Grant Agreement no. 215056

Title:	***D2.1 Taxonomy***
Editor:	*Eleni Kosta & Jos Dumortier (Katholieke Universiteit Leuven - Interdisciplinary Centre for Law and ICT)*
Reviewers:	*Javier Lopez (Universidad de Málaga)*
	Tobias Scherner (Johann Wolfgang Goethe-Universität)
Identifier:	*D2.1*
Type:	*Deliverable*
Version:	*1.0*
Date:	*17/07/2008*
Status:	*Final*
Class:	*Public*

Summary

The objective of the PICOS project in general 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. Therefore, this deliverable serves as an inventory of common terminology on trust, privacy and identity related aspects of identity management. The terminology included in this deliverable has been established within the PICOS Consortium and attempts to consolidate the different perspectives in a multidisciplinary report. The terms included in this deliverable will be considered as working definitions reflecting the project's focus, which aim at providing a common understanding among the project partners of the main terms that are used within the project.

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 located at 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 consciously leave private information online; 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 by scenarios of private and professional communities;
- *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), Jos Dumortier (ICRI-K.U.Leuven).
2.1 Terminology related to communities and usability	Christina Köffel (CURE), Katja Liesebach (GUF), Johann Schrammel (CURE)
2.2. Electronic and mobile communications terminology	Georg Kramer (TMO), Tobias Kölsch (TMO), Cathleen Simons (ATOS), Eleni Kosta (ICRI-K.U.Leuven)
2.3 Introductory terminology on privacy, identity management and trust	Katja Liesebach (GUF), Petr Svenda (Masaryk University), Vicente Benjumea (UMA), Cathleen Simons (ATOS)
2.4 Legal terms regarding data protection and identity management	Eleni Kosta (ICRI-K.U.Leuven), Cathleen Simons (ATOS)
2.5 Architecture and technical terminology	Stephen Crane (HPL), John O'Connell (HPF), Jean-François Coudeyre(HPF)
2.6 Terminology on assurance of technical trust and privacy properties	Issac Agudo (UMA), José Luis Vivas (UMA), Tobias Scherner (GUF)
3. Closing remarks	Eleni Kosta (ICRI-K.U.Leuven), all contributors
A.1 Glossary of angler and fisheries terminology	Bernd Ueberschär (IFM GEOMAR)
A.2 Terminology related to online gaming communities	Katja Liesebach (GUF), Christian Kahl (GUF)

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*
AARL	*Attribute Authority Revocation List*
AC	*Attribute Certificate*
ACRL	*Attribute Certificate Revocation List*
CRL	*Certificate Revocation List*
DBMS	*Database Management System*
dCRL	*Delta CRL*
DIT	*Directory Information Tree*
DN	*Distinguished Names*
DNA	*Deoxyribonucleic Acid*
EPRL	*End-entity Public-key certificate Revocation List*
iCRL	*Indirect CRL*
IDM	*Identity Management*
IEC	*International Electrotechnical Commission*
IMS	*Identity Management System*
IP	*Internet Protocol*
ISO	*International Standardisation Organisation*
ITU	*International Telecommunication Union*
JTC	*Joint Technical Committee*
OASIS	*Organization for the Advancement of Structured Information Standards*
P2P	*Peer-to-Peer*
P3P	*Privacy Preferences Protocol*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
SAML	*Security Assertion Markup Language*
SOA	*Source of Authority*

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

TA	*Trust Authority*
TPM	*Trusted Platform Module*
W3C	*World Wide Web Consortium*

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

1 Introduction

Eleni Kosta and Jos Dumortier (ICRI-K.U.Leuven)

The Taxonomy deliverable (D2.1) is the first deliverable of the PICOS project and is one of the activities of Work Package two, which bears the general title 'Requirements'. The objective of the PICOS project in general 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.

Therefore, this deliverable serves as a repository of common terminology on trust, privacy and identity related aspects. The terminology included in this deliverable has been established within the PICOS consortium and attempts to consolidate the different perspectives of different research disciplines. This multi-disciplinary activity cooperates therefore with community research activity, and forms a point of reference for the rest of the project.

As this deliverable is being prepared at the beginning of the project, it is impossible to create a full list of all the terms that will be critical for PICOS and to clearly define their special meaning in the context of the project. The terms included in this deliverable will therefore rather be considered as working definitions reflecting the project's focus, which aim at providing a common understanding, among the project partners, of the main terms that are used within the project.

The main instrument used for the initial collection of terms was an internal wiki, hosted on the internal PICOS website, which was enhanced and elaborated by the consortium members. 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. Taking this main aim into account, we identified the areas of major importance for PICOS and decided to focus on the terminology used in these areas. These areas are:

- Terminology related to communities and usability
- Electronic and mobile communications terminology
- Introductory terminology on privacy, identity management and trust
- Legal terms regarding data protection and identity management
- Architecture and technical terminology
- Terminology on assurance of technical trust and privacy properties

As the borders between some of the aforementioned categories are not very clear, it had to be decided how the terms would be classified under the relevant categories. It might be surprising at first sight for the reader to see that relevant terms are included under different sections. For instance the term "identity management" is listed under section '2.3: Introductory terminology on privacy, identity management and trust', while the term "identity management system" is mentioned in section '2.5: Architecture and technical terminology'. The differentiation in this example has a simple explanation in that while the term identity management belongs to the introductory terminology of basic terms on privacy, identity management and trust, the terms related to identity management systems are of a more technical background. Moreover, some very basic terms are mentioned in more than one section, as in the case of "Trust", which is mentioned both in '2.3: Introductory terminology on privacy, identity management and trust' and in '2.6: Terminology on assurance of technical trust and privacy

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

properties'. This happens because the term is of significant importance in both categories of terms and it has a different interpretation under each one of them.

The PICOS project is mainly focusing on online and mobile communities that exist in the real world and utilise online services to support their activities. In order to be able to first conceptually define the context of PICOS and, at a further stage, to test the platform that is to be built, three types of communities were chosen to be analysed: the angling, online gaming and independent taxi drivers' communities. Although the terminology related to the last aforementioned community is trivial and known to the broader public, the other two communities have terms unknown not only to the reader of the output of PICOS, but also to (at least the majority of) the consortium partners. Therefore, an Appendix was also drafted that includes definitions on (i) the Angler and Fisheries Terminology, and (ii) Online Gaming Communities. A third Appendix includes a list of all the terms for the convenience of the reader.

2 Terms and definitions

2.1 Terminology related to communities and usability

Christina Köffel (CURE), Katja Liesebach (GUF) and Johann Schrammel (CURE)

In the past few years, communications bandwidth has increased and mobile personal computing and communication devices with high computing processing power have become ubiquitous. These new technologies are widely available to citizens at low cost and enable the creation of many communities of ICT end-users, and the offering of round-the-clock access to the services that are provided by/for their communities [33]. The PICOS project is mainly focusing on online and mobile communities that exist in the real world and utilise online services to support their activities. Such communities can vary significantly between one another and can, for example, either be oriented around private or professional activities, have open or controlled membership, have or not have legal status, and have differing types of data exchange (e.g., voice audio, still images, video, et cetera). In this broad context, and given the diverging needs and expectations of each community, PICOS aims at building a state-of-the-art platform for providing the trust, privacy and identity management aspects desired of community services and applications on the Internet and in mobile communication networks.

Therefore, it is rendered necessary to commence with the description of the terms related to communities and usability. Defining the types of communities as a first step is essential in order to allow the reader to understand the landscape where PICOS wishes to build its platform. As already pointed out above, the terms included in this deliverable, and consequently in this chapter, will be considered as working definitions reflecting the project's focus, which aim at providing a common understanding among the project partners of the main terms that are used within the project. Terms relating to communities and usability that are coined by popular science, as well as wide spread definitions, have made finding the perfect definitions, at such an early stage of the project, especially hard, and even partially impossible. This is the reason why this part contains, to some extent, descriptions of terms instead of scientific definitions.

This chapter is further divided into three parts: section one presents the basic terminology regarding online and mobile environments in order to deploy the specific definitions about communities that are covered the second section; and the third section, finally, discusses the most important terms regarding usability in the context of PICOS. The terms in this chapter are not listed in alphabetical order, but are

rather presented in a logical order, so that the reader can use the first terms to understand the following ones.

2.1.1 Basic terminology for online and mobile environments

2.1.1.1 Context-rich Environments

Environments and applications are called context-rich when they possess a wide set of influencing parameters that entail a variety of use cases and scenarios. Such contextual information comprises of profiles (of resources, locations and users) and use-oriented references, and can be of a static (e.g., be invariant user profile data) or dynamic (e.g., have characteristics of relationships) nature. Based on the opinions expressed by [26], one example for a context-rich environment is the World Wide Web (or simply "Web").

2.1.1.2 Web 2.0

Web 2.0 is a term describing the trend in the use of World Wide Web technology and web design that aims to enhance creativity, information sharing, and, most notably, collaboration among users. These concepts have led to the development and evolution of web-based communities and hosted services, such as social-networking sites, wikis, blogs, and "folksonomies" [67]. The term and concept were primarily coined by Dale Dougherty and Craig Cline during a conference brainstorming session in 2004, and were made popular by the article "What is Web 2.0" by Tim O'Reilly in 2005 [46]. A concise definition of "Web 2.0" can be found in [45], which states that "Web 2.0 is the business revolution in the computer industry caused by the move to the Internet as platform, and an attempt to understand the rules for success on that new platform".

2.1.1.3 User

Users are persons that are using a system or part of a system or service to initiate or complete tasks, or for information, installation, maintenance or training purposes. From a usability perspective it is necessary to distinguish between users, clients and stakeholders (based on http://usecon.com, [61]).

In the context of PICOS, users are defined as all persons that are members of an online or mobile community and who are using the PICOS community platform.

2.1.1.4 Stakeholder

Stakeholders are all persons and organisations interested in a system or product because of financial, commercial or legal interests. All important stakeholders should be known and accounted for at the very beginning of a development process. Otherwise, requirements of the project will only be detected during the development process, or even from the later use of the product (http://usecon.com).

In PICOS, the following stakeholders can be identified: community members, community service providers, mobile operators, service providers and platform providers.

2.1.1.5 Client

From a usability point of view, there are two stakeholders that can adopt the role of a client: the purchaser of a product, and the end-user. As the purchaser of a product is not necessarily the end-user as well, the motivation of the user and client can vary from one another.

The field of usability is generally focused on the actual use of a system by the user. Thus, the term "client" will be distinguished from the use of the word in the technical area, where clients are applications that access remote services on another system. In a broader sense, clients can also be understood as devices, such as mobile phones (based on http://usecon.com, [67]).

In PICOS, two different types of clients can be distinguished: the operators (providers) of online or mobile community portals that are using the PICOS framework, and the end-users that are using the provided portals.

2.1.1.6 Interaction

Interaction describes an action-reaction system that occurs when two or more entities (such as persons, components of systems, services, et cetera) have an effect upon one another. The idea of a two-way effect is essential in the concept of interaction, as opposed to a one-way causal effect. In contrast to the computer science world where interaction often refers to transaction and communication, interactions between humans can be distinguished between conversation, transaction and collaboration (based on [67]).

In the PICOS project, interaction is defined as any action-reaction that occurs between the PICOS community platform and the user, between the platform and the operators, between the users themselves.

2.1.1.7 Online Collaboration

Collaborative interactions between people using the Internet are named as online collaboration. In general, online collaboration involves multiple people working to achieve a common goal by using online-based collaborative tools or applications. Reasons for online collaboration can be the development of an idea, the creation of a design, and the achievement of a shared goal. An online collaboration platform is an electronic platform that supports synchronous and asynchronous communication, cooperation and coordination through a variety of devices and channels. Record or document management, threaded discussions, audit history, and other collaboration supporting mechanisms designed to capture the efforts of many into a managed content environment are typical of these kind of platforms (based on [67]).

Online collaboration between PICOS community members takes place when they are actively interacting, i.e., communicating and collaborating, via the PICOS community platform.

2.1.1.8 Content

Content can be seen as information and experiences that may provide value for a user or audience. The word “content” is often used simultaneously to refer to media, which is erroneous as it really means the content of the medium rather than the medium itself. Likewise, the single word “media” and some compound words that include “media” (like multimedia and hypermedia) are also instead referring to a type of content (based on [67]).

2.1.1.9 Social Capital

In the literature, definitions of the term “social capital” vary widely — depending on the background and personal opinions of the authors. A basic definition is given by Sirianni and Friedland [54]:

> *Social capital refers to those stocks of social trust, norms and networks that people can draw upon to solve common problems. Networks of civic engagement, such as neighbourhood associations, sports clubs, and cooperatives, are an essential form of social capital, and the denser these networks, the more likely that members of a community will cooperate for mutual benefit.*

In PICOS, where virtual communities are the focus of investigations, “social capital” can be defined, as according to Daniel, Schwier, and McCalla, as “a common social resource that facilitates information exchange, knowledge sharing and knowledge construction through continuous interaction built on trust and maintained through shared understanding” [17].

2.1.1.10 Social Cohesion

Similar to "social capital", there are a variety of definitions for the term "social cohesion". Seeing both social capital and social cohesion as a unit, i.e., as important dimensions of the standard of living, the most appropriate definition is given by Ferroni [21], who states that "[s]ocial cohesion is the capacity for cooperation in society based on the set of positive effects accruing from social capital, in addition to the sum of factors promoting equity in the distribution of opportunities among individuals".

Adapted to PICOS, social cohesion can be described according to [31] as "the ongoing process of developing a community of shared values; shared challenges and equal opportunity [...], based on a sense of trust, hope and reciprocity among all community members".

2.1.1.11 Community Cohesion

As described in [65], a cohesive community has the following characteristics:

- There is a common vision and a sense of belonging together.
- The diversity of people's different backgrounds and circumstances are appreciated and positively valued.
- Those from different backgrounds have similar life opportunities.
- Strong and positive relationships are being developed between people from different backgrounds in the workplace, in schools and within neighbourhoods.

In essence, community cohesion is about recognising, supporting and celebrating diversity. It's about creating an environment where there is mutual respect and appreciation of the similarities and differences that make people unique.

Accordingly, "community cohesion" can be adapted to PICOS in a way that it refers to the aspect of togetherness and bonding exhibited by members of a community. Community cohesion acts as the "glue" that holds a community together.

2.1.2 Communities

2.1.2.1 Social Network

A social network is a structure representing social relations between entities often visualised by graphs containing nodes and edges. Social network structures are built based on one or more specific types of interdependency, such as values, visions, ideas, financial exchange, friends, kinship, dislike, conflict, trade, web links, sexual relations, disease transmission (epidemiology), or airline routes. The resulting structures are often very complex (based on [67]).

2.1.2.2 Social Network Analysis (SNA)

Social network analysis offers the methodology to conceptualise, to analyse and to interpret patterns of social ties by means of the visual and mathematical analysis of relationships between entities (see also [44]). An important parameter is the location of an entity in the network. The measurement of network location is finding the centrality of a node. By this, insight into various roles and groupings in a network is given, i.e., information about who are connectors, mavens, leaders, bridges, isolates, and where clusters are and who is in them, who is at the core of the network, and who is on the periphery.

In PICOS, applying SNA to communities can provide an understanding of communities' overall behaviour and development, and furthermore, result in indicators for their guidance and support.

2.1.2.3 Node

A node is an abstract basic unit used to build linked data structures such as trees, linked lists, and computer-based representations of graphs. Edges are the graphical lines connecting the nodes. In social networks, nodes are the individual actors within the networks, and edges or ties are the relationships between the actors.

2.1.2.4 Communities

As admitted by [25], there is no precise definition of the term "Community". According to him, the most general class of community is a set of people characterised by the following parameters:

- Community members share an awareness of being a member in a particular community. Community awareness is a state of mind that goes beyond more intellectual perception of a factual state. It also includes an emotional tie to the community and is connected with the will to be a part of it.
- A dense net of social relations exists among the members with a special emphasis on communication relations.
- Community members have a common pursuit which implies a motivation to actively participate in a community and which also implies a set of rules or conventions within a community.
- Community members share one or more similar personal parameters where common location of living or working and common interests are prominent examples. This gave raise to characterizations or terms such as community of practice, community of interest etc [25].

In general, it can be said that a community is a social group of entities sharing an environment, normally with shared interests. In contrast to social networks, which only represent entities that are in contact, relations in (human) communities are stronger, and, generally, a common objective is crucial for their cohesion. In communities, intent, belief, resources, preferences, needs, risks and a number of other conditions may be present and held in common. It may also affect the identity of the participants and their degree of cohesiveness.

From a psychological point of view, the motivation for participating in communities can be of an intrinsic or extrinsic nature. Intrinsically-motivated people behave and act driven by internal factors, such as, for example, the motivation related to the pleasure of doing a task itself, or from the sense of satisfaction in completing or even working on that task. This kind of behaviour is characteristic of the participation in private (leisure) communities. In contrast, external factors, such as rewards, money and grades often additionally influence the membership in professional communities (based on [67]).

2.1.2.5 Types of Communities

In the literature, a variety of approaches can be found to categorise communities — such as private/professional communities, online/offline communities, consumer-/business-oriented communities, et cetera — depending on the main aspects on which they are focussing ([9], [23] and [37]).

Since none of the available schemes matches the aims of the PICOS project, the categorisation of communities is the focus of a separate PICOS deliverable [PICOS, D2.2 Categorisation of Communities]. The PICOS categorisation is, among other things, based on the dimensions of usage,

context and purposes, structure, expected lifetime and formation characteristics, community member characteristics, interaction characteristics, content generation aspects, and type of media.

Since online and mobile communities are of special interest in the framework of PICOS, a short definition of these community types follows.

2.1.2.6 Online Community/Virtual Community

An online community is a group of people that primarily interact via information and communication technologies. Online communities have also become a supplemental form of communication between people who know each other primarily in real life.

Various means are used in social software separately or in combination, including text-based chat rooms and forums that use voice, video text or avatars. Significant socio-technical change has resulted from the proliferation of such Internet-based social networks. The agglomeration of all online communities is sometimes called the metaverse (based on [59]).

2.1.2.7 Mobile Community

A mobile community is a group of people generally united by shared interests or goals who interact either only by means of location-independent communication information and communication technologies or (also) via community platforms providing relevant mobile interfaces to their services.

2.1.2.8 Social Networking Community

With the rapid development of ICT and the possibilities to access the Internet, a special kind of online community has emerged during the last years: social networking communities (such as *MySpace.com*). Their intention is to provide a platform to primarily connect people who share interests and activities, or who are interested in exploring the interests and activities of others. Besides those who are engaged in the self-initiated exploring and joining of a network, an initial set of founders might also send out messages inviting members of their own personal networks to join them or their own networks, respectively. New members repeat the process, thus increasing the total number of members and links in the network.

2.1.2.9 Mass Online Social Network

In the context of Social Networking Communities, the term “mass social network” emerged referring to communities that encompass a considerable amount of members. They consist sometimes of the majority of the activities that can be done by all categories of social networking communities. They are also arenas that are rapidly allowing less “geeky” users to gain the necessary knowledge to move on to other niche-specific networks. Well known mass online social networks are *Facebook*, *Myspace*, and *Orkut* (based on [51]).

2.1.2.10 Community Member

A community member is a person that is participating in and using an online community. Regarding their communication behaviour, community members can be distinguished as follows [41]:

- **Founders** are a group of people that has launched and populated a community by inviting members (e.g., using contacts from their personal network).
- **Experts** have detailed and specific knowledge and experience within the domain of analysis. They own a central position in the network, and mostly possess of a high number of external linkages. In the literature, synonyms for this role include communicator, ambassador, connector, gatekeeper, and “linkerati”.

- **Knowledge brokers (or bridges)** have some knowledge of "who knows what". They build bridges between different clusters of otherwise unconnected sub-parts of the network.
- **Contact persons (or agents)** take a brokerage position in that they provide contacts with the experts without actively communicating the relevant knowledge themselves. They have an intermediary position between central (expert) and peripheral (consumer) network members.
- **Knowledge consumers** ask for knowledge from the experts. They have a peripheral network position.

In Internet culture, "lurkers" have come to play an additional and important role in the framework of communities. A lurker is a person who reads discussions on a message board, newsgroup, chat room, file sharing or other interactive system, but rarely participates (based on [67]).

Besides the above mentioned roles, further social roles can be distinguished based on the social behaviour of users in communities. For example, Renaud's classification of active users comprises of creators, critics, collectors, sociables, and onlookers [51].

2.1.2.11 (Online) Community Service

In general, community services refer to services that are performed by an entity (i.e., a person or organisation) for the benefit of the community as a whole [67]. Hence, an online community service can be either seen as the service an entity provides to an online community, or a service for the user itself provided through or by the community.

2.1.2.12 Social Networking Service

A social network service uses software to build online social networking communities for people who share interests and activities, or who are interested in exploring the interests and activities of others. Most services are primarily web-based and provide a collection of various ways for users to interact, such as chat, messaging, e-mail, video, voice chat, file sharing, blogging, discussion groups, and so on. The main types of social networking services are those that contain directories of some categories (such as former classmates), and are used as a means to connect with friends and recommender systems linked to trust. There have been some attempts to standardise these services, for example, by using the "friend of a friend" standard or the open source initiative. By using these standards, the need for duplicate entries of friends and interests could be avoided. However, this has led to some concerns about privacy, such as the possibility of automatically analysing data and relationships between users (based on [67]).

2.1.2.13 (Community) Service Provider

A community service provider is an application provider that provides community services to users (cf. section 2.2.3).

2.1.2.14 Service Aggregators

Service aggregators supply a broad range of different services such as video or multimedia. Ranging from full-fledged applications to small fragments of code that can be integrated into larger programs, they allow users to aggregate e-mail services, documents, or feeds into a single interface.

Web-based aggregators, which are of relevance for PICOS, are applications that reside on remote servers and are typically available as web applications, such as *Google Reader* or *Bloglines*. As the application is available via the Web, it can be accessed anywhere by a user with an Internet connection.

2.1.2.15 Collaborative Software

The term "collaborative software", also known as groupware, refers to software applications (e.g. e-mail, calendars, wikis, text chats) that are intended to support the distributed collaboration, coordination and cooperation of people. Usually, collaborative software is used for professional purposes.

2.1.2.16 Social Software/Social Network Application

With the spreading of social networking communities and the emergence of new collaborative tools, such as wiki and blog, the term "social network" was coined in 2000. Social software is, in general, defined as a range of web-based social network applications. These applications allow users to interact and share data with other users. This computer-mediated communication has become very popular with social sites like *MySpace* and *Facebook*, media sites like *Flickr* and *YouTube*, and commercial sites like *Amazon* and *eBay*. According to *Wikipedia*, many of these programs are service oriented (customisable), and have the ability to upload data or media. According to Schmidt, three application areas for social software can be identified [53]:

- **Information Management** allowing for the retrieval, assessment and management of online (available) information.
- **Identity Management** allowing for the representation of one's own identity on the Internet.
- **Relation Management** allowing for the mapping of personal contacts, their maintenance and the establishment of new relations.

2.1.2.17 Social Media and Content Sharing

The term "social media" describes a new set of Internet channels that enable shared community experiences, both online and in person. A community, in this context, is a group of people with common interests who connect with one another to learn, play, work, organise and socialise. Social media allow people with basic computer skills to tell their stories using publishing channels, such as blogs, video logs, photo sharing, podcasting and wikis. Social media and content sharing sites like *Youtube*, *Flickr* and *Wikipedia* allow the dissemination of all sorts of content and make it accessible in all contexts possible [51].

2.1.2.18 Blogs and Microblogs

A Weblog, or simply, a "blog", is a website that periodically contains new entries. A blog is usually maintained by an individual, with regular entries of commentary, descriptions of events, or other material, such as graphics or video (based on [67]). The blogosphere (i.e., the collectivity of blogs) is an immense social network interconnected by comments made on blogs and blogrolls (i.e., lists of blogs in the sidebar of a blog). Blogs diffuse messages, provoke debate, spread "the word" and influence opinions on products. Writing a blog allows the creation of corporate content that lives outside the corporate structure and produces traffic in a more efficient way [51].

2.1.2.19 Forum

A forum is an Internet Chat Room usually devoted to one particular subject, allowing participants to share experiences, advice and information with one another [24]. *Wikipedia* describes the term as "[a]n Internet forum is a web application for holding discussions and posting user-generated content. Internet forums are also commonly referred to as web forums, message boards, discussion boards, (electronic) discussion groups, discussion forums, bulletin boards or simply forums" [67].

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

2.1.2.20 Wiki

A wiki is a collaborative web application that allows users to add content, as on a forum, but also allows anyone to edit the content [24]. According to *Wikipedia* for instance, a wiki is a collection of web pages designed to enable anyone who accesses it to contribute or modify content, using a simplified mark-up language. Wikis are often used to create collaborative websites and to power community websites [67].

2.1.2.21 Chat Room

A chat room is a term used to describe any form of synchronous conferencing, occasionally even asynchronous conferencing. The term can thus mean any technology ranging from real-time online chat over instant messaging and online forums to fully immersive graphical social environments [67]. Therefore a chat room is an Internet environment in which participants can write messages to each other [24].

2.1.2.22 Instant Messaging

Instant Messaging (IM) is a form of real-time communication between two or more people based on typed text. The text is conveyed via computers connected over a network such as the Internet [67]**.** *Webopedia* describes Instant Messaging as a type of communications service that enables users to create a kind of private chat room with another user in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication [64].

2.1.2.23 Web Portal

According to *Wikipedia*, "a web portal is a site that provides a single function via a web page or site". Web portals often function as a point of access to information on the Web. Portals present information from diverse sources in a unified way. Aside from the search engine standard, web portals offer other services such as e-mail, news, stock prices and infotainment, and act as a service provider. Portals provide a way for enterprises to provide a consistent look and feel with access control and procedures for multiple applications, which otherwise would have been different entities altogether.

2.1.2.24 Community Web Portal

Community Web Portals serve as portals for the information needs of particular communities on the Web [57]. In their "Electronic Transactions on Artificial Intelligence", Erdmann et al. [19] describe community web portals as web portals that serve as high quality information repositories for the information needs of particular communities on the Web. A prerequisite for fulfilling this role is the accessibility of information. In community portals, this information is typically provided by the users of the portal, i.e., the portal is driven by the community for the community (based on [19]). Furthermore, community web portals are used to maintain contact with other community members.

2.1.2.25 Social Bookmarking

Social bookmarking is a way of storing, classifying, sharing and searching links through the practice of folksonomy techniques (see the section on Social Tagging/Folksonomy below) on the Internet. In a social bookmarking system, users store lists of Internet resources that they find useful, and other people with similar interests can view the links by category, tags, or even randomly [24]. Jean-Francois Renaud [51] defines social bookmarking sites as sites that have the practical advantage of sharing and reusing bookmarks anywhere on the Web. These sites, notably, allow links to point towards a site, but also to propagate information to an exclusive community. The most well known bookmarking sites are *del.icio.us*, *Magnolia* and *Stumbleupon*.

2.1.2.26 Social News

Digg, *Propeller* and *Reddit* (for English-speaking communities), or *Scoopeo*, *Nuouz*, *Wikio* and *Fuzz* (for French-speaking communities) are typical social news sites. These sites are suitable to reach the linkerati (a group of users prone to create links towards a site), and increase performance in search engines [51]. According to (http://webtrends.about.com/od/glossary/g/socialnewdef.htm), social news is a kind of social bookmarking website that is dedicated to current news, or a specific type of news such as sports or entertainment.

2.1.2.27 Social Tagging/Folksonomy

Wikipedia describes the term "folksonomy" as the practice and method of collaboratively creating and managing tags to annotate and categorise content. In contrast to traditional subject indexing, metadata here is generated not only by experts, but also by creators and consumers of the content. Folksonomy is a portmanteau of the words folk and taxonomy; hence a folksonomy is a user-generated taxonomy.

According to this definition, social bookmarking can be seen as sub-category of social tagging, since it includes blogs, pictures and social tagging entries [67]. Thomas Vander Wal defines folksonomy as the result of the personal free tagging of information and objects for one's own retrieval. The value of this external tagging is derived from people using their own vocabulary and adding explicit meanings, which may come from an inferred understanding of the information or the object [62]. Another definition of social tagging is made by Jakob Voss, according to whom the term "tagging" is referred to as, among other things, collaborative tagging, social classification, social indexing and folksonomy [63].

2.1.2.28 Social Searching

Social searching ranges from shared bookmarks to descriptive labels. It efficiently combines computer algorithms with human intelligence. Social searchers are people that use websites (mostly social networks) to investigate specific people, with whom they share an offline connection, to learn more about them [36].

2.1.2.29 Social Browsing

Social browsers are persons that use websites (mostly social networks) to find people or groups online with whom they would want to connect offline [36].

2.1.3 Usability

2.1.3.1 Human-Computer Interaction (HCI)

Wikipedia defines human-computer interaction (HCI) as the study of the interaction between people (users) and computers. It is often regarded as the intersection of computer science, behavioural sciences, design and several other fields of study. Interaction between users and computers occurs at the user interface (or simply interface), which includes both software and hardware, such as, for example, general-purpose computer peripherals and large-scale mechanical systems like aircraft and power plants [67]. Human-computer interaction is a subfield within computer science concerned with the design, evaluation, and implementation of interactive computing systems for human use, and with the study of major phenomena surrounding them (http://www.dgp.toronto.edu/people/ematias/faq/G/G-1.html).

The PICOS project will allow the researchers to investigate the design implications of interactive communities and their implementation. Furthermore, evaluation techniques applicable to online communities will be explored and assessed.

2.1.3.2 Usability

Usability describes the ease of use and the clarity of a hardware or software-based system, and should be understood as the quality of a technical system. Moreover, usability treats the design of a system according to the findings of ergonomics and describes the ease of a person accomplishing a goal using a given software system. In other words, it defines the objective and subjective quality of an interaction with a system; the quality of a system from the perspective of the actual user with defined intentions. Learnability, efficiency, memorability, low error rate and subjective satisfaction are criteria determining the usability of a system (http://usecon.com).

Two international standards further define usability and human-centred design:

- Usability refers to "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of user" (ISO 9241-11).
- "Human-centred design is characterized by: the active involvement of users and a clear understanding of user and task requirements; an appropriate allocation of function between users and technology; the iteration of design solutions; multi-disciplinary design" (ISO 13407, http://usability.gov).

The community platform developed within the PICOS project will be evaluated for its usability by assessing its learnability, efficiency, memorability, error rate and subjective satisfaction using usability evaluation methods, along with the application prototypes. As a result, a usable and understandable system will be created, allowing for a highly effective and sufficient user experience.

2.1.3.3 Ergonomics

Ergonomics is a scientific discipline concerned with the design of objects and tasks in order to improve the quality and efficiency of human work. It examines the concurrence of humans, the environment and tasks. According to *Wikipedia*, however, ergonomics is not only the scientific discipline concerned with design according to human needs, but it is also the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance [67]. The field is also called human engineering, and human factors engineering.

2.1.3.4 User Experience

User Experience broadens the focus of usability. The user is not interacting with an isolated system anymore, but he or she is rather involved in a technical environment where different parties try to communicate and collaborate at the same time. When different systems are to be distinguished from each other, it is not enough to detect its usability; a good system also provides a good user experience (http://usecon.com).

2.1.3.5 Usability Measurements

It is important to point out that usability is not a single, one-dimensional property of a user interface. According to (http://usability.gov), usability is a combination of factors including:

- **Ease of learning**: how fast can a user who has never seen the user interface before learn how to use it sufficiently well to accomplish basic tasks?

- **Efficiency of use**: once an experienced user has learned to use the system, how fast can he or she accomplish tasks?
- **Memorability**: if a user has used the system before, can he or she remember enough to use it effectively the next time, or does he or she have to start over learning how to use it?
- **Error frequency and severity**: how often do users make errors while using the system, how serious are these errors, and how do users recover from these errors?
- **Subjective satisfaction**: how much does the user like using the system?

2.1.3.6 User Interface/Human Machine Interface (HMI)

The user interface, or Human Machine Interface (HMI), is the aggregate of means by which users interact with a system, which could be a particular machine, device, computer application or another complex tool. The user interface provides means of:

- **Input**, allowing the users to manipulate a system; or
- **Output**, allowing the system to produce the effects of the users' manipulation.

The design of a user interface affects the amount of effort the user must spend to provide input for the system and to interpret the output of the system, and how much effort it takes to learn how to do this. Usability is the degree to which the design of a particular user interface takes into account the human psychology and physiology of the users, and makes the process of using the system effective, efficient and satisfying (based on [67]).

2.1.3.7 Graphical User Interface (GUI)

A Graphical User Interface (GUI) is a type of user interface that allows people to interact with a system — mostly electronic devices like computers, hand held devices (MP3 players, portable media players, gaming devices), household appliances and office equipment. As opposed to traditional interfaces, it presents graphical icons, visual indicators or special graphical elements called "widgets". The icons are often used in conjunction with text, labels or text navigation to fully represent the information and actions available to a user. But instead of offering only text menus, or requiring typed commands, the actions are usually performed through direct manipulation of the graphical elements (based on [67]).

2.1.3.8 User-Centred Design (UCD)

User-centred design (UCD) is an approach for employing usability. It is a structured product development methodology that involves users throughout all stages of product development, in order to create a system that meets users' needs. This approach considers an organisation's business objectives and the user's needs, limitations, and preferences (based on http://usability.gov). Therefore, user-centred design actively engages end users in all stages of the design process in order to understand and address their needs [24].

2.1.4 Usability Evaluation Methods

2.1.4.1 User Evaluation

A user evaluation is the systematic inspection of a system by users accomplishing certain tasks in a controlled environment. For the PICOS project, laboratory usability tests of the PICOS software are an integral part of the assessment of the usability of the system.

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

2.1.4.2 Focus Group

According to (http://usability.gov), a focus group is described as a moderated discussion among eight to twelve users, or potential users, of a system. A typical focus group is moderated by one discussion leader, lasts about two hours and covers a range of topics that are decided on beforehand. Furthermore, a guideline is created in advance that describes the course of the focus group.

As part of the the PICOS project, focus groups will be conducted with the major stakeholders, such as community members or service providers, in order to allow a better understanding of their needs and requirements.

2.1.4.3 Personas

Personas are a design tool based on the ideas of Alan Cooper, who is also considered to be the father of Visual Basic. In 1999, he released a book entitled "The Inmates are Running the Asylum", which is considered to be the founding work in the field of personas. According to [16], personas are “a precise descriptive model of the user, what he wishes to accomplish, and why. [… They] are based on the behaviours and motivations of real people. They represent them throughout the design process” [16]. Personas are also a detailed description of an imaginary person that embodies shared assumptions about users of a product, data regarding users of a product, or both [49].

In the PICOS project, personas can and will be used to unify the image of the users of the PICOS community software for all persons involved in the project (i.e., project members).

2.1.4.4 Usability Tests

Usability tests are the most renowned method to optimise the usability of a system. They combine a survey of a user’s interaction with the system with interviews and targeted questions. In a usability test, representative users try to do typical tasks with the system, while observers, including the development staff, watch, listen, and take notes. The system can be a web site, web application, or any other product, which does not have to be finished (http://usability.gov).

During the course of the PICOS project, usability tests will be conducted to identify usability problems, problems with the information architecture and potentials for user interface and interaction improvement of the PICOS system.

2.1.4.5 Expert Based Evaluation

In expert based evaluations, usability experts inspect systems according to certain principles. Usability inspection methods using experts are heuristic evaluation and cognitive walkthrough.

Expert based evaluations of PICOS interfaces and prototypes are an essential part of the usability evaluation of the project.

2.1.4.6 Interviews

Individual interviews typically refer to talking with one user at a time (for 30 minutes to an hour) face to face, by telephone, or with instant messaging or other computer-aided means. These interviews do not involve watching a user work. Thus, this is different from interviewing users in a usability testing session or conducting contextual interviews (http://usability.gov).

For the PICOS project, interviews will be conducted in combination with usability tests.

2.1.4.7 Community trials

Community trials are trials designed for the evaluation of lifestyle interventions that cannot be allocated to individuals.

Since PICOS is focusing on online and mobile communities, different types of communities are examined (as such) on certain aspects of the PICOS system. Therefore, requirements can be detected and feedback to existing prototypes can be given.

2.2 Electronic and mobile communications terminology

Georg Kramer (TMO), Tobias Kölsch (TMO), Cathleen Simons (ATOS) and Eleni Kosta (ICRI-K.U.Leuven)

The objective of the PICOS 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 are delivered by multiple communication service providers. In the context of the PICOS project, mobile communication services are defined as services that can be used from mobile terminals as well as from fixed line terminals.

One of the principle goals of PICOS is to ensure that community-supporting applications are reachable over the fixed Internet, and via mobile communications service providers. Therefore, besides the Internet based services offered by Internet service providers, a variety of community services require the involvement of a mobile communications service provider. Given the importance of electronic (including the Internet) and mobile communications, this chapter will present the basic terminology which has been developed by the TMO team and that will be used in the PICOS deliverables. This terminology will prevail in the private communication between the partners, who will aim to achieve a common understanding of this field.

2.2.1 Ad hoc Network

An ad hoc network is a network connection method (most often wireless) where the connection is established for the duration of one session and requires no base station [67].

2.2.2 Anonymous Peer to Peer (P2P)

An anonymous peer to peer (P2P) computer network is a particular type of peer-to-peer network in which the users are anonymous, or are given pseudonymous by default. The primary difference between regular and anonymous networks is in the routing method of their respective network architectures. These networks (both regular and anonymous) allow the unfettered free flow of information, legal or otherwise [67].

2.2.3 Application Provider

An application provider is characterised as an undertaking that provides some kind of value added service to a customer via his or her customer device. Often, an application provider combines enabling services to create more enhanced new services. For example, an application provider could take a customer's location from the mobile operator, retrieve a list of pharmacies from a pharmacy database, get a local map, and send a customer notification using the mobile operator's multimedia messaging service.

In context of PICOS, the terms "application provider" and "service provider" (see section 2.1.2.13 "(Community) Service Provider") are interchangeable.

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

2.2.4 Authentication Tool

An authentication tool is a means used to confirm that a person in fact is who he or she claims to be. In the context of PICOS this could, for example, be a digital certificate, but also a token or username/password combination [39].

2.2.5 Call

The term 'call', when used in the context intended by the EU *ePrivacy Directive*, refers specifically to a connection established by means of a publicly available telephone service between two parties, that allows communication between one or both parties to take place in real time (Art. 2e [4]). In a more general sense, the term refers to the act of 'calling out', or refers to a call-sign that identifies the originator of the communication or connection.

PICOS is concerned with mobile communities, which may be provided by a public mobile telephone operator, so recognising that the Directive places obligation on the operator to guarantee privacy means that PICOS could draw on this guarantee or may be expected to provide a similar guarantee.

2.2.6 CAPTCHA

A CAPTCHA is a type of challenge-response test used in computing to determine that the response is not generated by a computer. A common type of CAPTCHA requires the user to correctly type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. It is a contrived acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart", trademarked by Carnegie Mellon University [67].

2.2.7 Cipher text

Cipher text is encrypted text. This is different to plaintext, which is text before encryption [7].

2.2.8 Commercial Service

A commercial service is a service that has to be paid for by the end-customer. Payment may follow different models depending on the service, the relationship between the service provider and user, and the amount of money that is charged per service unit.

2.2.9 Communication

A Communication is any information exchanged or conveyed between a finite number of parties.

2.2.10 Context Awareness

Context awareness is the taking into account of an actual context (e.g., for a service), which can consist of location, presence information, current time, "buddy list" information, or other temporal information related to the Customer and his or her current service environment.

For example, a taxi driver on tour do not want to be disturbed by further orders and sets his presence status accordingly, so that the platform does not forward such requests.

2.2.11 Customer

A Customer is an end-user that has a Customer Device.

2.2.12 Customer Device

A Customer device is a computer or mobile phone that is used to communicate and use online services. The device contains two unique identifiers that are visible to the Mobile Network Operator, the International Mobile Subscriber Identity (IMSI), which uniquely identifies the customer contract and the International Mobile Equipment Identity (IMEI), which uniquely identifies the Customer device.

2.2.13 Customer Identity

A customer identity is a unique handle that identifies a Customer. In the PICOS context, this could be the IMSI.

2.2.14 Customer Notification

A Customer notification is a message that is actively pushed to the Customer by some means (e.g., SMS, WAP Push, Push E-Mail). When the context is clear, it can also simply be called notification.

2.2.15 Customer Service

A Customer service is a value that is delivered by an Application Provider to the Customer through his or her Customer device.

2.2.16 Electronic Communications Network

Electronic communications networks are transmission systems and, where applicable, switching or routing equipment and other resources, that permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems (to the extent that they are used for the purpose of transmitting signals), networks used for radio and television broadcasting, and cable television networks (irrespective of the type of information conveyed)(Art. 2a [3]). In the context of PICOS, the main electronic communications networks will be the Internet and the network of the mobile operator.

2.2.17 Electronic Communications Service

The term “electronic communications service” means a service normally provided for remuneration, and which consists wholly or mainly in the conveyance of signals on electronic communications networks (including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services). The term does not include information society services, as defined in Article 1 of Directive 98/34/EC. Information society services do not consist wholly or mainly of the conveyance of signals on electronic communications networks (Art. 2c [3]). Electronic communication services can be voice telephony, access to the Internet, electronic mail, et cetera.

2.2.18 Electronic Mail (E-Mail)

Electronic mail is any text, voice, sound or image message sent over a public communications network that can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient (Art. 2h [4]).

2.2.19 Enabling Service

An enabling service is a service that is not in itself targeted at the Customer, but is still thought to provide additional information or feature to some Application Provider who wants to provide a Customer Service built on top of the service.

LBS is a typical enabling service, where the location information about a customer is used to provide a value added service, e.g. the nearest pharmacy.

2.2.20 GSM, GPRS, UMTS

GSM, GPRS and UMTS are different generations of mobile communication standards. GSM provides circuit switch connections (dedicated one-to-one connections), GPRS enhances GSM by packet oriented connections with the feasibility for a mobile phone to be always on, and UMTS is the third generation standard with major enhancements in data transmission speed.

2.2.21 International Mobile Equipment Identity (IMEI)

International Mobile Equipment Identity or IMEI is a number unique to every GSM and UMTS mobile phone. It is usually found printed on the phone underneath the battery.

The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to "ban" the phone using its IMEI number. This renders the phone useless, regardless of whether the phone's SIM is changed [67].

2.2.22 International Mobile Subscriber Identity (IMSI)

An International Mobile Subscriber Identity or IMSI is a unique number associated with all GSM and UMTS network mobile phone users. It is stored in the SIM inside the phone and is sent by the phone to the network. It is also used to acquire other details of the mobile in the Home Location Register (HLR) or as locally copied in the Visitor Location Register. In order to avoid the subscriber being identified and tracked by eavesdroppers on the radio interface, the IMSI is sent as rarely as possible and a randomly-generated "Temporary Mobile Subscriber Identity" (TMSI) is sent instead [67].

In the context of PICOS, the IMSI or MSISDN is used to identify a customer.

2.2.23 Intelligent Network (IN)

The Intelligent Network is a concept where nodes in a mobile network can be programmed to handle voice calls in a specific and flexible way (e.g., so as to provide a virtual private number plan, to charge calls in a specific way, to change the source or destination number, and so on).

2.2.24 Java 2 Mobile Edition (J2ME)

The Java 2 Mobile Edition is a stripped version of the standard Java environment, adapted to mobile phones to provide an environment to run mobile applications.

2.2.25 Location Based Service (LBS)

A Location Based Service is a Customer Service that uses the Customer's location information to provide some kind of Context Awareness. In the context of PICOS, the taxi drivers could be informed about traffic jams on their way.

2.2.26 LBS pull service

An LBS pull service is a service that uses the current location of a Customer, and where the usage and the localisation are initiated by the Customer him or herself, such as, for example, with a pharmacy search.

2.2.27 LBS push service

An LBS push service is a service that uses the current location of a Customer, and where the service is subscribed to once by the Customer and the localisation is initiated by a different party, such as a location tracking service for pollen warnings.

2.2.28 Location data

Location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (Art. 2c [4]).

2.2.29 Mesh Network

A mesh network is a network in which all nodes are interconnected, either directly or indirectly [67].

2.2.30 Mobile Communication Services

For the PICOS project, mobile communication services are defined as services that can be used from mobile terminals as well as from fixed line terminals.

2.2.31 Mobile Network Operator (MNO)

A Mobile Network Operator is a company that has the radio communication infrastructure that is used by Customers to communicate and use Customer Services.

2.2.32 Mobile Subscriber Integrated Services Digital Network Number (MSISDN)

The MSISDN (Mobile Subscriber Integrated Services Digital Network Number) is the phone number that is visible to the Customer.

2.2.33 Network Authentication

Network authentication is a technical method to determine a Customer Identity that is based on the mobile network by, for example, resolving the MSISDN from the IP address of an online session.

2.2.34 Next Generation Network

Next Generation Network is a packet-based network where service control intelligence is separated from transport elements like routers or switches. The control intelligence is used to support all types of services like data, multimedia, voice telephony and broadband. Functional capabilities are not coupled with physical network elements.

2.2.35 Peer to Peer (P2P)

P2P is an abbreviation for Peer-To-Peer, a direct communication between two equal parties without an outstanding central server in between.

2.2.36 Policy Decision Point (PDP)

The Policy Decision Point is a function that evaluates privacy policies to answer whether the data delivery is allowed or denied. For example, a customer wants to be located only during business hours and configures his privacy settings accordingly. Any requests to his location information are checked by the PDP and denied during leisure time.

2.2.37 Policy Enforcement Point (PEP)

The Policy Enforcement Point is a control point that enforces the policy decision made by the PDP.

2.2.38 Presence Information

Presence information is one or more attributes that determines the reachability of a Customer, such as whether the customer is online, offline, busy, or reachable by phone.

2.2.39 Privacy Rights Management

Privacy Rights Management concerns the protection of personal data using a method based on the digital technology used to protect copyrights registered on data carriers (Digital Rights Management). The aim is to provide personal data with an inextricable digital label containing the privacy preferences of a user [39].

2.2.40 Public Communications Network

A public communications network is an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services (Art. 2d [3]).

2.2.41 Public Key Infrastructure (PKI)

Public key infrastructure (PKI) is a system of digital certificates, Certification Authorities, and other registration authorities that verify and authenticate the identity of each party involved in an Internet transaction. PKIs are currently evolving and there is not a single PKI, or even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary for

electronic commerce to become widespread. Most enterprise-scale PKI systems rely on certificate chains to establish a party's identity, as a certificate may have been issued by a certificate authority computer whose 'legitimacy' is established for such purposes by a certificate issued by a higher-level certificate authority, and so on. This produces a certificate hierarchy composed of, at a minimum, several computers, often more than one organization, and often assorted interoperating software packages from several sources [67]. A PKI enables users of a basically insecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority (http://searchsecurity.techtarget.com).

2.2.42 Public Service

Public services are services that are provided without restricting access to the service. However, the access may be limited by the availability of technology that is required to use the service.

2.2.43 Push-to-Talk (PTT)

The Push-to-Talk service is a walkie-talkie service based on the mobile network and allows instant voice communication, either one-to-one or within a group.

2.2.44 Roaming

Roaming is the situation of using a different mobile network than that of the own Mobile Network Operator, such as in the case of travelling abroad.

2.2.45 SIM card

The Subscriber Identity Module (SIM) stores the IMSI in a secure way on the mobile phone. This means for the context of PICOS, that the SIM card could be used to identify the customer (see 2.2.22).

2.2.46 Traffic data

Traffic data is any data processed for the purpose of the conveyance of a communication on an electronic communications network, or for the billing thereof. (Art. 2b [4])

2.2.47 Trusted Third Party

A Trusted Third Party delivers reliable and confidential services, such as reliable hosting services or the issuing of digital certificates (at present, the party issuing digital certificates is indicated by the term “CSP”) [39].

2.2.48 Value Added Service

A value added service is any service that 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. (Art. 2g [4])

In the context of PICOS, a value added service could be used to increase customer loyalty or to acquire/migrate customers using services provided by a different community.

2.2.49 WAP

The Wireless Application Protocol (WAP) is a set of technologies used to provide Internet content to mobile users. The content is delivered in WML (Wireless Markup Language), XHTML-MP (XML HyperText Markup Language) and other formats.

2.2.50 Wireless

The term "wireless" is generally used in relation to mobile IT equipment; it means any form of data transfer in which electromagnetic waves — rather than some form of wire — carry the signal over part, or the entire, communication path. See also GPS, handheld, mobile, Wi-Fi [24].

2.2.51 WLAN

A Wireless Location Area Network (WLAN) provides mobile Internet access.

2.3 Introductory terminology on privacy, identity management and trust

Katja Liesebach (GUF), Petr Svenda (Masaryk University), Vicente Benjumea (UMA) and Cathleen Simons (ATOS)

A principal goal of PICOS is to build a state-of-the-art platform for providing the trust, privacy and identity management aspects of community services and applications on the Internet and in mobile communication networks. This implies that the concepts of privacy, identity management and trust need to be clearly understood by the project partners in order to be able to build the PICOS architecture and develop the actual trials.

In every type of community, and especially in the three communities that are chosen as use cases in PICOS, i.e. the angling community, the taxi drivers' community and the online gaming community, some degree of identity information is required in order to ensure the participation of the user. This imposes a need for the ICT services that support a community to utilize identity management functions. It also raises fundamental questions for the community users, such as whom they can trust with their identity and other personal information, and how identity information and personal information is handled in the system.

It is important that the providers of community services are able to answer these trust and privacy questions in a manner that meets the participants' needs and complies with regulation. To do this, the design of the service provision infrastructure must have trust enablement and privacy compliance as essential characteristics. As new community-supporting services offered by communication service providers will increasingly become interoperable, this would require that provisions for trust enablement and privacy-respecting identity management also be interoperable between such communication service providers.

A new approach to identity management in community services is needed, in order to allow the trust of members of the community in other members, and in the service-provision infrastructure, the privacy of community members' personal information, the control by members of the information they share, and the interoperability of community-supporting services between communication service providers. This approach must be developed in an open manner, and requires technical advances in order to meet the requirements.

Given the significance of the terms “privacy”, “identity management” and “trust” in the context of PICOS, this chapter will try to define the relevant terminology and discuss the importance of some core concepts for PICOS. Existing research, such as the AN.ON terminology, and research conducted within the FP6 funded project PRIME, is used as a first building block in compiling a basic list of these terms.

2.3.1 Accountability

Accountability can be described as the state of bearing responsibility.

In the context of PICOS, this means that an entity is responsible for his or her actions, even if they have been carried out anonymously. Thus, in some situations, the system has the ability to discover the identity of the member that performed a given action, especially misuse. In some cases, for instance, a member’s actions may affect the reputation that such a member enjoys within the community, or even lead to the expulsion of the member from the community. This concept is closely related to non-repudiation, since a member is responsible for some action if there are some “non-repudiable” proofs that show that this member was indeed the one that performed the action in question.
The implementation of accountability is often connected with pseudonymity in that it allows the revealing of a member’s real identity when necessary, while maintaining anonymity in the normal course of events.

2.3.2 Anonymity

If a subject has anonymity it means that the subject is not identifiable within a set of subjects, which in turn is called the “anonymity set”. This means that an attacker cannot sufficiently identify the subject within such a set of subjects [47].

In the context of PICOS, anonymity refers to the property by which members of communities interact in such a way that they keep their privileges, but that their identities are unknown, and it is not possible to identify which member is actually performing a given transaction. In simple words, anonymity means that there is no sufficient correlation between a given action, and the member that performed it, for an attacker to identify the member.

2.3.3 Anonymity Set

An anonymity set is the set of all possible subjects with regard to being anonymous [47]. According to a different definition, an anonymity set is the set of all possible subjects in a given data collection context [5].

As already discussed above in section 2.3.2, anonymity is not an absolute value, but it is relative to the context where it is applied. In the context of PICOS, a member of a community, possibly anonymous, is allowed to carry out a given action, if it has enough privileges to do so (if it is member of the community and has a given reputation, has paid, et cetera), and so, the member is anonymous with respect to all other members that also enjoy the disclosed privileges, and could, therefore, carry out such a given action.

With respect to addressees, the anonymity set consists of the subjects who might be addressed. It should also be noted that anonymity is measured with respect to a set of observers, which are able to extract information depending on their view of the transaction, and the information they hold.

2.3.4 Anonymous

Being anonymous is the state of not being identifiable.

In the context of PICOS, a transaction is anonymous if it is not possible to identify which member of the community carried it out. Additionally, a member is anonymous while carrying out a transaction if it is not possible to identify which member of the community is indeed performing the transaction.

2.3.5 Certificate

A certificate is a digitally signed statement which authenticates a public key as belonging to the holder of a given pseudonym or civil identity, and can also include a period of validity [22]. The certificate is usually issued by an authority, the Certification Authority, and it is usually a signed statement that binds a public key with an identity, where the holder of the certificate (and owner of the identity) is the one that knows the corresponding private key.

In the context of pseudonymity, the certificate can also bind a public key with a pseudonym, in such a way that the one that knows the corresponding private key is the right holder of the pseudonym.

In the context of group signatures and alike, the certificate can bind a public key with an abstract concept (such as being member of a community), in such a way that all entities that can be authenticated with the public key are seen as the right holders of the abstract concept. Furthermore, in group signatures, many different private keys can be verified with the same public key of the group. In this context, the members of the group are anonymous within the group, as already discussed above, in section 2.3.2.

2.3.6 Civil Identity

A civil identity is the identity attributed to a person by a State (represented, for instance, by the social security number, or the combination of name, date of birth, and location of birth, et cetera) [47].

A civil identity can be also used in the online world by means of tools that convey the suitable information, such as, for example, a digital public key certificate binding one's name and passport number to a public key and issued by the government (in this case, the certificate binds the civil identity with a public key to enable digital authentication). If the certificate has been issued by a non-legally-binding authority, then the certificate does not entail legal responsibilities. It is important to remark that the civil identity, however, entails responsibilities (both in the offline and online worlds).

In the context of PICOS, the civil identity is the real identity of each member of a community, which is used in the same way as in the offline world and uniquely identifies the person. Every user has legal responsibilities attached to civil identity.

2.3.7 Convertibility

Convertibility is the transferability of attributes of one pseudonym to another [47].

Some solutions to provide anonymity are based on pseudonyms. However, several transactions performed under the same pseudonym could possibly be correlated, a fact that diminishes privacy. Thus, convertibility is a property by which some privileges can be transferred to be used under different pseudonyms, and therefore provides a way to break correlations in the use of privileges under different pseudonyms.

2.3.8 Credential

Credentials are evidence or testimonials concerning rights to actions or a reputation made by one entity (issuer) about another entity (user) [5]. According to the definition by Chaum [13], credentials are statements concerning an individual that are issued by organisations, and are, in general, shown to other organisations.

In the context of PICOS, a credential is a signed statement from a Certification Authority that binds a set of privileges (attributes) with a specific holder. These privileges may refer to community membership, reputation, et cetera, depending on the context of use.

2.3.9 Decentralised Trust

"Decentralised trust" is a term used to refer to the situation when trust is not maintained in a centralised way, but rather by the peers itself. An example of decentralised trust could be a reputation system that stores a reputation score on each peer separately, and not in a centralised database.

2.3.10 Delegation

Delegation is the conveyance of a privilege from one entity that holds such privilege, to another entity [29].

In the context of PICOS, at this stage it is still not clear if the delegation of privileges will be suitable or supported. Further research conducted in the course of the project will, however give a solution to this issue.

2.3.11 Dependability

Dependability is the trustworthiness of a computing system, which allows reliance to be justifiably placed on the service it delivers. Dependability comprises of, as special cases, attributes like reliability, availability, safety, integrity and maintainability. It relates to the identification and integration of approaches, methods and techniques for specifying, designing, building, assessing, validating, operating and maintaining computer systems, in which faults are considered as natural, anticipated events, and, thus, can be tolerated (http://www.dependability.org).

According to another definition given by [8], the dependability of a computing system is the ability to deliver services that can justifiably be trusted, or the system property that integrates such attributes as reliability, availability, safety, security and maintainability.

2.3.12 Digital Identity

Digital identity is the attribution of attributes to an individual person, which are immediately operationally accessible by technical means [47].

In the context of PICOS, the digital identity identifies a user in a technological system and provides the mechanisms to authenticate the real holder of the specified identity.

2.3.13 Digital Pseudonym

A digital pseudonym is a unique identifier suitable to be used to authenticate the holder's Items of Interest [47].

In the context of PICOS, at this stage it is not clear whether pseudonyms will be used to support anonymity. In any case, however, pseudonyms can be used to conceal the identity of the members of communities in that members act by means of their pseudonyms, holding their privileges and reputation. Anonymity is provided when the correlation between the member's identity and its pseudonym is not known *a priori*. This scheme, however suffers from the problem that all transactions carried out by using the same pseudonym can be correlated. On the contrary, systems based on pseudonyms make reputation easier to manage.

In this context, the word "digital" means that the pseudonym is managed using a mechanism that allows only the right holder of the pseudonym to be authenticated as such.

2.3.14 End Entity

An end entity is either: a public key certificate subject that uses its private key for purposes other than signing certificates; an attribute certificate holder that uses its attributes to gain access to a resource; or an entity that is a relying party [29].

In the context of PICOS, a member of a community is an end entity.

2.3.15 Entitlement Assessment

Entitlement assessment is the guarantee of access to the process of documenting skills and attitudes.

2.3.16 Fair Information Practices (FIP)

"Fair Information Practices" is a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy [7]. Generally, these practices can be said to be based upon the Fairness Principle according to which personal data must be processed fairly and lawfully (Art. 6a [1]). For more details on the Fairness Principle, see section 2.4.12 below.

2.3.17 False Identity

A false identity can either be a fictitious (i.e., invented) identity, or an existing (i.e., genuine) one that has been altered to create a fictitious identity.

2.3.18 Group Pseudonym

A group pseudonym refers to a set of holders, and may induce an anonymity set [47].

In the context of PICOS, it is not yet decided at this early stage of the project if this kind of pseudonym will be used. In any case, a group pseudonym is a pseudonym that is shared among a group of users. If group signatures are used, for instance, all members of a group can share the same pseudonym, which can be based on the definition of the group. Under the denomination of "Group of Anglers from Bristol", for example, a set of members of a community might be grouped and might define an anonymity set on its own. In this case, the members of the group are able to anonymously prove their membership, by being anonymously authenticated as members of this community.

2.3.19 Identical

The term "identical" describes the state of having all possible properties in common [5].

2.3.20 Identifiability

Identifiability of a subject, from an attacker's point of view, means that the attacker can sufficiently identify the subject within a set of subjects, the identifiability set [47]. [5] defines identifiability as the possibility of being individualised within such a set.

Identifiability is the contrary term of anonymity.

2.3.21 Identifiability set

An identifiability set is the set of all possible subjects that can be identified [47].

Identifiability set is the contrary term of anonymity set.

2.3.22 Identifier

An identifier is a symbol, or a set of symbols, of a subject that refers to a concept allowing it to be distinguished from others in a specific scope. An identifier could be, for instance, a name which is imposed by a third party [22].

In the context of PICOS, an identifier allows on to denominate, for instance, an entity (such as a member of community, service provider or authority) or a concept (such as a property or an attribute) in a unique manner in a specific context. It is a general term that may be used in many different contexts.

2.3.23 Identity

An identity is any subset of attributes of an individual subject that sufficiently identifies this individual subject within any set of subjects [47]. According to [22], an identity is a symbol or a set of symbols referring to an entity, i.e., a subject or an object, which distinguishes it from others in a specific scope. The identity could be a name imposed by a third party and is unique in a specific namespace.

In the context of PICOS, an identity is the symbol (or set of symbols) that uniquely identifies an entity within a specific scope. For instance, an identity can be used to uniquely identify a member within a community. The use of this identity may entail legal responsibilities.

2.3.24 Identity Life-cycle Management

Identity life-cycle management concerns the process and technologies for provisioning, deprovisioning, managing, and synchronising digital identities while complying with governing policies. The success of identity and access management will rely mostly on how efficiently the digital identity life-cycle can be managed. Identity life-cycle management services are used for security principal creation, attributes management, synchronisation, aggregation, and deletion. In addition, these actions must be accomplished securely with a thorough audit trail.

2.3.25 Identity Management

Identity management is the managing of various partial identities (usually denoted by pseudonyms) of an individual subject, i.e., the administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role [47].

In the context of PICOS, identity management is the management of the several identities (and privacy preferences) that an entity may own, depending on the context of use. For example, a user may belong to several online communities, and thus, depending on the context of use (community), the system can help the user in managing his or her identity, and in providing the necessary mechanisms to soundly create and use these identities in different contexts.

2.3.26 Informational Privacy

Information privacy can be defined as the self-determination of what information is known about a person and how it is used [5].

It refers to how personal data are collected, stored, disseminated, correlated and used by technological means. In some contexts, informational privacy also refers to the entities that are allowed to access some kinds of personal data. In the context of PICOS, it is necessary to specify what kind of personal data has to be collected from community members, who manages them and in which way, whom and under what conditions they are disclosed to, et cetera.

2.3.27 Information Technology

Information Technology includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organisation, storage and retrieval of information [iso.org].

2.3.28 Interpersonal Trust

Interpersonal Trust is the confidence in the intention and ability of other community members and providers. See section 2.3.66 below for the more general term of “trust”.

In this context, trust is a state of mind that enables its possessor to be willing to make him or herself vulnerable to another person — that is, to rely on another person, despite a positive risk that the latter will act in a way that can harm the possessor of the trust. Trust is a cognitive assessment tool and is formed, maintained and eroded differently in different types of relationships [27].

As defined in (http://www.Interpersonaltrust.com) interpersonal trust is the perception you have that the other person will not intentionally or unintentionally do anything that harms your interests. It is also the feeling that you can depend upon that other person to meet your expectations when you are not able to control or monitor the other person’s behaviour. Interpersonal trust always involves one person making him or herself vulnerable to another person’s behaviour. Usually, what you get from the expected behaviour is not as valuable as what you could lose, if your trust is violated. Trust is violated when the trusted person does not behave in a way that you expected, or behaves in an unexpected manner.

2.3.29 Linkability

The linkability of two or more items of interest (IOIs) such as subjects, messages or actions, from an attacker’s perspective, means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not [47].

Linkability is usually an undesirable property in privacy contexts, since in many circumstances it diminishes the level of privacy attained. For example, if it is possible to establish a link between the

identity of a member of the community and a given transaction, then anonymity cannot be preserved for this transaction. Also, if it is possible to establish a link between different transactions as being performed by the same anonymous member, then the privacy of the member that carried them out diminishes. This is because it is possible to establish a user profile based on this link that could even establish a link between the transactions and the identity of the user, which would break his or her anonymity. However, in some restricted scenarios, linkability may be a useful property. If pseudonyms are used, all transactions under the same pseudonym are linkable and allow the establishment of a reputation level for the pseudonym. Also, in anonymous systems, it may be possible to (conditionally) link (according to the user's will) an anonymous transaction with an anonymous reputation. Also, the linking of a given proof of different attributes to the same anonymous user provides robustness against anonymous user coalition attacks.

Linkability is the negation of unlinkability [47].

2.3.30 Multi-Property Features

Multi-Property features appear in case of anonymous/pseudonymous proof of simultaneous properties, if the scheme guarantees that all these properties do indeed belong to the same real (single) anonymous/pseudonymous entity.

2.3.31 Non-repudiable Action

An action is characterised as non-repudiable if the entity that performed it cannot deny that it did it, even if it carried it out anonymously (pseudonymously).

2.3.32 Partial Identity

A partial identity represents a subject in a specific context or role [47]. A partial identity is, alternatively, any set of data that characterises an individual to some degree within an anonymity set [5].

In the context of PICOS, a user may own many different partial identities, such that each one of them uniquely identifies the user within a given community.

2.3.33 Person Pseudonym

A person pseudonym is a substitute or alias for a data subject's civil identity.

2.3.34 Privacy

Privacy is the right of individuals to protect, safeguard and control the access, storage, distribution and use of information about themselves.

Solove [55] identified four categories of privacy violations from the perspective of law:

- **Information Collection**: surveillance and interrogation.
- **Information Processing**: aggregation, identification, insecurity, secondary use and exclusion.
- **Information dissemination**: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion.
- **Invasion**: intrusion and decisional interference.

2.3.35 Privacy-enhancing Identity Management

Given the restrictions on a set of applications, identity management is privacy-enhancing if it sufficiently preserves unlinkability (as seen by an attacker) between the partial identities of a person required by the applications [47].

Identity management is perfectly privacy-enhancing if it perfectly preserves the unlinkability between partial identities, i.e., by choosing the pseudonyms (and their authorisations) denoting the partial identities carefully, it maintains unlinkability between these partial identities from an attacker's perspective sot that it is as if the attacker is given the attributes with all pseudonyms omitted [47].

In the context of PICOS, identity management consists of managing the multiple identities that a user may own in different context of use, such as different communities where the user belongs to. This identity management is *privacy-enhancing* if it also considers the privacy of users, tries to keep the unlinkability of these partial identities for different communities, or even tries to keep multiple transactions of the same member within a given community unlinkable.

2.3.36 Privacy-Enhancing Technology (PET)

"Privacy Enhancing Technology" (PET) is a general term for a set of computer tools, applications and mechanisms that — when integrated in online services or applications, or when used in conjunction with such services or applications — allow online users to protect the privacy of their personally identifiable information (PII) provided to, and handled by, such services or applications [67].

PETs is a collection of information and communication technologies that strengthens the protection of individuals' private lives in an information system by preventing unnecessary or unlawful processing of personal data, or by offering tools and controls to enhance the individual's control over his or her personal data. A coherent system of ICT measures protects privacy by eliminating or reducing personal data, or by preventing unnecessary and/or undesired processing of personal data, without losing the functionality of the information system. The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. Examples include automatic anonymisation of data, encryption tools, cookie-cutters and P3P [20].

2.3.37 Privacy Preferences

Privacy preferences are prepared by a sharing party to express how personal information should be handled.

In the context of PICOS, the users can establish their preferences regarding their privacy (and disclosure of personal data) depending on the context of use. Therefore, they may specify what kind of information should be disclosed in order to become member of a community, and also what kind of information should be disclosed for the performance of a given transaction within a community.

2.3.38 Profile

A profile is a set of assertions (true or untrue facts), including behaviours, collected with the intention of identifying a person or set of persons [5].

In the context of PICOS, a profile is composed of all the information that can be collected and correlated as belonging to a single subject, even if its identity is unknown. These user profiles can be

used to extract very valuable information about users' preferences and behaviours. The creation of profiles is a threat to privacy, as the more the amount of information that can be collected and correlated, the more the privacy of users is threatened. In other words, profiling reduces the anonymity set for the collected information, and can even end up by identifying the real user. Thus, unlinkability among transactions is the most valuable mechanism to avoid the creation of user profiles. The use of pseudonyms is considered as a drawback in this scope, since they usually allow the correlation, to a greater or lesser extent, between different transactions being carried out by the same (unknown) individual.

2.3.39 Pseudonym

A pseudonym is an identifier for a subject other than one of the subject's real names [47]. According to [5], a pseudonym is an identifier of a subject other than the subject's civil identity.

In the context of PICOS, see the discussion above in section 2.3.13 on digital pseudonyms.

2.3.40 Pseudonymity

Pseudonymity is the use of pseudonyms as identifiers [47]. Pseudonymity identifies a holder, that is, one or more human beings who possess, but do not disclose, their true names [67].

In the context of PICOS, the community members may use identifiers chosen by themselves (nicknames), or (possibly temporal) identifiers assigned by the technological platform in order to achieve pseudonymity.

2.3.41 Pseudonymisation

Pseudonymisation is the process of replacing identifying characteristics with a label or a pseudonym [47].

When some information related to an identified individual (i.e., personal data) is known, pseudonymisation consists of replacing the identifying information with a pseudonym. This mechanism is also applied to databases, where the identifying information is replaced by pseudonyms.

2.3.42 Pseudonymous

A subject is pseudonymous if a pseudonym is used as an identifier instead of one or more of its real names [47].

2.3.43 Initially Non-public Pseudonym

The linking between an initially non-public pseudonym and a subject may be known by certain parties, but is not public, at least initially. For example, a bank account where the bank can look up the linking may serve as a non-public pseudonym. For some specific non-public pseudonyms, Certification Authorities could reveal the identity of the holder in the case of abuse [47].

2.3.44 Initially Unlinkable Pseudonym

The linking between an initially unlinkable pseudonym and a subject is, at least initially, not known to anybody with the possible exception of the holder him or herself. Examples of unlinkable pseudonyms

are (non-public) biometrics, like DNA information, unless they are stored in databases that link to a subject [47].

2.3.45 Public Pseudonym

The linking between a public pseudonym and a subject may be publicly known from the very beginning. The linking could, for instance, be listed in public directories such as a phone number entry in combination with its owner [47].

2.3.46 RAS

Reliability, availability, and serviceability (RAS) are considered to be important aspects of the design of any system. In theory, a reliable product should be totally free of technical errors [7].

2.3.47 Relationship Pseudonym

A relationship pseudonym is a pseudonym that is used with regard to a specific communication partner such as, for example, distinct nicknames for different communication partners.

In the context of PICOS, a user could own many different pseudonyms, each one for each community to which he or she belongs.

2.3.48 Reputation

The reputation of someone or something is the opinion that people have about what they are like, especially about how “good” they are.

Reputations in social community systems usually evolve with user action within the system, starting either from a pre-established reputation in the real world or from a neutral level. The technological platform should provide reasonable protection against an unjustified increase or decrease of user reputation that has the intention of either harming an honest user or increasing the reputation of a dishonest one.

2.3.49 Reputation Management

Reputation management is the process of tracking an entity’s actions and other entities’ opinions about those actions; reporting on those actions and opinions; and reacting to that report to create a feedback loop [67].

In the context of PICOS, reputation management is the mechanism that manages and supports the assignment of initial reputations to members of communities, and how this evolves along its lifetime within the community. Note that this reputation management system must be in concordance with the privacy mechanism provided by PICOS.

2.3.50 Reputation Score

A reputation score is the value or the set of values that captures how the user is perceived by other community members with respect to specific characteristics, like credibility or the ability to perform a certain task.

In the context of the PICOS project, the reputation score should capture characteristics like, for example, the ability to keep an exact fishing location secret or the trustworthiness of the stated sizes of catch fishes (for anglers); or the ability to communicate with a passenger, the condition of taxi cars, or time reliability (for taxi drivers).

Furthermore, when a member of a community anonymously posts some information to be shared with other members of the community, the reputation score associated with the post (and consequently, with the member that issued the post) is a measure of the trustworthiness of the information posted. This reputation score influences the level of trust that members of communities assign to this kind of anonymously posted information.

2.3.51 Reversible Anonymity/pseudonymity

Reversible anonymity/pseudonymity is a property by which it is possible, in an indirect way, to identify the user that carried out a given anonymous/pseudonymous transaction. In order for the process to be done with fairness, a Trusted Third Party (TTP) must be involved.

2.3.52 Revocable (Anonymous/pseudonymous) Privilege

A revocable (anonymous/pseudonymous) privilege is a property by which it is possible to revoke a given privilege for a given entity, even though the entity is able to anonymously/pseudonymously prove the privilege.

2.3.53 Risk

Risk is the exposure to the consequence of uncertainty [67].

2.3.54 Role Pseudonym

A role pseudonym is a pseudonym that is chosen for a use in a specific role (e.g., as a patient or customer).

In the context of PICOS, a user can own many different pseudonyms, each one for each role that he or she plays within the community to which he or she belongs.

2.3.55 Role Specification Certificate

A role specification certificate is a certificate that contains the assignment of privileges to a role [29].

2.3.56 Role-Relationship Pseudonym

A role-relationship pseudonym is a pseudonym that is used for a specific combination of a role and communication partner.

2.3.57 Safety

According to the *Compact Oxford English Dictionary*, safety is the condition of being safe (i.e., protected from danger or risk). A broader definition describes safety as the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event that could be considered non-desirable [67]. The system safety concept focuses on the

application of systems engineering and systems management to the process of hazard, safety and risk analysis (http://www.system-safety.org/).

2.3.58 Social Trust

Social trust is trust which arises through social mechanisms.

In the PICOS context, social mechanisms may differ depending on the target community; social trust can vary from personal trust established in real world (in the scenario of taxi drivers) to the establishment of social trust in a completely virtual environment (as in the case of online gaming).

2.3.59 Spatial Privacy

Spatial privacy is the self-determination of information entering a person's private space [5].

2.3.60 Technological Trust

Technological trust is the trust that arises through technological means, as opposed to social mechanisms [5].

2.3.61 Traceability

Traceability is the ability to gather information about a person or organisation without their knowledge [7]. In online communities, it is possible to gather information about the user and relay it to advertisers or other interested parties. Traceability requires the establishment of an unbroken chain of comparisons to stated references [42]. It can also be defined as the ability to track down the originator of an action, and it can be seen as the flipside idea to "anonymity" [14].

2.3.62 Traceable Anonymity/pseudonymity

Traceable anonymity/pseudonymity is a property by which it is possible to identify (by some indirect way), within a set, which anonymous/pseudonymous transactions were carried out by a given entity. It is done with fairness if a Trusted Third Party (TTP) is involved in the process.

2.3.63 Transaction Pseudonym

A transaction pseudonym is a pseudonym that is used for a specific transaction, meaning that a different pseudonym is used for each transaction [22].

2.3.64 Transferability (and Non-transferability)

For the transferability of attributes, see section 2.3.7 above on "Convertibility".

The transferability of pseudonyms is when a pseudonym can be transferred from one holder to another [47].

The term "transferability of attributes" refers to the ability to transfer the ownership of some attributes from one pseudonym to another, and is a widely used means to support the unlinkability of transactions by a user among organisations. Among others, the system created by [11] relies on this property.

Non-transferability of pseudonyms (and also of privileges) is an important feature that guarantees that privileges can only be enjoyed (used) by the proper holder of the privilege/pseudonym. For example, a system could incorporate some mechanisms to avoid the lending of privileges, and also the joining of privileges from different users.

2.3.65 Trust

Trust is "a person's expectation that an interaction partner is able and willing to behave promotively towards the person, even when the interaction partner is free to choose among alternative behaviors that could lead to negative consequences for the person. The degree of trust can be said to be higher the stronger the individual holds this expectation" [35]. Trust represents the expectation that the participants will enforce the rules defined in the community specification (or doctrine), and that the membership of the community will be governed by clearly defined constraints [32]. In other words, trust should be seen as "a generalized expectancy that the word, promise, oral or written statement of another individual or group can be relied on" [52].

Trust has been studied extensively in a number of disciplines. For instance, personality psychology focuses on trust as an individual characteristic, while social psychology focuses on the dynamics of trust between individuals. Economics and marketing look at trust in the context of commercial exchanges and transactions. Despite the multidimensional character of trust, however, the different conceptions all share common elements [18]. Generally, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. This trust may apply only for some specific function. The key role of trust in this framework is to describe the relationship between an authenticating entity and an authority; an entity should be certain that it can trust the authority to create only valid and reliable certificates [29].

Trust, from a technical point of view, is defined in section 2.6.9 below. As it is a core concept in the PICOS project, this definition should be read in order together with the one under 2.6.9 in order to understand its complex nature.

2.3.66 Trust Guidelines

Trust guidelines are guidelines covering the development of trustworthy ICT-mediated services: education, experimentation, restitution, guarantees, control, openness (http://trustguide.org.uk). They are also seen as a measure of how a member of a group is trusted by the other members [67].

2.3.67 Undetectability

Undetectability of an item of interest (IoI) such as a subject, message, event or action, from an attacker's point of view, means that the attacker cannot sufficiently distinguish whether the IoI exists or not [47].

In the PICOS context, such a property may be useful in scenarios where a community member does not like to reveal that he or she is sharing something (an IoI) with another member. In the online gaming scenario, in some instances, sharing means an existing relationship that spies or informants like to hide. Undetectability can also be of interest in the taxi scenario as well, where information about existing relationships can be of a competitive advantage to a rival taxi company.

2.3.68 Unlinkability

The unlinkability of two or more items of interest (IoIs), from an attacker's perspective, means that within the system (comprising these and possible other items), the attacker cannot sufficiently distinguish whether these IoIs are related or not [47]. According to [5], the unlinkability of two or more IoIs means that, within this system, these items are no more or less related than what is known according to *a priori* knowledge. Unlinkability is a very important concept, and it is the main mechanism to support privacy in technological systems, in that the unlinkability between an identified user and their actions guarantees their anonymity, and unlinkability among the actions themselves avoids profiling.

2.3.69 Unobservability

Unobservability of an item of interest (IoI) means (i) the undetectability of the IoI with regard to all not-involved subjects, and (ii) the anonymity of the subjects involved in the IoI, even with regard to the other subjects involved in that IoI [47]. [5] defines unobservability as the state of a member of an anonymity set that it is indistinguishable from any IoI at all.

In the PICOS context, see also the discussion and scenarios in section 2.3.67 above on undetectability.

2.3.70 Virtual Identity

The term "virtual identity" is sometimes used to mean digital identity or digital partial identity. However, due to the connotation with "unreal, non-existent, seeming", the term mainly applies to characters in a MUD (Multi User Dungeon) or MMORPG (Massively Multiplayer Online Role Playing Games), or to avatars [47].

2.4 Legal terms regarding data protection and identity management

Eleni Kosta (ICRI-K.U.Leuven) and Cathleen Simons (ATOS)

The principal objective of the PICOS project is to develop an open, privacy-respecting, trust-enabling identity management platform that supports the provision of community services by mobile communication service providers and the carrying out of marketing activities by third party sponsors/advertisers. The successful functionality of the PICOS platform will only be achieved when information about the users (or other entities) is collected and processed to the ends of PICOS. The processing of personal data in the platform entails the application of the European legal framework on data protection. The detailed requirements that need to be met in each specific scenario that will be served by PICOS will be discussed both in the PICOS D2.3 Contextual Framework Deliverable and in the PICOS D2.4 Requirements Deliverable. In this section, the basic principles that apply to the processing of personal data will be described, in order to assist in the creation of a common understanding between the project partners, beginning from the very early stages of the project. Moreover, a few more legal terms with specific interest for the PICOS project are also described.

2.4.1 Advanced Electronic Signature

An advanced electronic signature is an electronic signature that complies with a number of additional requirements. It should be: (1) uniquely linked to the signatory, (2) capable of identifying the

signatory, (3) created using means that the signatory can maintain under his or her sole control, and (4) usable to verify the integrity of the signed data (Article 2.2 [2]).

2.4.2 Consent of the Data Subject

Consent of the data subject means any freely given specific and informed indication of the dat subject's wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed (Art. 2h Data Protection Directive). One of the main goals of the PICOS project is to ensure that the platforms it will create will be able to provide the user with sufficient information in order to allow him or her to give his or her informed consent regarding the processing of his or her data.

2.4.3 Conservation Principle

The conservation principle means that personal data must be kept in a form that permits identification of data subjects for no longer than what is necessary for the purposes for which the data were collected, or for which they are further processed. (Art. 6e [1]). The PICOS platform will ensure that the data will be deleted, after the purpose for which they were collected, is fulfilled.

2.4.4 Controller

A controller (or data controller) is the natural or legal person, public authority, agency or any other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations, the controller, or the specific criteria for its nomination, may be designated by national or Community law (Art. 2d [1]). The problem of defining the controller of the data in new telecommunications networks has already been identified by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe:

> *Nowadays […] this model in which a sole person or body is responsible for determining the parameters of the automatic processing is increasingly challenged by examples to the contrary. Several actors, among which the controller or co-controllers, the processor(s) and the service provider(s) interact in the processing. As a result, data subjects might not always know whom to turn to in order to exercise their rights* [15].

Consequently, it is of seminal importance to examine and identify the data controller in the various scenarios of the PICOS project.

2.4.5 Data Minimisation Principle

The data minimisation principle means that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 6c [1]). This principle implies that the PICOS platform will be designed in a way to require the minimum amount of personal data.

2.4.6 Data Quality Principle

The data quality principle means that personal data should be accurate and, where necessary, kept up to date (Art. 6d [1]). The PICOS platform with be equipped with a functionality that checks the accuracy of the data and allows their modification in order to be kept up to date.

2.4.7 Data Recipient

A data recipient is a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether they are a third party or not. However, authorities that may receive data in the framework of a particular inquiry are not to be regarded as recipients (Art. 2g [1]). At the designing phase of the project, data recipients will be considered the partners of the PICOS consortium, to whom the data of the platform and application prototypes will be disclosed.

2.4.8 Data Subject

A data subject is a person who can be identified, directly or indirectly, and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (see art. 2.a [1]). In the framework of PICOS, data subjects are mainly the users of the PICOS platform.

2.4.9 Electronic Signature

An electronic signature is data in electronic form that are attached to or are logically associated to other electronic data, and serve as a method of authentication (Article 2.1 [2]). As already implied by the definition of electronic signatures, they can be used as a method of authentication in the context of PICOS.

2.4.10 Eligibility

Eligibility is the state of meeting required conditions; or the state of being qualified to participate or be chosen (based on http://www.merriam-webster.com).

In the framework of PICOS, this term is used to illustrate if someone in entitled to join an online community, or if someone can access certain services inside a community.

2.4.11 Entity

An entity is an individual (person), organisation, device or process (http://jungla.dit.upm.es/~pepe/401). The concept of entities covers the data subject, the data controller, the data processor and the various other actors that are present on the PICOS platform.

2.4.12 Fairness Principle

According to the fairness principle, personal data must be processed fairly and lawfully (Art. 6a [1]). The PICOS project will make sure the processing of personal data will only be done under fair conditions, and in a lawful and legitimate way.

2.4.13 Finality Principle (Purpose Limitation Principle)

This principle means that personal data must be collected for specified, explicit and legitimate purposes. The purpose of the processing should be defined at the latest at the moment of the collection of the data (Art. 6b [1]). In the PICOS project, the purposes for which the processing of personal data will be needed will be examined at an early stage.

2.4.14 Identity Fraud

Fraud is committed when somebody uses deception to obtain goods, services or money (http://www.homeoffice.gov.uk). Identity Fraud occurs when a false identity, or someone else's identity details, are used to support unlawful activity, or when someone avoids an obligation/liability by falsely claiming that he or she was the victim of Identity Fraud. Examples of Identity Fraud include using a False Identity or someone else's identity details (e.g., name, address, previous address, date of birth, et cetera) for commercial, economic or monetary gain; or obtaining goods or information; or obtaining access to facilities or services (such as opening a bank account, applying for benefits or obtaining a loan/credit card). (http://identity-theft.org.uk/definition.html). PICOS will build secure and trustworthy communication channels, which will minimise the danger for Identity Fraud.

2.4.15 Identity Theft

Identity Theft occurs when someone uses your personally identifying information, like your name, Social Security Number, credit card number or driver's licence without your permission, in order to impersonate you and commit fraud or other crimes (http://www.ftc.gov). It is also a crime in itself. Identity Theft is committed when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether, in the case of an individual, the victim is alive or dead (http://identity-theft.org.uk/definition.html). The information can be used to obtain credit, merchandise and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen (http://searchsecurity.techtarget.com). In order to properly define Identity Iheft, it is critical to define the negative impact experienced by the individual whose identity has been stolen. One of the negative repercussions of Identity Theft is financial loss, as thieves will have access to credit cards, bank accounts, et cetera. Furthermore, if the Identity Theft continues for a longer period of time, it can have a serious impact on the victim's good name. Credit reports, criminal records, employment history — they can all be affected by identity theft (http://internetsecuritypw.wordpress.com). Identity Theft and Identity Fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain (http://www.usdoj.gov). PICOS will build secure and trustworthy communication channels, which will minimise the danger for Identity Theft, as well for Identity Fraud, as already mentioned above.

2.4.16 Impersonation

According to the *Compact Oxford English Dictionary*, impersonation is the act of pretending to be another person for the purposes entertainment or fraud. The PICOS technologies channels will be built in a way not to allow impersonation of the user.

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

2.4.17 Information Security Governance

Information Security Governance is a framework/discipline that, according to *Wikipedia*, provides protecting information and information systems to counter unauthorised access, use, disclosure, modification or destruction. It is the system by which the current and future use of ICT is directed and controlled, and it involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring of […]. Information Security Governance includes the strategy and policies for using ICT within an organisation (Australian Standard for Corporate Governance of ICT).

2.4.18 IT Governance

IT Governance is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that an organization's IT sustains and extends the organisation's strategies and objectives (http://www.itgi.org). Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT [66].

2.4.19 Personal Data

Personal data are any information relating to an identified or identifiable natural person (i.e., a data subject); an identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (Art. 2a [1]). As PICOS is a project focusing on online and mobile communities and their users, any information relating to a user that can be identified will be considered as personal data.

2.4.20 Privacy Ontology

Privacy ontology describes the knowledge about the data protection domain in a standard, unambiguous manner, with the aim of converting privacy legislation into a language that is understood by an information system, so that the system in question automatically applies the prevailing privacy legislation to the processing of personal data, thus preventing unlawful processing [39].

2.4.21 Privacy Policy

A privacy policy is a legal notice on a website providing information about the use of personal information — particularly personal information collected via the website — by the website owner. Privacy policies usually contain details of what personal information is collected, how the personal information may be used, the persons to whom the personal information may be disclosed, and the security measures taken to protect the personal information [67].

In the context of PICOS, users may want to be able to automatically detect and match privacy policies against their personal policies. They may also want to negotiate a mutually acceptable policy. At present, privacy policies are used extensively by websites, but in many cases they represent the only outwardly facing acknowledgement of privacy. Community providers may need to offer more, and be more open about how and why they use personal data. In a P2P situation, personal privacy policies may be required.

2.4.22 Processing of Personal Data

Processing of personal data (or simply processing) is any operation or set of operations that is performed on 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 (Art. 2b [1]). Simply put, any action on information that can be linked to a user (or a natural person in general) is considered as processing of personal data.

2.4.23 Processor

A processor (or data processor) is a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller (Art. 2e [1]). The data processor acts under the orders of the data controller, who determines the purposes and means of the processing of personal data. In the PICOS project, it is of seminal importance to define the controller of the data, as already discussed (see the discussion concerning "data controller" in section 2.4.4 above), and distinguish him or her from the data processor.

2.4.24 Sensitive Data

Sensitive data is a special category of personal data that individuals, on average, prefer to be known only to a few selected others, and thus merits special legal protection. From a purely legal point of view, sensitive data are "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" (Art. 8 [1]). It is important to examine whether PICOS involves sensitive data, as their processing may take place only under specific conditions, defined restrictively in the data protection legislation.

2.4.25 Supervisory Authority

Each European Member State will provide that one or more public authorities are responsible for monitoring the application, within its territory, of the provisions adopted by the Member States pursuant to this Directive, which are commonly known as Supervisory Authorities. Each Member State will also provide that the supervisory authorities are to be consulted when administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data are drawn up. These authorities will, in particular, be endowed with investigative powers, such as powers of access to data forming the subject-matter of processing operations, and powers to collect all the information necessary for the performance of its supervisory duties. The members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they may have had access (based on Art. 28 Data Protection Directive).

2.5 Architecture and technical terminology

Stephen Crane (HPL), John O'Connell (HPF) and Jean-François Coudeyre (HPF)

One of the basic tasks PICOS has to achieve is to create a technical architecture and design for the PICOS community platform. This includes the data model that contains the relevant identity information, the tools that provide the identity, privacy and trust management functions, the data flows

between them, and the protocols for these. The essential goals and attributes of the architecture and design are to cater for the identity information flow needs of new, context-rich mobile communication services for communities, whilst meeting their participants' requirements for trust and privacy in an acceptable, trustworthy, open and scalable manner. Therefore, an introduction to the architecture and technical terminology that will be important for PICOS is essential and will be the main focus of this chapter.

2.5.1 Anonymous Credentials

Anonymous credentials (also called private or convertible credentials) are secondary credentials that are derived from a certificate issued to a different pseudonym of the same person. Multiple anonymous certificates can be created from a single certificate that are neither linkable to each other, nor to the issuance interaction in which the master certificate was obtained [22].

In the PICOS project, a user may wish to interact with a community at several levels, depending on their confidence in the ability of the community to protect their privacy, or on the trust they have in other users. A user may have several levels of "visibility", ranging from open through to very private. Anonymous credentials (or pseudonyms) may provide the latter. In practice, a user may switch between credentials (and levels of visibility) depending on the community they interact with, or even the nature of the interaction with the community.

2.5.2 Appliance

The term 'device' and 'appliance' are synonymous. See section 2.5.61 above on "Device" for a full definition.

For the functionality of appliances in PICOS, also see section 2.5.61 above.

2.5.3 Attribute Authority (AA)

An Attribute Authority (AA) is an authority that assigns privileges by issuing attribute certificates [29]. In a distributed trust model, the cross-certificate structure is used for both of these [29].

In the context of PICOS, the AA may best be thought of as a PICOS Trust Authority (TA), an entity that both the user and the community trust to validate user identity or entitlement. The AA could be the community provider or an independent entity, possibly providing a similar service to many communities. It may also be a general purpose portal to multiple communities.

2.5.4 Attribute Authority Revocation List (AARL)

An Attribute Authority Revocation List (AARL) is a revocation list of attribute certificates issued by Attribute Aythorities that are, in turn, no longer considered valid by the issuing authority [29].

For PICOS, the AARL may be used to identify AAs that a community no longer trusts to issue valid anonymous credentials. In a peer-to-peer community, users may revoke an AA to prevent other users from choosing that AA.

2.5.5 Attribute Certificate (AC)

An Attribute Certificate (AC) is a data structure, digitally signed by an Attribute Authority, which binds some attribute values with identification information about its holder [29].

The Attribute Certificate within PICOS would provide users with validated information about new or existing members, thereby providing a route to building trust.

2.5.6 Attribute Certificate Revocation List (ACRL)

An Attribute Certificate Revocation List (ACRL) is a revocation list of attribute certificates that are no longer considered valid by the issuing authority [29].

In PICOS, the ACRL would provide a means to discard unreliable Attribute Certificates.

2.5.7 Authentication Token (Token)

An authentication token, or simply token, is the information conveyed during a strong authentication exchange, which can be used to authenticate its sender [29].

In a system like PICOS, authentication tokens will be necessary to strongly authenticate users, because the traditional face-to-face process is not possible online. An authentication token is one way to achieve strong authentication across a remote connection, and it can also be applied to strongly authenticate a service provider.

2.5.8 Authority

An authority is an entity that is responsible for the issuance of certificates. Two types are defined in this specification: certification authorities, which issue public-key certificates, and attribute authorities, which issue attribute certificates [29].

Both types of authorities will probably be required in PICOS, though they may be provided by the same entity. They both essentially endorse information about users. It is possible that, in a peer-to-peer community, each user might endorse their own information or information of others that they know well (this situation is known as an introductory service).

2.5.9 Authority Certificate

An authority certificate is a certificate issued to an authority (either to a certification authority or to an attribute authority) [29].

In the context of the PICOS project, authority certificates may be useful if a community devolves its responsibilities to other authorities, for example, if it outsources functionalities such as user registration.

2.5.10 Base CRL

A Base CRL is the root of a Certificate Revocation List. Changes in the CRL, referred to in [29] as “delta CRL” or just “deltas”, combine with the Base CRL to record the up-to-data status of entities described in the list. For example, the delta CRL would record the change in status of a particular attribute of the entity described in the Base CRL, such as, for example, “certificate revoked”. The advantage of delta CRLs is that they are compact and easier to manage than a potentially very large Base CRL.

In the context of PICOS, this and other certificate-related terms are essential to the operation of a certification process, but do not provide any unique features to communities or to PICOS.

2.5.11 Biometric Encryption/Decryption

Biometric encryption covers the conversion of biometric data into a form called “cipher text”, which, in turn, cannot be easily understood by unauthorised people. Decryption, on the other hand, is the process of converting encrypted data back into their original form, so that they can be understood [7].

Biometric Encryption is a process that securely binds a PIN or a cryptographic key to biometric data, so that neither the key nor the biometric data can be retrieved from the stored template. The key is re-created only if the correct, live biometric sample is presented on verification [12].

Strong identification based on biometric data may be required within PICOS, if the basis of trust is to be able to reliably re-identify individuals. In normal practice, recovering a key from biometric data will require additional services (such as secure storage), as the biometric data, possibly in association with a PIN, will unlock a safe that holds the key securely. However, deriving the key from the biometric data may only be feasible for a certain application. Biometrics may be the most acceptable means of identification/verification to members, but they also raise additional privacy concerns, like DNA profiling and links with law enforcement.

2.5.12 Biometric Enrolment

Biometric enrolment is the process of collecting biometric samples from a person, and the subsequent preparation and storage of biometric reference templates representing that person’s identity [7]. It has also been defined by (http://ecommittees.bsi-global.com/bsi/controller/IST_33-0401_06.pdf?livelinkDataID=14471175&download=true) as the process of creating and storing a data record containing biometric and non-biometric data that belong to an individual.

For the significance of biometric enrolment in PICOS, see section 2.5.13 below on biometric templates.

2.5.13 Biometric Sample

A biometric sample is the information obtained from a biometric device that contains encoded information on distinctive human characteristic data, such as a fingerprints, retina patterns or voice prints. Alternatively, a biometric sample is defined as information obtained from a biometric sensor, either directly or after further processing (http://ecommittees.bsi-global.com/bsi/controller/IST_33-0401_06.pdf?livelinkDataID=14471175&download=true).

For the significance of biometric enrolment in PICOS, see section 2.5.13 below on biometric templates.

2.5.14 Biometric Template

A biometric template is a digital representation of an individual’s distinct characteristics, representing information extracted from a biometric sample. Templates can vary between biometric modalities as well as vendors. Not all biometric devices are template based. For example, voice recognition typically relies on being able to match certain attributes of the captured voice pattern with a template that defines some (but not all) of the distinguishing attributes of the individual [7]. The stored feature set, labelled with the user’s identity, is referred to as a biometric template [30]. A biometric sample or combination of biometric samples that is suitable for storage serves as a reference for future

comparison (http://ecommittees.bsi-global.com/bsi/controller/IST_33-0401_06.pdf?livelinkDataID=14471175&download=true).

If biometric data (such as fingerprints or iris prints) are used in PICOS, then measures on how to produce and protect a template that is used in the verification process will be necessary. The whole biometric life-cycle will need careful consideration. The "trigger point", where entered biometric data is accepted as a match for a pre-agreed (stored) description of that data (the template), will also need to be carefully defined to avoid excessive false positives/negatives during recognition.

2.5.15 Biometric Threshold

A biometric threshold is a predefined number, often controlled by a biometric system administrator, that establishes the degree of correlation necessary for a comparison to be deemed a match [48]. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold [7]. According to (http://ecommittees.bsi-global.com/bsi/controller/IST_33-0401_06.pdf?livelinkDataID=14471175&download=true), a biometric threshold is a predefined value that establishes the degree of similarity or correlation (that is, a score) necessary for a biometric sample to be deemed a match with a biometric reference template.

For the significance of biometric enrolment in PICOS, see section 2.5.13 above on biometric templates.

2.5.16 CA-certificate

A CA-certificate is a certificate for one Certification Authority issued by another one [29].

For the role of CA-certificates within PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.17 Cancellable Biometrics

Cancellable biometrics is a method of enhancing the security and privacy of biometric authentication. Instead of enrolling with your true finger (or other biometric source), the fingerprint is intentionally distorted in a repeatable manner, and this new print is used. If, for some reason, your old fingerprint is "stolen", an essentially "new" fingerprint can be issued by simply changing the parameters of the distortion process. This also results in enhanced privacy for the user, since his or her true fingerprint is never used anywhere, and different distortions can be used for different types of accounts. The same technique can also be used with other biometrics [50]. Cancellable biometrics performs a distortion of the biometric image or features before matching. The variability in the distortion parameters provides a cancellable nature to the scheme. Cancellable biometrics may be seen to represent a promising approach to address biometric security and privacy vulnerabilities [67].

There is concern that biometrics are private, personal information, that, if exposed, could severely compromise or disadvantage individuals. Recovery from exposure is an important consideration, which will be taken into consideration in the PICOS project. To some extent, avoiding the problem in the first place through careful system design is the answer. For example, *Trustguide* (www.trustguide.org.uk) discusses restoration as being a key trust enabler.

2.5.18 Certificate Policy

A certificate policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range [29].

Where a PICOS community issues or accepts certificates, the policy would provide a user or another authority with information to enable the usefulness of the certificate to be determined.

2.5.19 Certification Practice Statement (CPS)

A Certification Practice Statement (CPS) is a statement of the practices that a Certification Authority employs in issuing certificates [29].

A PICOS community that issues certificates may use a Certification Practice Statement to explain features of the certification process to potential users.

2.5.20 Certificate Revocation List (CRL)

A Certificate Revocation List (CRL) is a signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types cover particular scopes [29].

Within the context of PICOS, a Certificate Revocation List has essentially similar purpose to the Attribute Certificate Revocation List (ACRL).

2.5.21 Certificate User

A certificate user is an entity that needs to know, with certainty, the attributes and/or public key of another entity [29].

For Certificate Users in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.22 Certificate Serial Number

A certificate serial number is an integer value, unique within the issuing authority, that is unambiguously associated with a certificate issued by that authority [29].

For the certificate serial number in PICOS, see section 2.5.9 above concerning Base CRLs..

2.5.23 Certificate-using System

A certificate-using system is an implementation of those functions defined in this Directory Specification that are used by a certificate-user [29].

For the certificate-using system in PICOS, see section 2.5.9 above concerning Base CRLs..

2.5.24 Certificate Validation

Certificate validation is the process of ensuring that a certificate was valid at a given time, including possibly the time of the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e., were not expired or revoked) at that given time [29].

For the certificate serial number in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.25 Certification Authority (CA)

A Certification Authority (CA) is an authority trusted by one or more users to create and assign public-key certificates. Optionally, the CA may create the users' keys [29].

For the Certification Authority in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.26 Certification Authority Revocation List (CARL)

A Certification Authority Revocation List (CARL) is a revocation list containing a list of public-key certificates issued to certification authorities that are no longer considered valid by the certificate issuer [29].

For the Certification Authority Revocation List in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.27 Certification Path

A certification path is an ordered sequence of public key certificates of objects in the Directory Information Tree (DIT, which concerns data represented in a hierarchical tree-like structure consisting of the Distinguished names (DNs) of the directory entries [could this instead or also refer to the relevant section on DITs? (section 2.5.39)]) that, together with the public key of the initial object in the path, can be processed to obtain the final object in the path [29].

For the Certificate Path in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.28 Claim

A claim is a statement made by an entity (the claimant) about another entity (the claim's object) to an other entity or a set of entities (the claimant's addressee). A claim can be endorsed by a third party that certifies the claim to have been made in an integrity-protected manner. An example for a claim is "The requester is of age greater than 18 years, claimed by the requester, endorsed by an EU-Member State-issued passport". A claim request (or a request for claims) is issued in order to obtain claims that satisfy the access control policy for a requested resource [22].

Where users are engaged in many communities, such as the ones supported by PICOS, claims issued by a commonly trusted third party would be useful in establishing trust or agreeing rights and entitlements. It should be pointed out that the term "claim" is used in exactly the same way by Microsoft's *Windows CardSpace*. One can imagine a *CardSpace*-like wallet containing identity cards used to access communities, when each card also carries user-defined preferences, covering privacy and other individual requirements.

2.5.29 Controlled Release

Controlled release is the condition when personal information is shared with a third party with pre-agreed terms of use.

Prior to sharing personal information with a PICOS community provider or community member, the user may specify how his or her information can be used by way of preferences on, for example,

duration, purpose and onward sharing. These preferences would be described alongside the data items at the time of sharing, and be ideally bound to each item or to the set of data.

2.5.30 CRL Distribution Point

A CRL distribution point is a directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one Certification Authority, or may contain revocation entries for multiple ones [29].

For the CRL distribution point in PICOS, see section 2.5.9 above concerning Base CRLs. The CRL distribution point in PICOS could be a function provided by the community operator or a trusted third party.

2.5.31 Cross-certificate

A cross-certificate is a public-key or attribute certificate that enables a subject certified by one Certificate Authority (CA) to be checked by another CA. Cross-certificates are exchanged between CA and CA, and between Attribute Authority (AA) and AA. Cross-certificates provide a way for a hierarchy of CAs/AAs to be created, such that subjects can be authorised regardless of the issuing CA [29].

For cross-certificates in PICOS, see section 2.5.9 above concerning Base CRLs. A cross-certificate is particularly relevant when considering multiple communities or "communities of communities".

2.5.32 Cryptographic System (Cryptosystem)

A cryptographic system, or simply a cryptosystem, is a collection of transformations from plain text to cipher text and vice versa, with the particular transformation(s) to be used being selected by keys, either Public/Private or Secret Keys, depending whether the cryptosystems is asymmetric or symmetric. The transformations are normally defined by a mathematical algorithm [29].

Within PICOS, cryptographic systems are a building block of the certification process and anonymous/pseudonymous credentials, which are required to provide confidentiality and integrity of data, as well as strong authentication.

2.5.33 Data Confidentiality

This service can be used to provide for the protection of data from unauthorised disclosure. The data confidentiality service is supported by the authentication framework. It can be used to protect against data interception [29].

Confidentiality services typically rely on a *data encryption mechanism* to translate confidential data into a protected state (subsequently described as *encrypted*). It is usually no longer necessary or appropriate refer to the protected (encrypted) data as confidential.

A data confidentiality service is also responsible for translating the encrypted data into a decrypted state, thus restoring it to a confidential state.

In PICOS, data confidentiality may be used to control access to information in transit or storage.

2.5.34 Data Integrity

Data integrity is a service designed to protect data from unauthorised or accidental modification.

Integrity services normally use a function like a hash, or a cryptographic digital signature mechanism, to produce a condensed representation of data. They provide an important check on data that must not change (or where change must be made obvious). Sometimes, this condensed representation is called a (digital) signature. The integrity of data is said to be preserved when the signature of the data in question matches a reference signature. The reference signature would most probably have been created at the same time as the original data.

Data integrity could be used in PICOS in order to detect and prevent unauthorised modification of data. If described in terms of hash functions, it may also be used to produce digests of data and support a signature scheme.

2.5.35 Data Availability

According to the notion of data availability, data and supporting systems must always be available when required.

In PICOS, on demand access to the community and the supporting user data is essential in order to maintain confidence in the community. Safe operation of the community is likely to be highly dependent on operating data being available when required.

2.5.36 Data Sharing

Data sharing is the ability to share the same data resource between multiple applications or users. It implies that the data are stored in one or more servers in the network and that there is some software locking mechanism that prevents the same set of data from being changed by two people at the same time. Data sharing is a primary feature of a database management system (DBMS) (http://www.answers.com).

Data Sharing is a feature common to communities and especially so in the context of PICOS, where members generate data about other members. Privacy of this data will be a key concern for members. Members may want to identify other members who access data about them. Where simple access control is not enough, it may be necessary to log and audit access made by members.

2.5.37 Delegation

Delegation is the conveyance of a privilege from one entity that holds such privilege, to another entity [29].

A PICOS community may choose to delegate authority for specific functions to another entity. The entity possessing the delegated authority may need to demonstrate that authority to a user, and would probably do so using the processes described under the definition of Credential, i.e. where a Certification Authority binds a set of privileges (attributes) to a specific user.

2.5.38 Delegation Path

A delegation path is an ordered sequence of certificates that, together with authentication of a privilege asserter's identity, can be processed to verify the authenticity of an asserter's privilege [29].

For delegation paths within PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.39 Delta-CRL (dCRL)

A Delta-CRL is a partial revocation list that only contains entries for certificates that have had their revocation status changed since the issuance of the referenced Base CRL [29].

For the Delta-CRL in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.40 Device

A device (or end device or end-user device) is the appliance that users interact with directly, e.g. a mobile phone, PDA, or laptop. The device is often considered to be personal.

PICOS does not attempt to define an end-user device, and is essentially platform-agnostic. However, since PICOS is concerned with mobile communities, it is likely that the device will be designed to be able to operate in a mobile environment, which will place some constraints on platform functionality (such as display size and connectivity).

2.5.41 Directory Information Tree (DIT)

A Directory Information Tree (DIT) is data represented in a hierarchical tree-like structure consisting of the Distinguished Names (DNs) of the directory entries.

2.5.42 Distributed Service Architectures

A distributed service architecture can be defined as an architecture that enables the delivery of services over the Internet. If the service architecture is fully distributed, then there is no single point of failure.

Assuming that PICOS is based on a set of services provided locally and remotely by one or more providers, where these services are essentially “distributed” across the community, architecture that describes the implementation and access to each service will be required.

2.5.43 End-entity Attribute Certificate Revocation List (EARL)

An end-entity attribute certificate revocation list (EARL) is a revocation list of attribute certificates that are issued to holders who are not also Attribute Authorities, and that are no longer considered valid by the certificate issuer [29].

For end-entity attribute certificate revocation lists in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.44 End-entity Public-key Certificate Revocation List (EPRL)

An end-entity public-key certificate revocation list (EPRL) is a revocation list of public-key certificates that are issued to subjects who are not also Certification Authorities, and that are no longer considered valid by the certificate issuer [29].

For end-entity public-key certificate revocation lists in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.45 Environmental Variables

Environmental variables are the aspects of policy required for an authorisation decision that are not contained within static structures, but are available through some local means to a privilege verifier (e.g., the time of day or a current account balance) [29].

It is likely that context will play an important role in determining rights and trust within the PICOS project. For example, location may influence which communities can be accessed and for what purpose. Location would be held in a local environmental variable.

2.5.46 Full Certificate Revocation List

A full Certificate Revocation List (CRL) is a complete revocation list that contains entries for all certificates that have been revoked for the given scope [29].

For full Certificate Revocation Lists in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.47 Hash Function

Hash functions are mathematical functions that map values from a large (or possibly very large) domain into a smaller range. A "good" hash function is one of which the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range [29].

For the use of hash functions in PICOS, see Data Integrity in section 2.5.33 above. Hash functions are seen as a cryptographic building block used by the credential process for signature generation and integrity checking processes.

2.5.48 Holder

A holder is an entity to whom some privilege has been delegated, either directly from the Source of Authority, or indirectly through another Attribute Authority [29].

A holder is PICOS is the user of a community provider, or a trusted third party.

2.5.49 Identity Federation

In information technology (IT), the term "federated identity" has two general meanings. The first meaning is the virtual reunion, or assembled identity, of a person's user information (also known as the "principal"), stored across multiple distinct identity management systems. Data a joined together by use of the common token, which is usually the user name. The second meaning is the process of a user's authentication across multiple IT systems or even organisations. Federated identity, or the "federation" of identity, describes the technologies, standards and use-cases that serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. It can improve privacy compliance by allowing the user to control what information is shared, or by limiting the amount of information shared. Identity federation can be accomplished any number of ways, some of which involve the use of formal Internet standards, such as the OASIS SAML specification, and some

of which may involve open source technologies and/or other openly published specifications (for example, Information Cards, OpenID, the Higgins trust framework or Novell's Bandit project) [67].

Where multiple communities interact, or where a community relies on an external identification service in the context of PICOS, then the use of federated identification may be appropriate. Federation can raise concerns about privacy, such as when sharing personal identification information with an entity other than the service (community) provider.

2.5.50 Identity Management System (IMS)

An identity management system (IMS) in its broadest sense refers to the technology-based administration of identity attributes, including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role [22]. Identity Management involves the management of the identity life cycle of entities (subjects or objects), during which the system can: establish an identity by linking a name or number with the subject or object; re-establishe the identity (i.e., links a new or additional name, or number, with the subject or object); describe the identity (assigns attributes or re-describes the identity by changing attributes applicable); or even destroy the identity [67].

An IMS is part of lifecycle management, which covers users and personal data. It is likely to be a critical part of PICOS and it will strongly define the architecture of the project. The phrase "from cradle to the grave" illustrates the impact that identity has during the lifetime of a community member.

2.5.51 Indirect Certificate Revocation List (iCRL)

An indirect certificate revocation list (iCRL) is a revocation list that at least contains revocation information about certificates issued by authorities other than the one that issued the iCRL [67].

For indirect certificate revocation lists in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.52 International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are two specialised bodies created for worldwide standardisation. National bodies that are members of the ISO or IEC participate in the development of International Standards through technical committees, established by the respective organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, governmental and non-governmental, in liaison with the ISO and IEC, also take part in the work. In the field of information technology, the ISO and IEC have established a joint technical committee: ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to the national bodies for voting. Publication as an International Standard requires approval by at least 75 per cent of the national bodies casting a vote (http://ecommittees.bsi-global.com/bsi/controller/IST_33-0401_06.pdf?livelinkDataID=14471175&download=true).

Where it makes sense, PICOS should consider adopting standardised approaches and contributions to the standardisation process. It is possible that a standard approach will instil trust and confidence in members, and could lead to more robust implementations. Collaborations between communities, especially with the larger existing communities, may demand the adoption of standards. Standards that relate to cryptography, or security in general, should be adopted, again, to instil confidence among members.

2.5.53 ISO/IEC JTC 1

ISO/IEC JTC 1 is a joint technical committee that was formed in 1987 between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), for the standardisation in the field of information technology. The number "one" in the name refers to the fact that it is the first and only formal collaboration between the ISO and IEC (http://www.birds-eye.net).

For the role of ISO/IEC JTC 1 in PICOS, see section 2.5.50 above on ISO.

2.5.54 ISO/IEC JTC 1 SC 27

ISO/IEC JTC 1 SC 27 is a subcommittee of ISO/IEC JTC 1. Titled "Security Techniques", its area of work is the standardisation of generic methods and techniques for IT Security. The scope of this area of work for SC 27 includes the standardisation of cryptographic algorithms for integrity, authentication, and non-repudiation services. Furthermore, it includes the standardisation of cryptographic algorithms for confidentiality services for use in accordance with internationally accepted policies. Current activities of SC 27 are divided into five working groups:

- Working Group 1: Information security management systems.
- Working Group 2: Cryptography and security mechanisms.
- Working Group 3: Security evaluation criteria.
- Working Group 4: Security controls and services.
- Working Group 5: Identity management and privacy technologies. (http://ecommittees.bsi-global.com/bsi/controller/IST_33-0401_06.pdf?livelinkDataID=14471175&download=true)

For the role of ISO/IEC JTC 1 SC 27 in PICOS, see section 2.5.50 above on ISO.

2.5.55 ISO/IEC JTC 1 SC 27 WG 5

The scope of SC27/WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data (http://ecommittees.bsi-global.com/bsi/controller/IST_33-0401_06.pdf?livelinkDataID=14471175&download=true).

For the role of ISO/IEC JTC 1SC 27 WG 5 in PICOS, see section 2.5.50 above on ISO.

2.5.56 Key Agreement

A key agreement is a method for negotiating a key value online without transferring the key, even in an encrypted form, such as, for example, the Diffie-Hellman technique (see ISO/IEC 11770-1 for more information on key agreement mechanisms) [29].

Unique one-to-one relationships may be established in PICOS between user and community operator, or between user and user. Although public key solutions that enable safe sharing of information and strong identity exist, for efficiency reasons, shared key solutions may be necessary. Key agreements, and, more generally, key management services, will be required.

2.5.57 Mix

A Mix is a computer that mediates between senders and recipients. A Mix is a store-and-forward device that accepts a number of fixed-length messages from numerous sources, performs cryptographic transformations on the messages, and then forwards the messages to the next destination in an order not predictable from the order of inputs [67].

Anonymous communications can be achieved in PICOS through mix networks, and it is possible that, if truly anonymous (e.g. P2P) communication is necessary, then some variation of a mix network will be required.

2.5.58 Object Method

An object method is an action that can be invoked on a resource (e.g., a file system may have read, written and executed object methods) [29].

For object methods in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.59 One-way Function

A one-way function is a (mathematical) function f that is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that f(x) = y. There may be a few values y for which finding x is not computationally difficult [29].

For the role of one-way function in PICOS, see section 2.5.45 above on Hash Function.

2.5.60 Onion Routing

Onion routing is a technique for pseudonymous (or anonymous) communication over a computer network [67].

For the role of Onion Routing in PICOS, see section 2.5.55 above on Mixes.

2.5.61 P3P

The Privacy Preferences Protocol (P3P) is a tool that enables easy communication about the privacy preferences of Internet users in a standardised form that can be read by the information system. The JRC (Joint Research Centre of the EU situated in Ispra, Italy) developed a version of P3P in accordance with the EU Directive [39]. The Platform for Privacy Preferences is a protocol that specifies a way to determine if a website's security policies meet a user's privacy requirements (http://searchsecurity.techtarget.com). The Platform for Privacy Preferences Project (P3P) enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents (www.w3.org).

PICOS should consider the value of providing privacy policy information to members using P3P. P3P is not as widely adopted as some would hope, and it is not clear what anything other than a satisfactory report signifies. However, it is an easy way to communicate to members something about privacy policy, and if standardised across multiple communities, it may provide a benefit to members with regard to trust establishment and the sharing of personal information.

2.5.62 Platform

A platform is a collection of resources, hardware and/or software that enable the delivery of a service to users through end devices. The term “end devices” typically refers to an appliance, e.g., a notebook, PDA or mobile phone. In practice, a platform may be described using an architectural or framework representation. The platform may consist of hardware, firmware, operating system and application software, but it will be defined by the fact that is offers a set of useful services that support a higher level of objective, such as a community.

The services that community members use, and which actually define the community profile and behaviour (i.e., its role, target audience, et cetera), are provided by an underlying set of functions that relies on hardware, software, networking and end devices. In PICOS, it is this functionality that defines the platform. The platform integrates with (or interoperates with) the community data and applications to deliver services to community members.

2.5.63 Platform Virtualisation

According to *Wikipedia*, virtualisation is a broad term that refers to the abstraction of computer resources.

The current trend is to build virtual platforms on top of physical platforms. The advantage of this is that it is possible to control the interaction between virtual platforms and restrict access to the underlying physical properties, like storage and communication. This leads to the concept of containment, which is essential for good security, and something that is difficult to achieve on a platform that only supports shared applications. PICOS could take advantage of this technology to run, for example, trusted client applications, so that other users know that they cannot be interfered with.

2.5.64 Policy Mapping

Policy Mapping relates to when a Certification Authority (CA) in one domain certifies a CA in another domain. Certification is achieved through an exchange of certificates. For one CA to recognise the certificate of another, a description of acceptable attributes is required. This description is represented in a policy to which each CA agrees. It is possible that each CA will describe their requirements in a slightly different way. Thus the policy will need to “map” the capabilities of one CA to the requirements of another in a mutually acceptable manner [29].

For the policy mapping in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.65 Privacy-Enhancing Identity Management System (PE-IMS)

A Privacy-Enhancing Identity Management System (PE-IMS) is an Identity Management System (IMS) that, given the restrictions of a set of applications, sufficiently preserves unlinkability, as seen by an adversary, between the partial identities and corresponding pseudonyms of a person [22].

In the context of PICOS, privacy-enhancing identity management systems, which can be applied across multiple communities, may be used to ensure that identity can be validated without needing to reveal excessive information about the individual. The conditions on which information is released could be context based, a feature that is normally not found in a traditional IMS.

2.5.66 Privacy Preferences

Privacy preferences are instructions prepared by the sharing party (typically the individual) and express how personally their information should be handled by the receiving party.

For the setting up of privacy preferences within PICOS, see section 2.5.28 above on “Controlled Release”.

2.5.67 Private Key

In the context of a public key cryptosystem, a private key (or, a secret key) is the key of a user’s key pair, which is known only by that user [29].

In the PICOS project, a private key will be required for signing and sharing of confidential information, for strong identification and integrity checking processes.

2.5.68 Privilege

A privilege is an attribute or property assigned to an entity by an authority [29].

In the context of PICOS, a privilege could also be described as an entitlement to a service, or, more loosely, as an authority.

2.5.69 Privilege Asserter

A privilege asserter is a privilege holder, who uses his or her attribute certificate or public-key certificate to assert privileges [29].

A privilege asserter, as well as other privilege-related terms, is essential to the operation of a privilege management process, but does not provide any unique features to communities, or to PICOS.

2.5.70 Privilege Management Infrastructure (PMI)

Privilege management infrastructure (PMI) is the infrastructure that is able to support the management of privileges in support of a comprehensive authorisation service and in relationship with Public Key Infrastructure [29].

For the role of Privilege Management Infrastructures in PICOS, see section 2.5.69 above on “Privilege Asserter”.

2.5.71 Privilege Policy

A privilege policy is the policy that outlines conditions for privilege verifiers to provide and perform sensitive services to/for qualified privilege asserters. A privilege policy relates attributes associated with the service, as well as attributes associated with privilege asserters [29].

For privilege policies in PICOS, see section 2.5.69 above on “Privilege Asserter”.

2.5.72 Privilege Verifier

A privilege verifier is an entity that verifies certificates against a privilege policy [29].

For the role of privilege verifiers in PICOS, see section 2.5.69 above on “Privilege Asserter”.

2.5.73 Public Key

In the context of a public key cryptosystem, a public key is the key of a user's key pair which is publicly known [29].

For the creation and use of public keys in PICOS, see section 2.5.69 above on "Privilege Asserter".

2.5.74 Public Key Certificate (PKC)

A Public Key Certificate (PKC) binds a public key (and the corresponding private key) to information that identifies the holder of the key pair. A digital signature can be formed using the private key, and subsequently checked, using a publicly available public key. The validity of the public key (i.e., the fact that it belongs to the individual who claims to have made the signature) is usually confirmed by checking the public key certificate, with reference to the Certification Authority that issued the certificate [29].

A PICOS user may be required to obtain a certificate for his or her public key from a mutually trusted authority. The certified key could be used to validate a public key before sharing sensitive information with the entity that holds the corresponding private key.

2.5.75 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is the infrastructure that is able to support the management of public keys in order to support authentication, encryption, integrity and non-repudiation services [29].

Although PKI provides the supporting infrastructure for operations involving public keys, in the context of PICOS, it may create an overhead that goes beyond the capabilities of smaller communities.

2.5.76 Reliability

Reliability is an attribute of any computer-related component (software, hardware, or a network, for example) that consistently performs according to its specifications (http://whatis.techtarget.com). In general, reliability is the ability of a person or system to perform and maintain its functions in routine circumstances, as well as hostile or unexpected circumstances. The IEEE defines it as "the ability of a system or component to perform its required functions under stated conditions for a specified period of time" [67]. Reliability metrics include the following averages: POFOD (probability of failure on demand), ROCOF (rate of failure occurrence), MTTF (mean time to failure), and AVAIL (availability or uptime) (http://www.answers.com).

2.5.77 Relying party

A relying party is a user or agent that relies on the data in a certificate in order to make decisions [29].

Relying parties used in PICOS are described above in section 2.5.69 on "Privilege Asserter".

2.5.78 Role Assignment Certificate

A role assignment certificate is a certificate that contains the role attribute, which assigns one or more roles to the certificate subject/holder [29].

In an anonymous interaction between two or more entities, as it will be defined in the PICOS project, knowing the role, but not the identity of the entities, may be sufficient to establish trust and permit the transaction to go ahead.

2.5.79 Sensitivity

Sensitivity is the characteristic of a resource that implies its value or importance [29]. For example, medical information is considered by most individuals to be sensitive and private (whereas a telephone number is probably just private).

As PICOS is going to focus on various communities, as regards sensitivity, it may need to differentiate between different types of personal information, like personal versus sensitive data, the latter typically being used to refer, among other things, to medical, religious or sexual information.

2.5.80 Simple Authentication

Simple authentication is authentication by means of simple password arrangements [29].

Simple authentication could be a simple, inexpensive means to authenticate users within PICOS, but may not be strong enough for every application. If so, then a token based or biometric authentication may be required.

2.5.81 Security Policy

A security policy is the set of rules laid down by the security authority governing the use and provision of security services and facilities [29].

A security policy is typically an internal document that describes how security is managed. Such a document in the context of PICOS is one that supports the operation of a system, and may be shared between cooperating community providers, but is normally not shown to the users (customers).

2.5.82 Self-issued Attribute Certificate (Self-issued AC)

A self-issued Attribute Certificate (self-issued AC) is an attribute certificate for which the issuer and the subject are the same Attribute Authority (AA). An Attribute Authority might use a self-issued AC, for example, to publish policy information [29].

For self-issued ACs in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.83 Self-issued Certificate

A self-issued certificate is a public-key certificate for which the issuer and the subject are the same Certification Authority (CA). A Certification Authority might use self-issued certificates, for example, during a key rollover operation to transfer trust from the old key to the new key [29].

For self-issued certificates in PICOS see, section 2.5.9 above concerning Base CRLs.

2.5.84 Self-signed Certificate

A self-signed certificate is a special case of self-issued certificates in which the private key used by the Certification Authority to sign the certificate corresponds to the public key that is certified within the

certificate. A Certification Authority might use a self-signed certificate, for example, to advertise their public key or other information about their operations [29].

For self-signed certificates in PICOS see section 2.5.9 above concerning Base CRLs.

2.5.85 Source of Authority (SOA)

A Source of Authority is an Attribute Authority that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges [29].

For source of authority in PICOS see, section 2.5.9 above concerning Base CRLs.

2.5.86 Spoke-hub

A spoke-hub is a model or network in which all routes move along spokes, passing through a central hub, arranged similarly to a bicycle wheel [67].

When spoke-hubs are used in PICOS, they will most likely imply a centralised architecture, where a single entity controls the community. This is different to the situation in a peer-to-peer community, where there is no central authority and all users carry equal status.

2.5.87 Strong Authentication

Strong authentication is authentication by means of cryptographically derived credentials [29].

In the context of PICOS, strong authentication is considered to be a token or biometric based authentication, as opposed to simple password authentication.

2.5.88 Trust Anchor

A trust anchor is a set of the following information, in addition to the public key: an algorithm identifier, public key parameters (if applicable), a distinguished name of the holder of the associated private key (i.e., the subject CA) and, optionally, a validity period. The trust anchor may be provided in the form of a self-signed certificate, and is trusted by a certificate-using system and used for validating certificates in certification paths [29].

For trust anchors in PICOS, see section 2.5.9 above concerning Base CRLs.

2.5.89 Trusted Platform Module (TPM)

A Trusted Platform Module (TPM) offers facilities for the secure generation and limiting the use of cryptographic keys, as well as a hardware pseudo-random number generator. It also includes capabilities such as remote attestation and sealed storage. Remote attestation creates a hash key-summary of a system's hardware and software, which is very difficult to be forged. To what extent the software is being summarised is decided by the software that is encrypting the data. This allows a third party to verify that the software has not been changed.

Sealing encrypts data in such a way that it may be decrypted only when the TPM releases the right decryption key, which it only does if the exact same software from when the data were encrypted is present.

Binding encrypts data using the TPM's endorsement key, a unique RSA key burned into the chip during its production, or another trusted key.

A TPM can be used to authenticate hardware devices. Since each TPM chip has a unique and secret Private RSA key burned into it during its production, it is capable of performing platform authentication. For example, it can be used to verify that the system seeking access is the expected system [67].

In the context of PICOS, it may become necessary to use some of the functionalities that a TPM offers, such as key storage. For certain, more tightly controlled platforms, e.g. mobile phones, that are able to attest to a trustworthy implementation, functionalities of TPM may be essential in establishing trust.

2.5.90 Uncontrolled Release

When an individual shares personal information without stating how the information should be used, it is described as an Uncontrolled Release (of personal information). This differs from a Controlled Release, when information is released to a third party on pre-agreed terms of use.

If a PICOS user can identify, and therefore strongly trusts, a community operator or other user, he or she may be willing to simply hand over personal information without any concern for how the information might be used. Alternatively, he or she may prefer to employ Controlled Release.

2.5.91 User-Controlled Identity Management System

A user-controlled identity management system is an IMS that makes the flow of the user's identity attributes explicit, and gives its user a large degree of control. The guiding principle is "notice and choice" [22]. A different description of a user-controlled IMS could be that it makes the flow of its user's identity attributes explicit to the users, and gives its user a large degree of control [47].

A user-controlled identity management system is similar to the notion of Controlled Release, but with the addition of some kind of feedback/acknowledgement that confirms receipt of an action, or that specific actions have been performed.

2.5.92 W3C

The World Wide Web Consortium (W3C) is an international consortium where member organisations, a full-time staff, and the public work together to develop Web standards. The W3C was founded in 1994 by Tim Berners-Lee, the original architect of the World Wide Web. W3C's mission is: "[t]o lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web" (http://www.w3.org). The World Wide Web Consortium is a consortium concerned with the development of interoperable technologies (standards, software and tools) for theInternet. Among other things, W3C developed and improved P3P [39].

For the importance of W3C for PICOS, see the discussions above in section 2.5.50 on "ISO", and section 2.5.59 on "P3P".

2.6 Terminology on Assurance of Technical Trust and Privacy Properties

Issac Agudo (UMA), José Luis Vivas (UMA) and Tobias Scherner (GUF)

Assurance is intended to be an integral part of the PICOS solution, and therefore will be a major evaluation criterion for the resulting platform. Hence, this chapter will briefly describe the basic terms related to the assurance of technical trust and privacy properties. Many definitions are drawn from Chapters 17 and 18 in Matt Bishop's "Introduction to Security", and are discussed in the context of PICOS [10].

2.6.1 Assurance

The 'ISO/IEC TR 15443-1'1 standard defines assurance as the performance of appropriate activities or processes intended to instil confidence that a system or product meets its security objectives. The term security is used here in the sense of multilateral security, which takes into account the interests of the user, including requirements on privacy. Assurance in the wider sense includes all activities required for structuring the product or system that is to be assured, such as an in-depth risk analysis for finding threats and providing countermeasures. Assurance in the narrower sense uses predefined testing algorithms to verify the correctness of well defined security functions. It is important to understand that assurance and confidence are not identical terms. Confidence relates to an individual's belief, whereas assurance refers to the demonstrated ability of the product or system to meet its objectives. As such, good assurance constitutes the basis for confidence [34].

2.6.2 Design Assurance

Design assurance is the evidence that a design meets the requirements of the security policy. Within PICOS, this corresponds to the assurance of the architecture design.

2.6.3 Evaluation Methodology

An evaluation methodology is a methodology that provides measurements of trust based on the security requirements and evidence of assurance. Evaluation methodologies provide: (i) a set of requirements defining the security functionality of the system; (ii) a set of assurance requirements describing the steps for establishing that a system meets its functional requirements; (iii) a methodology for determining that the system meets its functional requirements; and (iv) a measure of the level of trust indicating the trustworthiness of the system with respect to its security functional requirements. Examples of evaluation methodologies are *TCSEC* (Orange Book) [60], *FIPS* [43], the *Common Criteria* [58], and *SSE-CMM* [56]. For the needs of PICOS, the most relevant evaluation methodology is the Common Criteria.

2.6.4 Implementation Assurance

Implementation assurance is the evidence that an implementation is consistent with established security policies. Within PICOS, implementation assurance refers to the assurance of the platform and application prototypes.

2.6.5 Operational Assurance

Operational assurance is the evidence that a system meets the requirements of its security policy during installation, configuration and operation.

2.6.6 Policy Assurance

Policy assurance is the evidence that the set of requirements of a security policy is complete, consistent, and technically sound.

2.6.7 Requirement

A requirement is a goal that must be satisfied.

In the context of PICOS, the term "requirement" could have different meanings, depending, for instance, on the context in which it is used, the technical and personal background of the persons using the term, et cetera. Since PICOS focuses on trust, privacy and identity management, "requirement", in the context of assurance, is used to express the fact that a stakeholder of the system has requested that a certain protection goal should be achieved. The research challenge is that, although, on the one hand pure security requirements are well researched and can be modelled with the help of well known methodologies such as the Common Criteria, terms such as trust, privacy and identity management, on the other hand, are not clearly defined. This last issue will certainly have an impact upon the correctness and completeness of the corresponding requirements. Hence, it is important to consider how this kind of requirement can be precisely formulated. Given the importance of requirements for the creation of the PICOS architecture, a separate deliverable D2.4 will focus on this topic and try to elaborate requirements for Trust, Privacy and Identity Management for Online and Mobile Communities in general, and, more specifically, for the three PICOS applications, i.e. the Angling Community, the Taxi Driver Community, and the Online Gaming Community.

2.6.8 Trustworthiness

A system is trustworthy if there is enough credible evidence that the system meets a set of given requirements.

In PICOS, research beyond the pure technical aspect of trustworthiness will be conducted. A stakeholder needs to be convinced that a system meets its requirements. Whereas a simple awarded seal could be enough evidence for some stakeholders that a system is trustworthy, other audiences might request more elaborate evidence, such as, for instance, the verification of test results through the review of test procedures, or the requirement that repeated checks must be performed by several trusted entities.

2.6.9 Trust

Trust is a measure of trustworthiness that relies on evidence provided.

In the context of PICOS, a redefinition of the technical meaning of "trust", directed to a broader audience, is recognised to be of great value. From an assurance perspective, the audience for trust is comprised mainly, although not exclusively, by the members of the PICOS consortium and the stakeholders of the future system. Experiences gained in earlier research projects have shown that the translation of technical terms from one to other research disciplines is crucial for the overall success of

a project. Trust is also defined above in section 2.3.66. As "trust" is a core concept in the PICOS project, both definitions must be read in order to fully appreciate the complex meaning of the term.

2.7 Closing remarks

Eleni Kosta (ICRI-K.U.Leuven), all contributors

Online and mobile communities are at the centre of investigations and developments of the PICOS project. Establishing definitions of community-related terms, and their application to the project's objectives, are of great importance in order to provide common knowledge within the project consortium and thus providing a working basis for the overall project. The main challenge in defining these terms was the broadness and variety of existing definitions in the field, which were often of a popular science character. On the one hand, this can be seen as an indicator of the actual attractiveness of this topic in research and practice. On the other hand, finding universal definitions was difficult. Consequently, working definitions describing these terms in the frame of PICOS were specified instead of real definitions. The relevant terms regarding electronic and mobile communications follow, and are further complemented by the legal provisions on the protection of personal data in this field.

A principal goal of PICOS is to build a state of the art platform for providing the trust, privacy and identity management aspects of community services and applications on the Internet and in mobile communication networks. This implies that the concepts of privacy, identity management and trust need to be clearly understood by the project partners in order to be able to build the PICOS architecture and develop the actual trials.

The terms described in the section on Architecture and Technical Terminology relate to the provision of privacy and trust services to a broad community that are likely to be present in the mobile communities that PICOS will research. Many of the terms listed originate from traditional technical security research areas such as cryptography, computer security and information management. Other terms have their origin in the social sciences. Trust and privacy are terms that most people are familiar with, but which require a formal definition if they are to have useful meaning in PICOS. Providing this level of clarity is important for those who will be researching further in the specific fields, but it is also important in a project like PICOS that involves cross-discipline research. Finally, assurance is intended to be an integral part of the PICOS solution, and, therefore, the basic terms related to the assurance of technical trust and privacy properties are included in this Taxonomy.

The Taxonomy deliverable is the outcome of the close cooperation of the PICOS consortium in order to pursue a common understanding of the basic concepts that will play a significant role in discussions throughout the project life, and will be of seminal importance for the future of the project. During the life of the project, supplementary investigations of online and mobile communities will be conducted. This will result in a clearer picture of PICOS's communities and related topics. The output of this Taxonomy deliverable is updated on the designated wiki on the internal site of the PICOS project. This wiki will serve as the means to keep the Taxonomy as a living document that will be enriched during the project's whole lifetime, and will allow the definitions of concepts to mature along with the research conducted in the project.

Appendix A

In the PICOS project, three communities are chosen to serve as use cases. These are the Angling Community, the Online Gaming Community and the Taxi Drivers' Community. Given that the terminology used to describe angling and fisheries is rather unknown to the majority of the members of the PICOS consortium and other layman readers, this Appendix contains a glossary, where the basic terms regarding Angling and Fisheries is included (A.1). A common understanding among the PICOS consortium members on the terminology typically used within angling communities is considered as useful, specifically when it comes to the evaluation of the PICOS approach and platform with end-users in real-world contexts. In order to meet these requirements, various sources were explored for significant terms, and the suitability of these sources for compiling a comprehensive chapter on "Angler and Fisheries Terminology" was evaluated. The majority of these resources were online based. The following documents and repositories were then selected, from which terms were extracted:

- Lockwood, S.J., Ed., 2001: A Glossary of Marine Nature Conservation and Fisheries. Countryside Council for Wales, Bangor. ISBN: 1 861 69 085 1, p. 92.
- FishBase glossary of terms (www.fishbase.de/ListByLetter/GlossaryListA.htm);
- The Angler Advantage website and technology, glossary "Fishing Terms & Techniques" (www.theanglersadvantage.com/about.php);
- Orvis glossary on flyfishing terms (www.orvis.com);
- The English Fly Fishing Shop: an international glossary of flyfishing terms (www.flyfishing-flies.com);
- DFO's Statistical Services, Canada (www.dfo-mpo.gc.ca);
- NOAA Fisheries Office of Science and Technology (www.st.nmfs.noaa.gov);
- Convention of Biological Diversity, 1992 (www.cbd.int/convention/)
- www.wikipedia.org

The second part of the Appendix (A.2) contains terminology related to the Online Gaming Community. A part on taxi driver terminology, was not, however, created, as such terminology is of common use and does not present any particular difficulties to the average user.

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

A.1 Glossary of Angler and Fisheries Terminology

Bernd Ueberschär (IFM GEOMAR)

A.1.1 3ACFA

The Advisory Committee on Fisheries and Aquaculture. This body is a committee of (EC) DG Fisheries that includes representatives from the fishing and aquaculture industries, as well as non-governmental organisations representing the interests of consumers, the environment and development.

A.1.2 AFTM

The Association of Fishing Tackle Makers (UK based).

A.1.3 AFTMA

The American Fishing Tackle Manufactures Association. Its activities include setting technical standards for fishing tackle.

A.1.4 Anglerboard.de

The largest virtual angling community on the Internet in Germany, with about 43 000 registered members.

A.1.5 Angling

The activity of fishing with a hook and a line.

A.1.6 Annotated Bibliography of Fly Fishing

An annotated bibliography on *Wikipedia* that is intended to list both notable and not so notable works (non-fiction and fiction) in English related to the sport of fly fishing, listed by year published [67].

A.1.7 Anthropogenic

Caused by human activity; generally applied to sediment or other pollutants.

A.1.8 Bag Limit

The number of fish an angler may legally keep per day.

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

A.1.9 Bait

Any organism, but usually animal in origin, that is attached to fishing gear to attract fish. For example, crab pots are baited with fish, long-lines are baited with fish or molluscs, and anglers use worms and soft-shelled ("peeler") crabs.

A.1.10 Baitfish

Baitfish are small fish caught for use as bait to attract large predatory fish, particularly game fish. Species used are typically those that are common and breed rapidly, making them easy to catch and in regular supply. Examples of marine baitfish are anchovies, halfbeaks, and scads. Freshwater baitfish include any fish of the minnow or carp family (compare also with 'Bait'). In most countries, only dead baitfish are permitted to be hooked.

A.1.11 Bern Convention

The Bern Convention is the common name for the Council of Europe Convention on the Protection of European Wildlife and Natural Habitats (Bern 1979). The convention offers protection to plants, invertebrates and all vertebrates, and is binding on all signatories.

A.1.12 Big Game Fishing

Sometimes called offshore sport fishing or offshore game fishing, this is a form of recreational fishing, targeting large bony fish such as tuna and marlin in the open sea. This is often some distance from land and, in some fishing grounds, out of sight of land. It is conducted recreationally, as well as in competitions.

A.1.13 Biodiversity

The variability among living organisms from all sources including, among others, terrestrial, marine and other aquatic ecosystems, and the ecological complexes of which they are part; this includes diversity within species and ecosystems.

A.1.14 Biodiversity Convention

The UN Convention on Biodiversity signed at the UNCED "Earth Summit" in Rio de Janeiro 1992 to safeguard the total variety of animals, plants and all other living matter on Earth, i.e., to safeguard the world's biodiversity, and their habitats.

A.1.15 Biomass

The aggregate amount of living matter or a specific species within a specific habitat; expressed in units of pounds per acre.

A.1.16 Biotope

The physical habitat with its associated, distinctive, biological communities. The smallest unit of a habitat that can be delineated conveniently, it is characterised by the community of plants and animals living there.

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

A.1.17 Birds Directive

The EU Directive on the Conservation of Wild Birds (79/409/ EEC) seeks to protect all wild birds and the habitats of listed species, in particular through the designation of special protection areas (SPAs).

A.1.18 Black-fish

Fish that are landed in commercial quantities without being recorded in vessels' fishing log books, or without being declared to the appropriate authority as required by EU fishery regulation.

A.1.19 Bonn Convention

The Bonn Convention refers to the Convention on Migratory Species of Wild Animals (Bonn 1979), which seeks to co-ordinate the conservation of migratory species, particularly of those species whose lifecycle takes them across international and jurisdictional boundaries. Agreements reached under the convention include ASCOBANS [67].

A.1.20 Bowfishing

Fishing with a bow and arrow. It is permitted on many American waters, and the quarry is usually "trash" fish such as carp that are competing with more highly prized species such as bass. The arrow is tied to the end of a line and the reel is mounted on the bow.

A.1.21 Breaking Strength

The amount of effort required to break a single strand of unknotted monofilament or braided line, usually stated in pounds.

A.1.22 Brailer

A brailer is a "landing net" or a "dip net", which is used to land (big) fish properly and in accordance with the animal rights declarations. In most cases, it has a long handle, except for fly-fishing, where the handle needs to be short. A brailer is an item of essential, basic equipment for almost any fishing activity (with maybe except game fishing on the ocean) and, by law, in many countries anglers are requested to use a brailer when landing a fish.

A.1.23 By-catch

The catch of non-target species and undersized fish of the target species. By-catch of commercial species may be retained or discarded along with non-commercial by-catch.

A.1.24 "Buy your rod licence online"

The UK Environment Agency is the leading public body for protecting and improving the environment in England and Wales. It offers a convenient online system to purchase rod licences (credit card payment supported). Any angler aged 12 years or over, fishing for salmon, trout, freshwater fish or eels in England (except the River Tweed), Wales or the Border Esk and its tributaries in Scotland, must have an Environment Agency rod licence (http://www.environment-agency.gov.uk/subjects/fish/399730/)

A.1.25 Car Fishing

Some water courses, lakes and ponds can be accessed via car. For convenience, anglers have their car at the angling site. This is most common at "put-and-take" ponds (compare with section A.1. below on "Put-and-take").

A.1.26 Carrying Capacity

Maximum level the biomass of an animal population can reach in accordance to the quality of the environment.

A.1.27 CFP

The Common Fisheries Policy of the European Union (as revised in Council Regulation 3760/92). It provides the framework for the management of the EU fishery sector, including all marine fisheries within 200 miles of member states' baselines.

A.1.28 Charismatic Species

A species that is readily recognised, frequently with widespread popular appeal. They are sometimes used to focus attention on a (conservation) campaign or used as a logo, e.g., the Marine Conservation Society dolphin or WWF panda.

A.1.29 Closed Seasons

A period during which fishing for a particular species, often within a specified area, is prohibited.

A.1.30 Coarse Fishing

Many years ago, the English gentry classified fish into categories. Salmon and trout were considered more palatable than the other varieties of fish, and were classified as "game" fish. All other fish present were classified as "coarse" fish.

A.1.31 Coast Fishing

Mostly used to designate all inshore fishing activities in salt water.

A.1.32 Cohort

All the fish, or animals in a population that are of the same age, i.e., all fish spawned in the same year.

A.1.33 Collapsed Stock

The decline in spawning stock biomass (SSB), through sustained fishing pressure or natural causes, to the point where it no longer generates sufficient recruits to support a fishery.

A.1.34 Creel Limit

The daily number of fish an angler can keep in possession, as set by state regulations. Can vary from water to water, which means that anglers must check the relevant fishing regulations.

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

A.1.35 CPR

Short for Catch, Photograph, Release.

A.1.36 DG Environment

The Directorate General, or department, in the European Commission (EC) that has lead responsibility for EU environmental policy, including marine nature conservation. Formerly known as DG XI.

A.1.37 Discards

Any fish, or other living matter caught when fishing, that is not retained but returned to the lake, stream or sea — alive or dead.

A.1.38 European Anglers Alliance (EAA)

A pan-European organisation with 5 million members in 19 countries. The EAA is recognised as a non-governmental organisation by the European Commission and its Statutes are registered in Strasbourg. The EAA has a permanent office in Brussels and employs a full-time Secretary-General (http://www.eaa-europe.org).

A.1.39 Exclusive Economic Zone (EEZ)

The MFCMA defines this zone as contiguous to the territorial sea of all atages with a coastline and its possessions, and extending seaward 200 nautical miles measured from the baseline from which the Territorial Sea is measured.

A.1.40 European Fishing Tackle Trade Association (EFTTA)

A trade association for manufacturers and wholesalers of sport fishing equipment. EFTTA members can exhibit at EFTTEX, the leading international fishing tackle trade exhibition. Membership is open to manufacturers, wholesalers, agents and press in the tackle industry. The EFTTA was established in London in 1981, as an international, independent association to serve the European fishing tackle trade by campaigning to promote sport fishing, environmental issues and international business.

A.1.41 Ecology

The branch of biology dealing with the relationship between organisms and their environment.

A.1.42 Ecosystem

A discrete unit comprising both living and non-living parts; it can range in size from something as small and ephemeral as an intertidal pool, to, for example, the North Sea or Earth's oceans.

A.1.43 Eddy

A patch of water that is less disturbed than the surrounding water, found, for instance, on the edge of a current or where two streams converge.

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

A.1.44 Environmentally Sustainable Fisheries

Fisheries (recreational or professional) that safeguard the requirements of all animals and plants within an ecosystem or habitat, and do not cause irreversible or other significant, long-term change to the environment, or the communities of species that live within that environment.

A.1.45 Fish Stock

Scientifically, a population of a species of fish that is isolated from other stocks of the same species and does not interbreed with them and can, therefore, be managed independently of other stocks (gene pools). However, in EU legislation the term "stock" is used to mean a species of fish living in a defined sea area. The two definitions are not always synonymous.

A.1.46 Fishery Management

The integrated process of information gathering, analysis, planning, decision making, the allocation of resources, formulation, and enforcement of fishery regulations that governs present and future fishing activities, in particular to ensure the continued productivity of a resource (EC 1999).

A.1.47 Fishery Management Plan (FMP)

A plan developed by a Regional Fishery Management to manage a fishery resource.

A.1.48 Fisherman

One who engages in fishing for sport, as an occupation, or for food.

A.1.49 Fishery

A term used for a lake, river or stream where people can catch fish, or even a particular kind of fish, such as bass or trout.

A.1.50 Fishing Access Site

The name and location of a place where angling is accepted.

A.1.51 Fisheries Regulations

Fisheries regulations are restrictions on fishing activities imposed by state governments, and are enforceable under various acts. Regulations also inform those anglers that do not require a fishing licence that they are still subject to such regulations. It is the angler's responsibility to ensure they are aware of the current and complete list of fishing regulations.

A.1.52 Fly Fishing

A method of fishing that utilizes an artificial fly, a long flexible rod, a reel, and line.

A.1.53 Fly Tying

The process of building fishing flies using thread and various other materials.

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

A.1.54 Game Fish

Species of fish, caught for sport, that fights hard when hooked. Legal game fish are defined in statutes. There are more fish sought for sport than are listed as game fish (compare with section A.1.55 below on "Game Fishing").

A.1.55 Game Fishing

Many years ago, the English gentry classified fish into categories. Salmon and trout were considered more palatable than the other varieties of fish, and were classified as "game" fish. All other fish present were classified as "coarse" fish (compare with section A.1.12 above on "Big Game Fishing", and section A.1.30 on "Coarse Fishing").

A.1.56 Gear

Any tools used to catch fish, such as rod and reel, hook and line, nets, traps, spears and baits.

A.1.57 Gutted Weight

The weight of fish with their viscera removed.

A.1.58 Habitat

The natural environment where animals, fishes, and plants live.

A.1.59 Habitats (and Species) Directive

Council Directive 92/43/EEC on the conservation of natural habitats and of wild flora and fauna, which requires EU member states to protect scheduled species and to designate and manage special areas of conservation (SAC).

A.1.60 Hydrology (Hydrologic)

The science that deals with the distribution, properties, and circulation of water on land surface, in the soil, underlying rocks, and in the atmosphere.

A.1.61 IGFA

The International Game Fish Association, located in Florida.

A.1.62 ICES

The International Council for the Exploration of the Sea, an independent scientific advisory body founded in 1902. It is funded by 19 member states' governments from around the North Atlantic (including Canada and the USA) and Baltic Sea. It encourages research into fish stocks, their biology and all factors (natural and man made) that may affect their abundance. It does not undertake research in its own right, but has a secretariat (in Copenhagen) to facilitate and co-ordinate collaboration, including fishery stock assessments, between member states.

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

A.1.63 ICZM

Integrated coastal zone management, which is the co-ordination of all activities, and regulatory and management functions, to safeguard all natural resources and processes found in and affecting the coastal zone.

A.1.64 Ice Fishing

A specialised form of angling for fishing through holes cut in the ice of frozen-over waters. The species sought include crappies, walleye, northern pike, pickerel, and perch, and the principal techniques are jigging and tilt (or tip-up) fishing. Jigging involves working a natural bait with a short stick, which has especially shaped handle around which the line is wound. In tilt fishing, the bait is fished static from a rig incorporating an arm or flag that tilts up to signal a bite.

A.1.65 Introduced Species

Any species that occurs outside its normal geographic range as a direct or indirect result of human activity, and has not been found to have occured naturally in the area in historic times. The term applies equally to non-self sustaining (alien) populations and to established non-native species.

A.1.66 Ichthyology

The specific branch of zoology that deals with the study of fishes.

A.1.67 Jigging

Fishing by jerking a jig or other bait up and down in the water (typically an ice-fishing technique, but also used for cephalopode fishing).

A.1.68 Jig

A small artificial lure with a metal head, often dressed with feathers.

A.1.69 Keeper

For anglers, typically any fish that is worth taking home to eat. For lakes with special regulations, it can be fish of specified lengths that are legal to harvest, like in fisheries where there are slot limits.

A.1.70 Lake Fishing

All kinds of recreational fishing activities in large (mostly natural) lakes.

A.1.71 Limit-out

To catch the daily limit legally allowed for a species of fish.

A.1.72 Marine Stewardship Council (MSC)

A non-governmental organisation that encourages consumers to purchase fish taken only from environmentally responsible and sustainable fisheries. All fish products that MSC judge to be from such sustainable fisheries will be permitted to carry an “eco-friendly” seal of approval.

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

A.1.73 Marine Recreational Anglers

Those people who fish in marine waters primarily for recreational purposes. Their catch is primarily for home consumption, although occasionally, a part or all of their catch may be sold and enter commercial channels.

A.1.74 Mariculture

Marine aquaculture.

A.1.75 Marine Protected Area (MPA)

Any area of intertidal or subtidal terrain, together with its overlying water and associated flora, fauna and historical and cultural features, that has been reserved by law or other effective means to protect part or all of the enclosed environment.

A.1.76 Migratory Fish

A high proportion of the commercially exploited species in the North Atlantic undergo migrations (directional movements of anything from a few hundred to tens of thousands of kilometres) during their lifetimes, if not seasonally.

A.1.77 Minimum Landing Size (MLS)

The smallest length at which it is legal to retain a fish or offer it for sale. Ideally, it is the minimum length at which not less than 50 per cent of a given species first reach sexual maturity.

A.1.78 Mobile Fishing Gear

Any gear that is towed or otherwise moved through the water, e.g., trawls, seines, dredges, et cetera.

A.1.79 Monofilament

A clear, supple nylon filament used in all types of fishing that is available in many breaking strengths (see section A.1.21 above on “Breaking Strength”) and diameters.

A.1.80 National Federation of Anglers (NFA)

The governing body for freshwater angling in England. The organisation actively promotes and encourages angling development from the grass roots level, through to clubs and regional bodies, to international squads.

A.1.81 Native Species

Self-sustaining populations that can be rare or commonplace, but have not been introduced into an area by human intervention, either deliberately or accidentally.

A.1.82 Natura 2000

The EU-wide network of protected sites established under the Birds Directive (SPA) and the Habitats Directive (SAC).

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

A.1.83 Nongame Fish

All species of fish that are not game fish (see also section A.1.54 above on “Game Fish”).

A.1.84 Over-fishing

Fishing pressure beyond what a sustainable population of fish or stocking effort can be maintained.

A.1.85 Pole Fishing

A way to fish using a simple fishing rod (usually very long, such as 10 metres) with no reel. Targets are mainly carp-like fishes.

A.1.86 Possession Limit

The maximum limit or amount of a fish species set by regulation that may be possessed at one time by any one person.

A.1.87 Put-and-take

Refers to a fishery where catchable-sized fish are stocked (typically trout, but not exclusively) and caught by anglers in a relatively short period of time.

A.1.88 Quota

A fixed proportion of the TAC allocated to each fishing nation. This national quota allocation is further sub-divided into quotas for specific areas, seasons, fisheries or organisations such as producer organisations (POs).

A.1.89 Recreational Fishing

Recreational fishing, also called sport fishing, is fishing for pleasure or competition. It can be contrasted with commercial fishing, which is fishing for profit; most frequently, it is represented by beach and boat angling.

A.1.90 Recreational Sea Fishing

Often not licensed, but is subject to minimum landing size (MLS) regulations, and its activities can be curtailed by quota restrictions.

A.1.91 Recruitment

The number of young fish that grow into adults during a specific time interval.

A.1.92 Release

Returning a fish, in the best possible condition after removal of the hook, to the water from which it was taken.

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

A.1.93 Rio Convention

UN Convention on Biodiversity (UNCED 1992).

A.1.94 Rules and Regulations

Recreational fishing has conventions, rules, licensing restrictions and laws that limit the way in which fish may be caught, the International Game Fish Association (IGFA) makes and oversees a set of voluntary obligations. Typically, these prohibit the use of nets and the catching of fish with hooks not in the mouth. Enforceable regulations are put in place by Governments to ensure sustainable practice amongst anglers. For example in the Republic of Ireland, the Central Fisheries Board oversees the implementation of all angling regulations, which include controls on angling lures, baits and number of hooks permissible, as well as licensing regimes and other conservation based restrictions.

A.1.95 Sea Fishing

All fishing activities in marine waters primarily for recreational purposes (Compare "Marine recreational anglers).

A.1.96 Size Limit

The legal length that a fish must be if it is in possession.

A.1.97 Slot Limit

Dictates that fish within a specified minimum and maximum size range must be released.

A.1.98 Specimen Fishing

Aims to catch just a specific fish species. Serious anglers spend a lot of money for the right specimen fishing tackle (such as rod, reel and equipment), which actually can make the difference in whether or not one lands a large specimen of the target fish. For example, specimen carp fishing is the fastest growing section of freshwater fishing in the world, with over 2.5 million registered members of carp angling societies.

A.1.99 Standing Stock

The total number or biomass of a population at a given time.

A.1.100 Stock Biomass

The total weight of all fish of all ages in a given population or stock.

A.1.101 Stock Enhancement

Any measure that will improve the abundance of a stock, but, more generally, also applied to hatchery rearing and releasing to the wild of fish, particularly salmon, crustacea and molluscs.

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

A.1.102 Sustainable Fisheries

Fisheries with an annual catch, including discards, that does not exceed the surplus production of the stock (i.e., does not exceed annual growth, plus recruitment, less the annual natural mortality).

A.1.103 Threatened Fish Species

Endangered fish species for which the categories, definitions and criteria used are those of the International Union Conservation of Nature Red List Categories (1994).

A.1.104 Total Allowable Catch (TAC)

The quantity of fish that can be taken from each stock each year. The figure is agreed on by the Fisheries Council of Ministers each December for the following year. EU member states are allocated a fixed proportion of the TAC as their national quota.

A.1.105 Total-fishingclub.com (TFC)

The largest online angling community in the UK (http://www.total-fishingclub.com)

A.1.106 UKBAP

The UK Biodiversity Action Plan, the Government's programme aimed at meeting some of its obligations under the UN Convention on Biodiversity (1992). A wide range of habitat action plans (HAP) and species action plans (SAP) are being implemented to help safeguard and improve the conservation status of priority habitats and priority species.

A.1.107 UK Rivers Network

An interesting network for recreational fishing. Its website (http://www.ukrivers.net/fishing.html) provides useful introductions, and a beginners' guide for recreational fishing novices. It also provides a useful introduction on fishing in general, "and everything you ever wanted to know". Furthermore, there are some comments concerning the significance of sport fishing, which is one of the top sports and pastimes in UK. There are over 4 million anglers in the UK, and some 34 million people fish in the US each year. Further the responsibility of Anglers for their environmental is stressed here: Anglers don't just enjoy themselves: they are at the front-line of river conservation. They have an interest in keeping rivers clean, well-stocked, and non-polluted.

A.1.108 VDSF

Verband Deutscher Sportfischer e.V., the umbrella organisation for German recreational anglers with around 700 000 members.

A.1.109 Waders

High topped waterproof boots. There are two main types used in fishing: boot foot and stocking foot. Boot foot waders have boots built in, which means that only they need to be worn. Stocking foot waders, in contrast, require the use of a pair of wading shoes, but provide better support and traction.

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

A.2 Terminology related to Online Gaming Communities

Katja Liesebach (GUF) and Christian Kahl (GUF)

A.2.1 Avatar

The term “avatar” stems from the Hinduism, and is used to describe the descending of a deity to earth. In the Internet world, avatars are graphical representatives of virtual identities. Within a Massively Multiplayer Online Game (MMOG), a player acts as such a fictional character (his or her so-called avatar), and controls its actions within the game. Avatars are used to characterise oneself and to be recognisable by others. In many games, they are described by various attributes (name, look, role, et cetera) that may be adapted by the player.

A.2.2 Guild

Guilds are groups of players within a Massively Multiplayer Online Game (MMOG). They typically have common goals within the game that cannot be achieved by a single player on his or her own. Therefore, the members of a guild act in a collaborative manner. Depending on the game, sometimes terms such as clan or alliance are used synonymously with guild.

A.2.3 Life Simulation

Life simulations can be, in general, compared to Massively Multiplayer Online Games (MMORPGs), but are not necessarily of a gaming character. Rather, they simulate parts of real life, and often contain controls for one or more virtual life forms [6]. Life Simulations therefore have strong economic and legal relations to the real world. Often, avatars control, or have a bearing on, all aspects of digital life.

A.2.4 Massively Multiplayer Online Game (MMOG)

A multiplayer or online game is a video or computer game that can be played by multiple players simultaneously over a network (usually the Internet and/or LAN). The term “Massively Multiplayer Online Game” describes games (also called MMOGs or simply MMOs) that are only playable online, in contrast to single player games, which have an additional multiplayer mode. With the growing availability of broadband Internet access, massively multiplayer online games have become available and accessible for a mass market. They allow millions of players to connect and play the same game together online.

Different genres of MMOGs exist, such as:

- MMORPG (Massively multiplayer online role-playing game) (e.g., *World of Warcraft*, *EVE Online*, *Final Fantasy XI*).
- MMORTS (Massively multiplayer online real-time strategy) (e.g., *Travian*, *Saga*, *Mankind*).
- MMOFPS (Massively multiplayer online first-person shooter) (e.g., *PlanetSide*, *Huxley*, *Darkfall*).

A.2.5 Massively Multiplayer Online Role-Playing Game (MMORPG)

In such massively multiplayer online games, a player takes the role of a character within at least one persistent world. A persistent world is a virtual world comparable to the real world that is enduringly accessible for a player and still exists when a player is not online or actively participating.

A.2.6 Massively Multiplayer Online Real-Time Strategy (MMORTS)

According to *Wikipedia*, MMORTSs can be described as follows:

> *Massively Multiplayer Online Real-Time Strategy is a genre of online computer game that combines real-time strategy (RTS) with a large number of simultaneous players over the Internet. Players will often assume the role of a general, king or figurehead of some kind, leading an army into battle, while at the same time maintaining the resources needed for such warfare. The titles are often based in a sci-fi or fantasy universe and are distinguished from single or small-scale multiplayer RTSs by the number of players and common use of a persistent world, generally hosted by the game's publisher, which continues to evolve even when the player is not currently playing.*

A.2.7 Massively Multiplayer Online First-Person Shooter (MMOFPS)

According to *Wikipedia*, MMORTSs can be described as follows:

> *Massively multiplayer online first-person shooter (MMOFPS) is a sub-category of the massively multiplayer online game (MMOG) Internet computer game genre, which combines first-person shooter-style game play with the game design elements that typify the MMOG genre; namely, a persistent world populated by a large number of concurrent players, and in-depth player character progression mechanics. Whereas most MMOGs typically feature relatively slow-paced, "turn-based" combat, an MMOFPS requires a high degree of hand-eye coordination and twitch-based skills.*

A.2.8 Mobile/Pervasive Gaming

A "pervasive game is a game that has one or more salient features that expand the contractual magic circle of play socially, spatially or temporally" [40]. The terms mobile gaming and pervasive gaming are often used synonymously. Mobile games are played by using mobile devices.

A.2.9 Non-Player Character (NPC)

An in-game character controlled by a computer.

A.2.10 Play

According to [28], "play is a voluntary activity or occupation executed within certain fixed limits of time and place, according to rules freely accepted but absolutely binding, having its aim in itself and accompanied by a feeling of tension, joy and the consciousness that it is 'different' from 'ordinary life'". The term "gaming" is often used as a synonym for playing a game.

A.2.11 Player Character (PC)

An in-game character controlled by a human player.

A.2.12 Virtual Worlds

"The term Virtual Worlds describes online immersive, 'game-like' environments where participants engage in socialization, entertainment, education, and commerce. As a genre, these environments are classified as massively multiplayer online (i.e., MMO) virtual environments" [38].

Virtual worlds can be divided into Massively Multiplayer Online Games like *World of Warcraft* (http://www.wow-europe.com) and *Travian* (http://www.travian.org), and Life Simulations, such as Second Life (http://secondlife.com).

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

A.3 List of terms included in the deliverable

2.1 Terminology related to communities and usability

2.1.1 Basic terminology for online and mobile environments
2.1.1.1 Context-rich Environments
2.1.1.2 Web 2.0
2.1.1.3 User
2.1.1.4 Stakeholder
2.1.1.5 Client
2.1.1.6 Interaction
2.1.1.7 Online Collaboration
2.1.1.8 Content
2.1.1.9 Social Capital
2.1.1.10 Social Cohesion
2.1.1.11 Community Cohesion
2.1.2 Communities
2.1.2.1 Social Network
2.1.2.2 Social Network Analysis (SNA)
2.1.2.3 Node
2.1.2.4 Communities
2.1.2.5 Types of Communities
2.1.2.6 Online Community/Virtual Community
2.1.2.7 Mobile Community
2.1.2.8 Social Networking Community
2.1.2.9 Mass Online Social Network
2.1.2.10 Community Member
2.1.2.11 (Online) Community Service
2.1.2.12 Social Networking Service
2.1.2.13 (Community) Service Provider
2.1.2.14 Service Aggregators
2.1.2.15 Collaborative Software
2.1.2.16 Social Software/Social Network Application
2.1.2.17 Social Media and Content Sharing
2.1.2.18 Blogs and Microblogs
2.1.2.19 Forum
2.1.2.20 Wiki
2.1.2.21 Chat Room
2.1.2.22 Instant Messaging
2.1.2.23 Web Portal
2.1.2.24 Community Web Portal
2.1.2.25 Social Bookmarking
2.1.2.26 Social News
2.1.2.27 Social Tagging/Folksonomy
2.1.2.28 Social Searching
2.1.2.29 Social Browsing
2.1.3 Usability
2.1.3.1 Human-Computer Interaction (HCI)

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

2.2.29 Mesh Network
2.2.30 Mobile Communication Services
2.2.31 Mobile Network Operator (MNO)
2.2.32 Mobile Subscriber Integrated Services Digital Network Number (MSISDN)
2.2.33 Network Authentication
2.2.34 Next Generation Network
2.2.35 Peer to Peer (P2P)
2.2.36 Policy Decision Point (PDP)
2.2.37 Policy Enforcement Point (PEP)
2.2.38 Presence Information
2.2.39 Privacy Rights Management
2.2.40 Public Communications Network
2.2.41 Public Key Infrastructure (PKI)
2.2.42 Public Service
2.2.43 Push-to-Talk (PTT)
2.2.44 Roaming
2.2.45 SIM card
2.2.46 Traffic data
2.2.47 Trusted Third Party
2.2.48 Value Added Service
2.2.49 WAP
2.2.50 Wireless
2.2.51 WLAN

2.3 Introductory terminology on privacy, identity management and trust

2.3.1 Accountability
2.3.2 Anonymity
2.3.3 Anonymity Set
2.3.4 Anonymous
2.3.5 Certificate
2.3.6 Civil Identity
2.3.7 Convertibility
2.3.8 Credential
2.3.9 Decentralised Trust
2.3.10 Delegation
2.3.11 Dependability
2.3.12 Digital Identity
2.3.13 Digital Pseudonym
2.3.14 End Entity
2.3.15 Entitlement Assessment
2.3.16 Fair Information Practices (FIP)
2.3.17 False Identity
2.3.18 Group Pseudonym

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

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

2.5.5 Attribute Certificate (AC)
2.5.6 Attribute Certificate Revocation List (ACRL)
2.5.7 Authentication Token (Token)
2.5.8 Authority
2.5.9 Authority Certificate
2.5.10 Base CRL
2.5.11 Biometric Encryption/Decryption
2.5.12 Biometric Enrolment
2.5.13 Biometric Sample
2.5.14 Biometric Template
2.5.15 Biometric Threshold
2.5.16 CA-certificate
2.5.17 Cancellable Biometrics
2.5.18 Certificate Policy
2.5.19 Certification Practice Statement (CPS)
2.5.20 Certificate Revocation List (CRL)
2.5.21 Certificate User
2.5.22 Certificate Serial Number
2.5.23 Certificate-using System
2.5.24 Certificate Validation
2.5.25 Certification Authority (CA)
2.5.26 Certification Authority Revocation List (CARL)
2.5.27 Certification Path
2.5.28 Claim
2.5.29 Controlled Release
2.5.30 CRL Distribution Point
2.5.31 Cross-certificate
2.5.32 Cryptographic System (Cryptosystem)
2.5.33 Data Confidentiality
2.5.34 Data Integrity
2.5.35 Data Availability
2.5.36 Data Sharing
2.5.37 Delegation
2.5.38 Delegation Path
2.5.39 Delta-CRL (dCRL)
2.5.40 Device
2.5.41 Directory Information Tree (DIT)
2.5.42 Distributed Service Architectures
2.5.43 End-entity Attribute Certificate Revocation List (EARL)
2.5.44 End-entity Public-key Certificate Revocation List (EPRL)
2.5.45 Environmental Variables
2.5.46 Full Certificate Revocation List

2.5.47 Hash Function
2.5.48 Holder
2.5.49 Identity Federation
2.5.50 Identity Management System (IMS)
2.5.51 Indirect Certificate Revocation List (iCRL)
2.5.52 International Organization for Standardization (ISO)
2.5.53 ISO/IEC JTC 1
2.5.54 ISO/IEC JTC 1 SC 27
2.5.55 ISO/IEC JTC 1 SC 27 WG 5
2.5.56 Key Agreement
2.5.57 Mix
2.5.58 Object Method
2.5.59 One-way Function
2.5.60 Onion Routing
2.5.61 P3P
2.5.62 Platform
2.5.63 Platform Virtualisation
2.5.64 Policy Mapping
2.5.65 Privacy-Enhancing Identity Management System (PE-IMS)
2.5.66 Privacy Preferences
2.5.67 Private Key
2.5.68 Privilege
2.5.69 Privilege Asserter
2.5.70 Privilege Management Infrastructure (PMI)
2.5.71 Privilege Policy
2.5.72 Privilege Verifier
2.5.73 Public Key
2.5.74 Public Key Certificate (PKC)
2.5.75 Public Key Infrastructure (PKI)
2.5.76 Reliability
2.5.77 Relying party
2.5.78 Role Assignment Certificate
2.5.79 Sensitivity
2.5.80 Simple Authentication
2.5.81 Security Policy
2.5.82 Self-issued Attribute Certificate (Self-issued AC)
2.5.83 Self-issued Certificate
2.5.84 Self-signed Certificate
2.5.85 Source of Authority (SOA)
2.5.86 Spoke-hub
2.5.87 Strong Authentication
2.5.88 Trust Anchor

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

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

A.1.24 "Buy your rod licence online"
A.1.25 Car Fishing
A.1.26 Carrying Capacity
A.1.27 CFP
A.1.28 Charismatic Species
A.1.29 Closed Seasons
A.1.30 Coarse Fishing
A.1.31 Coast Fishing
A.1.32 Cohort
A.1.33 Collapsed Stock
A.1.34 Creel Limit
A.1.35 CPR
A.1.36 DG Environment
A.1.37 Discards
A.1.38 European Anglers Alliance (EAA)
A.1.39 Exclusive Economic Zone (EEZ)
A.1.40 European Fishing Tackle Trade Association (EFTTA)
A.1.41 Ecology
A.1.42 Ecosystem
A.1.43 Eddy
A.1.44 Environmentally Sustainable Fisheries
A.1.45 Fish Stock
A.1.46 Fishery Management
A.1.47 Fishery Management Plan (FMP)
A.1.48 Fisherman
A.1.49 Fishery
A.1.50 Fishing Access Site
A.1.51 Fisheries Regulations
A.1.52 Fly Fishing
A.1.53 Fly Tying
A.1.54 Game Fish
A.1.55 Game Fishing
A.1.56 Gear
A.1.57 Gutted Weight
A.1.58 Habitat
A.1.59 Habitats (and Species) Directive
A.1.60 Hydrology (Hydrologic)
A.1.61 IGFA
A.1.62 ICES
A.1.63 ICZM
A.1.64 Ice Fishing
A.1.65 Introduced Species

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

A.1.66 Ichthyology
A.1.67 Jigging
A.1.68 Jig
A.1.69 Keeper
A.1.70 Lake Fishing
A.1.71 Limit-out
A.1.72 Marine Stewardship Council (MSC)
A.1.73 Marine Recreational Anglers
A.1.74 Mariculture
A.1.75 Marine Protected Area (MPA)
A.1.76 Migratory Fish
A.1.77 Minimum Landing Size (MLS)
A.1.78 Mobile Fishing Gear
A.1.79 Monofilament
A.1.80 National Federation of Anglers (NFA)
A.1.81 Native Species
A.1.82 Natura 2000
A.1.83 Nongame Fish
A.1.84 Over-fishing
A.1.85 Pole Fishing
A.1.86 Possession Limit
A.1.87 Put-and-take
A.1.88 Quota
A.1.89 Recreational Fishing
A.1.90 Recreational Sea Fishing
A.1.91 Recruitment
A.1.92 Release
A.1.93 Rio Convention
A.1.94 Rules and Regulations
A.1.95 Sea Fishing
A.1.96 Size Limit
A.1.97 Slot Limit
A.1.98 Specimen Fishing
A.1.99 Standing Stock
A.1.100 Stock Biomass
A.1.101 Stock Enhancement
A.1.102 Sustainable Fisheries
A.1.103 Threatened Fish Species
A.1.104 Total Allowable Catch (TAC)
A.1.105 Total-fishingclub.com (TFC)
A.1.106 UKBAP
A.1.107 UK Rivers Network

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

3 References

[1] *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*, Official Journal L 281/31.

[2] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (eSignatures Directive)*, Official Journal L 13/12.

[3] *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 108/33.

[4] *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 201/37

[5] *PRIME Glossary*; available online at: https://prime.inf.tu-dresden.de/prime/space/Dictionary.

[6] Adams, E. and Rollings, A., *Fundamentals of Game Design (Game Design and Development)*. 2006, New York: Prentice Hall.

[7] Applied Biometrics. available online at: http://www.appliedbiometrics.co.uk/biometrics/what-is-biometrics.

[8] Avizienis, A., et al., *Fundamental Concepts of Dependability*. Research Report No 1145, LAAS-CNRS.

[9] Beinhauer, M., et al., *Virtual Community – Kollektives Wissensmanagement im Internet*, in *Electronic Business and Knowledge Management – Neue Dimensionen für den Unternehmenserfolg*, A.W. Scheer, Editor. 1999, Physica Verlag: Heidelberg.

[10] Bishop, M., *Introduction to Security*. 2004.

[11] Camenisch, J. and Lysyanskaya, A. *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation*. in *EUROCRYPT 2004, Lecture Notes in Computer Science 2045*. 2001.

[12] Cavoukian, A., *Biometric Encryption - A positive sum-technology that achieves strong authentication, security AND privacy*. 2007.

[13] Chaum, D., *Security without identification: Transaction systems to make Big Brother obsolete.* Communications of the ACM. **28**(10): p. 1030-1044.

[14] Clayton, R. *The Limits of Traceability*, 2001; available online at: http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html.

[15] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, *Opinion of the T-PD n the interpretation of the concepts of automatic processing and controller of the file in context of worldwide telecommunications networks.* as adopted by the T-PD at its 23rd meeting, T-PD-BUR (2006) 08 E fin (Strasbourg, 15 March 2007), 2007.

[16] Cooper, A., *The Inmates Are Running the Asylum: Why High-Tech Products Drive Us Crazy and How to Restore the Sanity*. 1999, Indianapolis: SAMS.

[17] Daniel, B., et al., *Social Capital in Virtual Learning Communities and Distributed Communities of Practice.* Canadian Journal of Learning and Technology, 2003. **29**(3).

[18] Egger, F.N., *From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce.* PhD Thesis, Eindhoven University of Technology (The Netherlands). ISBN 90-386-1778-X, 2003.

[19] Erdmann, M., et al., *From Manual to Semi-automatic Semantic Annotation: About Ontology-based Text Annotation Tools.* Electronic Transactions on Artificial Intelligence, URL: http://www.ida.liu.se/ext/epa/ej/etai/2001/015/01015-etaibody.pdf

[20] European Commission, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs),* COM/2007/0228 final.

[21] Ferroni, M., *Social Capital and Social Cohesion: Definition and Measurement. Medicion de la Calidad de Vida.* (IDB) Sustainable Development Department. Inter-American Development Bank. Washington DC. Taller de Consulta sobre. December 8, 2006. PowerPoint Presentation. URL: http://www.iadb.org/res/publications/pubfiles/pubP-854.ppt. .

[22] Fischer-Hübner, S. and Hedbom, H., *D14.1.c – PRIME Framework V3. Public Project Deliverable.* March 17, 2008.

[23] Fremuth, N. and Tasch, A.E., *Virtuelle und mobile Communities*, in *Working Report for Institute for Information, organisation, and Management at Technische*, R. Reichwald, Editor. 2002, Universität München: München.

[24] Futurelab, *Innovation In Education.* URL: http://futurelab.org.uk/glossary/

[25] Groh, G., *Ad-Hoc Groups in Mobile Communities – Detection, Modelling and Applications.* PhD Dissertation, available online at http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2005/groh.pdf, 2005.

[26] Grosky, B., *Keynote on The Multimedia Semantic Web.* URL: http://lsdis.cs.uga.edu/SemWebCourse_files/Grosky-Keynote.ppt

[27] Hill, C. and O'Hara, E., *A Cognitive Theory of Trust.* Minnesota Legal Studies, 2005(Research Paper No. 05-51).

[28] Huizinga, J., *Homo Ludens: A Study of the Play-Element in Culture*. 1950, Boston: Beacon Press.

[29] ITU, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, in *Series X: Data Networks, Open System Communications and Security, ITU-T X.509 TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU*. 2005.

[30] Jain, A., et al., *Biometric Template Selection: A case Study in Fingerprints.* Appeared in Proc. of 4th Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA), LNCS 2688, pp. 335-342, Guildford, UK, 2003.

[31] Jeannotte, S.M., *Social Cohesion Around the World: An International Comparison of Definitions and Issues.* Prepared for the Strategic Research and Analysis Directorate, Department of Canadian Heritage, 2001.

[32] Keoh, S.L., et al., *PEACE : A Policy-based Establishment of Ad-hoc Communities.* Proceedings of the 20th Annual Computer Security Applications Conference, 2004: p. 386-395.

[33] Koch, M., et al., *Mobile Support for Lifestyle Communities*, in *Working Report for Institute for Information, organisation, and Management at Technische*, R. Reichwald, Editor. 2002, Universität München: München.

[34] Kohlweiss, M. and Rannenberg, K., *D5.1.a – PRIME Overview of existing assurance methods in the area of privacy and IT security*. June 01, 2005.

[35] Koller, M., *Risk as a Determinant of Trust.* Basic and Applied Social Psychology, 1988. **9**(4): p. 265-276.
[36] Lampe, C., et al., *A Face(book) in the Crowd: Social Searching vs. Social Browsing.* 2006.
[37] Lohse, C., *Online Communities.* Thesis at Technische Universität München, 2002.
[38] Mennecke, B.E., et al., *Second Life and Other Virtual Worlds: A Roadmap for Research.* 28th International Conference on Information Systems (ICIS), 2007.
[39] Ministry of the Interior and Kingdom Relations, t.N., *Privacy –Enhancing Technologies White Paper for Decision-Makers*. December 2004.
[40] Montola, M., *Exploring the Edge of the Magic Circle: Defining Pervasive Games.* DAC 2005 conference. University of Copenhagen, Copenhagen, 2005.
[41] Müller-Prothmann, T., *Leveraging Knowledge Communication for Innovation - Framework, Methods and Applications of Social Network Analysis in Research and Development*. Europäische Hochschulschriften. 2006, Frankfurt Peter Lang.
[42] National Institute of Standards and Technology. *NIST policy on traceability*; available online at: http://ts.nist.gov/Traceability/Policy/nist_traceability_policy-external.cfm.
[43] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules, FIPS PUB 140-2*.
[44] Nooy, W.d., et al., *Exploratory Social Network Analysis with Pajek*. 2005, Cambridge: Cambridge University Press.
[45] O'Reilly, T., *Web 2.0 Compact Definition: Trying Again.* URL: http://radar.oreilly.com/archives/2006/12/web-20-compact-definition-tryi.html. , 10 December 2006.
[46] O'Reilly, T., *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*. URL: http://www.oreilly.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html. , 30 September 2005.
[47] Pfitzmann, A. and Hansen, M., *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology.* available at: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.
[48] PRIVARIS. *Biometric security glossary*; available online at: http://www.privaris.com/library/biometrics_security_glossary.html.
[49] Pruitt, J. and Adlin, T., *The Persona Lifecycle – Keeping People in Mind Throughout Product Design*. 2006, San Francisco: Morgan Kaufmann.
[50] Ratha, N.K., et al., *Enhancing Security and Privacy in Biometrics-based Authentication Systems.* IBM Systems Journal 2001. **40**(3): p. 614-634.
[51] Renaud, J.-F., *Integrate Social Media into the Web Strategy: an overview.* URL: http://www.adviso.ca/en/integrate-social-media-into-the.html February 2008.
[52] Rotter, J.B., *Interpersonal Trust, Trustworthiness, and Gullibility.* American Psychologist, 1980. **35**(1): p. 1-7.
[53] Schmidt, J., *Social Software: Onlinegestütztes Informations-, Identitäts- und Beziehungsmanagement.* Forschungsjournal Neue Soziale Bewegungen, 2006. **2006**(2): p. 37-46.
[54] Sirianni, C. and Friedland, L., *Social Capital.* URL: http://www.cpn.org/tools/dictionary/capital.htmlhttp://www.cpn.org/tools/dictionary/capital.html. , 1995.
[55] Solove, D., *A Taxonomy of Privacy.* University of Pennsylvania Law Review. **154**(3): p. 477.

[56] SSE-CMM, *Systems Security Engineering Capability Maturity Model Project, Systems Security Engineering Capability Maturity Model, Version 2.0, April 1999.*
[57] Staab, S., et al., *Semantic Community Web Portals.* Computer Networks, June 2000. **33**(1): p. 473-491.
[58] The Common Criteria, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model.* Available from http://www.oc.ccn.cni.es/pdf/CCPART1V2.2R326.PDF.
[59] Tuomi, I., *Internet, Innovation and Open Source: Actors in the Network.* First Monday, 2001. **6**(1).
[60] United States of America, D.o.D., *Trusted Computer Systems Evaluation Criteria, , DoD 5200.28-STD.* 1985.
[61] Usecon, *The Usability Consultants.* URL: http://usecon.com/ [Last Access: 2008-06-05].
[62] Vander Wal, T., *Folksonomy Coinage and Definition.* URL: http://www.vanderwal.net/folksonomy.html Feb 2007.
[63] Voss, J., *Tagging, Folksonomy & Co - Renaissance of Manual Indexing?* arXiv:cs/0701072v2, 2007.
[64] Webopedia, http://www.webopedia.com/TERM/I/instant_messaging.html
[65] Website of Castle Morpeth Borough Council. *Definition of Social Cohesion*; available online at: http://www.castlemorpeth.gov.uk/SERVICES/COUNCIL/EQUALITY_AND_DIVERSITY/Pages/CommunityCohesion.aspx.
[66] Weill, P. and Ross, J., *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. 2004, Boston Harvard Business School Press.
[67] Wikipedia, www.wikipedia.org.