Herndon, VA: International Systems Security Engineering Association [ISSEA]. Available from: http://www.sse-cmm.org/index.html.

[110] Strunk E. and Knight J., 'The Essential Synthesis of Problem Frames and Assurance Cases', *Proceedings of 2nd International Workshop on Applications and Advances in Problem Frames, co-located with 29th International Conference on Software Engineering*, Shanghai, May 2006.

[111] Sun Microsystems, 'Java Card Platform Specification v 3.0', http://java.sun.com/javacard/downloads/index.jsp. 2008 [Last Access: 2008-08-16].

[112] Sweeney L., 'k-Anonymity: A model for protecting privacy', *International Journal on Uncertainty*, Fuzziness and Knowledge-based Systems, 10(5):557-570, May 2002.

[113] Syverson P.F., Goldschlag D.M., Reed, M.G., 'Anonymous connections and onion routing', in IEEE Symposium on Security and Privacy, pp. 44-54, Oakland, California, 1997.

[114] Ubois J., 'Online Reputation Systems', in Release 1.0 Vol. 21, No. 9 (23 October 2003).

[115] Verheul E.R., 'Self-blindable credential certificates from the weil pairing', in *ASIACRYPT 2001: Advances in Cryptology*, volume 2248 of Lecture Notes in Computer Science, pages 533-551. Springer-Verlag, 2001.

[116] Walden, I., 'Data Protection', in Reed C., Angel J., *Computer Law*, 5th edition, Oxford University Press, 2003.

[117] Wasserman S., Faust K., *Social Network Analysis: Methods and Applications*, 1994, Cambridge University Press.

[118] Wilson R.L., Rosen P.A., 'Protecting data through perturbation techniques: The impact on knowledge discovery in databases', *Journal of Database Management*, 14(2):14-26, 2003.

[119] Wright J., Stepney S., Clark J.A., Jacob J., 'Designing Anonymity: A Formal Basis for Identity Hiding', *University of York Yellow Report*, Heslington, York, 2005.

[120] Wyseur B., Michiels W., Gorissen P., Preneel B., 'Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings', *the 14th Annual Workshop on Selected Areas in Cryptography*, 2007.

[121] Xu K., *Mobile agent security through multi-agent cryptographic protocols*, PhD thesis, University of Nort Texas, 2004.

[122] Yee N., 'Motivations of Play in Online Games', *Journal of CyberPsychology and Behavior*, Vol. 9, Mary Ann Liebert Inc. Publishing, New Rochelle, USA, 2007, pp. 772-775.

Annex 1

Related projects on trust (State-of-the-Art)

Trust is a fundamental concept in business, social and computing interactions between entities. Research in the area of trust for computer science has become increasingly important due to the growth of transactions made through the Internet and new ways of communication.

The term trust management was first coined by Blaze (Blaze et al., 1996) as an attempt to build a coherent framework for security policies, credentials and trust relationships. A trust management system should comply with a language for actions, a naming of principles, a language for policies, a language for credentials and a compliance checker. While most of the work done in trust management is related to the specification of trust relationships, an important part of the study of trust is the mechanisms and tools used for analysis and verification of these models.

There are several projects and organizations devoted to the study of trust in this field. We will here mention some of them and will highlight their main aims and results.

GridTrust http://www.gridtrust.eu/html/index.jsp

The overall objective of this project is to develop the technology to manage trust and security for the Next Generation Grids (NGG).

GridTrust will leverage current work on security requirements, modelling and analysis of complex systems, information and network security, and trust and security management, and adapt them for the Next Generation Grids.

The main output of GridTrust is a framework consisting of: (1) a methodology and an interactive execution environment that will help Grid service requestors and providers to express and reason about trust, security and privacy properties for different kinds of virtual organisation (VO) topologies, taking into account aspects such as self-organisation, self-management, self-adaptation and evolvability; (2) a reference Grid Security Architecture, including autonomic policy management for fine grained usage control of Grid resources; and (3) an open source reference implementation of trust and security management systems, validated by scenarios in the business domain.

The resulting tools will be of a generic nature and will be validated on innovative applications from different application sectors. The tools will be compliant with the Open Grid Services Architecture (OGSA).

Open TC http://www.opentc.net/

The Open Trusted Computing (OpenTC) consortium is an R&D project focusing on the development of trusted and secure computing systems based on open source software. The project targets traditional computer platforms as well as embedded systems such as mobile phones.

The goal of OpenTC is to reduce system-related threats, errors and malfunctions.

The lack of platform security in today's computers has given rise to waves of successful attacks, resulting in severe damage to enterprises and potential failures in critical infrastructure.

The OpenTC consortium will define and implement an open Trusted Computing framework. The architecture is based on security mechanisms provided by low level operating system layers with isolation properties and interfaces to Trusted Computing hardware. These layers make it possible to lever enhanced trust and security properties of the platform for standard operating systems, middleware, and applications.

The suggested architecture is applicable to a wide range of platform types, e.g. servers, GRID technology, mobile phones and industrial automation. It provides basic building blocks for complex, distributed scenarios with inherent, multilateral trust and security capabilities. The framework will be built around the "Trusted Platform Module" (TPM) specified by the Trusted Computing Group (TCG), and the new generation of x86 CPUs from Intel and AMD

To enable maximum community benefit, project results will be integrated in and distributed as Open Source software, supporting Linux in particular.

The project aims to have the first Open Trusted Computing prototypes available around the time when proprietary Trusted Computing operating systems and solutions are expected to come to the market.

Trust4All http://www.win.tue.nl/trust4all/

Trust4All is an ITEA funded project. The problem that the Trust4All project aims to solve is how to establish and maintain the correct operation of a system while the software embedded in the system is being upgraded and extended (while the system is in use by a customer).

The trust model the project envisages assumes that trust relations change over time. For example, a component trust decision may be based on shared trust resources and they, in turn, are constantly changing. The dynamicity of trust relations requires mechanisms for establishing a level of trust at run-time. This is in contrast to the current situation where a certain level of trust is established by (formal) verification/extensive testing of a software configuration before deployment. The techniques for establishing trust before deployment have become inadequate, especially in component based systems, due to the more and more dynamic software configurations required by today’s applications.

PRIME https://www.prime-project.eu/

All social and economic interactions between human beings in modern civilisation require the exchange of some personal data. *The decision what data to make available is made intuitively in normal life*, such as, for instance, the one of whether or not to state your name when shaking hands.

In the online world, every person has to handle *numerous accounts and data sets*. These so-called "*partial identities*" will increasingly play a key role in future electronic services, as well as in public security (e.g., border controls). They may very well convey sensitive personal data, such as patient health data, employee data, credit card data, etc.

Surveys have shown that people now feel their *privacy is at risk* from identity theft and erosion of individual rights. In the Information Society, people want to interact securely and safely while maintaining control of their personal data.

PRIME focuses on **solutions for privacy-enhancing identity management** that support end-users' sovereignty over their private sphere, and enterprises' privacy-compliant data processing.

TrustCom http://www.eu-trustcom.com/

The mission of the TrustCoM integrated project is to provide a trust and contract management framework to enable the definition and secure enactment of collaborative business processes within Virtual Organisations that are formed on-demand, are self-managing and evolve dynamically, and share computation, data, information and knowledge across enterprise boundaries, in order to:

- tackle collaborative projects that their participants could not undertake individually; or
- to collectively offer services to customers that could not be provided by the individual enterprises.

Such VOs will be based on new forms of collaboration in which participants (enterprises or individuals) can specify and negotiate their own conditions of involvement by means of electronic contracts, whose operation is supported and enforced by the computing infrastructure. Such collaborations can be established only in a secure environment where the controls and procedures are automated based on clear specifications of trust, risk and policy.

To achieve this mission, TrustCoM will conduct multidisciplinary research into complex, adaptive and self-organising systems in order to deliver a novel trust and contract management reference framework that will enable collaborative work within on-demand created and self-managed dynamic collaborative networks of businesses and governments built on top of the emerging convergence of Web Services and Grid technologies.

TuBe http://www.cs.helsinki.fi/group/tube/

The TuBE project opens a series of projects on trust management. The project aims to define a trust management architecture that addresses application level needs; such architecture will address trust issues, and express and manage trust information and system management facilities that apply trust information. The architecture will especially focus on detecting misbehaviour and contractual breaches

in virtual enterprises. Further along during the project series, middleware level services for counteractions will also be demonstrated.

CoreGrid

The CoreGRID Network of Excellence (NoE) aims at strengthening and advancing scientific and technological excellence in the area of Grid and Peer-to-Peer technologies. To achieve this objective, the Network brings together a critical mass of well-established researchers (155 permanent researchers and 168 PhD students) from forty-one institutions, who have constructed an ambitious joint programme of activities. This joint programme is structured around six complementary research areas that have been selected on the basis of their strategic importance, their research challenges, and the recognised European expertise to develop next generation Grid middleware, namely:

- knowledge & data management;
- programming models;
- architectural issues: scalability, dependability, adaptability;
- Grid information, resource and workflow monitoring services;
- resource management and scheduling;
- Grid systems, tools and environments.

The Trust and Security activity in CoreGRID (http://www.coregrid.net/mambo/content/view/192/277/) runs as a horizontal integration activity related to all the research areas, and makes the Network participants aware of the use of the technologies associated with trust and security.

iTrust http://www.itrust.uoc.gr/

iTrust is an Information Society Technologies (IST) Working Group that started on 1st of August, 2002. The Working Group is being funded as a Concerted Action/Thematic Network by the Future and Emerging Technologies (FET) unit of the IST programme.

The aim of iTrust is to provide a forum for the cross-disciplinary investigation of the application of trust as a means of establishing security and confidence in the global computing infrastructure while recognizing trust as a crucial enabler for meaningful and mutually beneficial interactions.

The proposed forum will bring together researchers with a keen interest in the complementary aspects of trust, from technology-oriented disciplines and the field of law, social sciences and philosophy. This will hence provide the consortium participants (and the research communities associated with them) with the common background necessary for advancing toward an in-depth understanding of the fundamental issues and challenges in the area of trust management in open systems.

iTrust will lead to the definition of a number of closely interacting research projects focusing on different aspects of trust management or introducing trust management into existing and emerging technologies, regulatory and legislative frameworks.

Trust Online: Using social dilemma testing to study effects on trust
http://research.microsoft.com/scg/

Microsoft Social Computing Group

Microsoft

Social Dilemma Testing studies how different modes of communication and different aspects of the user interface affect trust and cooperation between users. To study the interactions, a new type of user testing adapted from quantitative sociological techniques is used to examine interactions between users.

Trust http://cswww.essex.ac.uk/Research/trust/index.htm

Machine Learning and Intelligent Agents Group. University of Essex

University of Essex

This project investigates issues regarding trust relationships between agents that interact in electronic marketplaces. In particular, we are interested in trust-related issues that arise in a market place scenario that involves a number of agents that depend on each other in order to achieve their goals. The markets that we are currently investigating are populated by seller, intermediary and buyer agents. Buyers wishing to obtain goods turn to intermediaries who negotiate with sellers/suppliers. The levels of intermediary agents vary. In such an environment, agents may have different strategies and a different disposition towards trust. Consequently, there is a need to study trust, compare different trust models and the effects of trust in the market environments.

Security and Trust in Sensor Networks
http://research.cens.ucla.edu/projects/2006/Systems/Security_Trust/default.htm

Center for Embedded Networked Sensing (CENS). University of California Los Angeles (UCLA)

NSF Science & Technology

Networks of wirelessly interconnected embedded sensors and actuators promise an unprecedented ability to observe and manipulate our physical world. Indeed, recent years have seen much research on understanding the fundamental properties of such networks, and on developing algorithms and hardware-software building blocks for cheap and energy-efficient implementation. However, as with almost every disruptive technology that has impacted human society, the benefits of embedded networked sensors are accompanied by significant risk factors and potential for abuse. If wireless sensor networks are to be the eyes and ears of our society, then one needs to answer the following question: How can a user trust the information provided by the sensor network? This has become a key bottleneck that still hinders the wide scale adoption and deployment of embedded networked sensing in day-to-day life.

The PICOS project receives research funding from the Community's Seventh Framework Programme.

Research efforts in this domain are motivated by two key observations. First, sensor networks are highly susceptible to malicious behaviour wherein an adversary can capture nodes and subsequently pose as an authenticated node in the network. Sensor networks often operate unattended in physically insecure environments, and are designed with an emphasis on numbers and low cost, which makes measures such as tamper-proof hardware not cost effective. This makes the problem of developing secure sensor network applications, which heavily relies on inherent trust and collaborative behaviour between network nodes, even more challenging. Second, sensor networks are deeply coupled with the physical world, which influences the tasks that they perform (detection, identification, tracking, inference, reconstruction, etc.) as well as the core middleware services they depend on (node location, timing synchronization, sensor calibration, etc.). This coupling opens up new types of security attacks whereby a malicious adversary seeks to subvert the sensor network by exploiting weaknesses at the interface between the sensor network and the physical world. The adversary can cause an event-detection and tracking task to fail by manipulating the node localization or timing synchronization processes, or by manipulating the sensing channel.

A Service Oriented Trust Development Platform
http://www.trustedwebservices.org/content/view/36/36/1/0/lang,en/SafeLayer

Trust is a key issue to develop business, either in a traditional or in an electronic environment. In order to take direct decisions with minimum risk, trust management creates a unified framework for specifying and interpreting security policies, credentials and relationships. In a closed virtual organization, trust is commonly established with the use of Trusted Third Parties (TTP), and propagated in a hierarchical model. However, this architecture is not appropriate for a global scenario formed by isles of TTP: trust management can quickly become extremely complex and tedious for people to maintain. The solution is a TDP that automates the trust management to make decisions about trust as users (Relying Parties) themselves would do.

The key principles of a TDP are the following:

- Hiding the complexity of trust development to produce a final diagnosis of the trust level of a transaction, operation, document, etc. A trust evaluation is performed using all the security data involved in an operation (certificate chains, certificate revocation lists, time stamps, etc.), in consideration of the trust offered by the TTPs (CA, VA, TSA, etc.) that issued them.
- Delegating security configuration in a centralized system based on policies that release the consumers (users, applications or other web services) from its complexity.
- Easing the use, integration and interoperability of digital signatures and envelopes, and encapsulating all the standard formats (PKCS#7, CMS/CAdES, S/MIME, XMLDSig, XAdES, XML-Enc, PDF, etc.) and its processing complexity under a common service interface.
- Providing a centralized point of accounting and auditing, and even trust archiving, and thus making it feasible to manage and develop trust material for long periods of time.

On the other hand, it is important that a TDP can be easily integrated with other services and accessible from any device. Our proposal is to deploy a TDP as a web service (WS) that offers an interface fully based on Extensible Markup Language (XML). XML is currently the universal format to represent structured documents and data on the Web. In the TDP, it will be used in service invocations as well as in configuration, personalization, monitoring, auditing and access control. TDP

transactions are wrapped with SOAP, which defines a standard framework for the composition of request/response messages to a service. WSDL provides an abstract definition of the service independent of the programming language used in its implementation, and UDDI is used for the publication and discovery of the services.

The proposed trust management framework is flexible and scalable, and not only addressed to provide services for the internal security consumption. It can also be seen as a trusted platform that can be integrated in the enterprise workflows. The TDP provides business components with specialized trusted security services. The main TDP components are the following:

- An Authentication and Authorization service that includes different authentication mechanisms such as login/password, certificate-based (TLS/SSL, digital signature, etc.), etc. This service also includes an open authentication extension mechanism (one-time password, tokens, kerberos, etc.), which makes possible the addition of new mechanisms. Access control is internally enforced and the Authorization service can be consumed through SAML protocol.
- An information management service which uses XML to provide uniform object and/or entity profiles: users, applications, web services, policies, certificates, logs/audit, etc.
- A digital signature service that allows the generation of basic signatures in different well-known formats (PKCS#7/CMS, PDF, XMLDsig/XAdES and S/MIME).
- An advanced digital signature service that adds reliable time and revocation information to previously signed documents, as a base for long term signatures.
- A digital signature verification service (includes advanced or long term signatures) independent from the supplier, certificate verification mechanism (CRL, OCSP, etc.) and signature format.
- A digital signature custody service that enables the maintenance the signature's validity for long periods of time, and thus, therefore, the implemention of long term digital signatures by using the XAdES ES-A standard.
- A document enciphering and deciphering service using PKCS#7/CMS and XML-Enc formats.
- A document enciphering key custody service that guarantees long term access to protected data.
- A key management service for key generation, registration, consultation, verification, etc., for instance, based on XKMS.

Access to the security services is performed with standardized WS protocols: Oasis DSS (Digital Signature Services), WSS (Integrity and confidentiality of SOAP messages) and SAML (Single-Sign On and Federation) are the basic standards.

Trust services are as accessible in their composition, orchestration and consumption as any other business services from an SOA. The TDP facilitates for the rest of the business components a set of security specialized services that they can consume, such as:

- Authentication, authorization and unified access control.
- Identity federation.
- Federation of attribute entity information.
- Cryptographic key management, secure sessions, single sign-on, etc.

- Generation and validation of digital signatures.
- Data protection.
- Information notarization for non-repudiation using long-term digital signatures.

The PICOS project receives research funding from the Community's Seventh Framework Programme.