PICOS: Legal, economic and technical evaluation of the first platform and community prototype

Isaac Agudo
University of Malaga
53 PUBLICATIONS 416 CITATIONS
SEE PROFILE

Mohamed Bourimi
DB Systel
65 PUBLICATIONS 453 CITATIONS
SEE PROFILE

Stefan Eicker
University of Duisburg-Essen
57 PUBLICATIONS 154 CITATIONS
SEE PROFILE

Eva Ganglbauer
14 PUBLICATIONS 224 CITATIONS
SEE PROFILE

Grant Agreement no. 215056

`

Title:	***D8.1 Legal, economic and technical evaluation of the first platform and community prototype***
Editor:	*Eleni Kosta (Katholieke Universiteit Leuven)*
Reviewers:	*Jean-François Coudeyre (Hewlett-Packard Centre de Compétence France)*
	Stefan Eicker (IT-Objects GmbH)
	Erik Heimann (IT-Objects GmbH)
Identifier:	*D8.1*
Type:	*Deliverable*
Version:	*1.0*
Date:	*26.04.2010*
Status:	*Final*
Class:	*Public*

Summary

In this deliverable a multi-disciplinary evaluation of the work performed during the first cycle of the PICOS project is conducted. The PICOS Platform Design and Architecture v1, the PICOS Platform Prototype v1 and the PICOS Angling Community Application Prototype v1 are evaluated from a legal, economic, technical and usability point of view. This multi-disciplinary evaluation focuses on the privacy and trust related elements of the PICOS project. One of the main aims of this evaluation is to highlight the PICOS concepts and to assess the way in which they were implemented in the PICOS platform design and architecture, the PICOS platform prototype and the PICOS Angling Community Prototype during the first cycle of the project. Based on their findings, the evaluators further propose recommendations that will be taken into account for the design and the development of the PICOS platform and application prototypes during the second cycle. The evaluation of the assurance in PICOS is conducted in detail under WP3, the outcome of which is already included in deliverables D3.1.1, D3.2.1 and D3.3.1. Given the fact that the WP3 deliverables are confidential, this present deliverable contains for reasons of completeness also a summary of the basic findings of the Assurance evaluation.

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 Compétence 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

D2.1 Taxonomy	July 2008
D2.2 Categorisation of Communities	July 2008
D2.3 Contextual Framework	November 2008
D2.4 Requirements	November 2008
D4.1 Platform Architecture and Design v1	March 2009
D5.1 Platform description document v1	October 2009
D6.1 Community Application Prototype 1	December 2010
D7.1a User Evaluation Plan	December 2009
D7.2a First Community Prototype: Lab and Field Test Report	February 2010
D9.1 Web Presence	February 2008
D9.2.1 Exploitation Planning	May 2009
D9.3.1 Dissemination Planning	May 2009

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

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

Grant Agreement no. 215056

The PICOS Deliverable Series

Vision and Objectives of PICOS

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

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

PICOS documentation

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

Planned PICOS results

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

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

Foreword

PICOS partners from various disciplines have contributed as authors to this document.

As the title of the deliverable “Legal, economic and technical evaluation of the first platform and community prototype” clearly indicates, Deliverable D8.1 is a collective work by the WP8 Evaluation team whose members are listed below. Each partner contributed expertise in different fields of knowledge which resulted in a truly multi-disciplinary evaluation of the PICOS platform design and architecture, the PICOS platform prototype and the PICOS Angling Community Application Prototype.

Special mention goes to Pete Bramhall and Stephen Crane (HP Labs) for providing a very comprehensive summary of the work realised in the context of WP4 (PICOS Platform design and architecture) and WP5 (PICOS Platform Prototype), and to Alberto Crespo Garcia, for the thorough presentation of the work conducted in WP6 (PICOS Angling Community Prototype.

The Contributors to the D8.1: “Legal, economic and technical evaluation of the first platform and community prototype” are:

Isaac Agudo, Mohamed Bourimi, Stefan Eicker, Eva Ganglbauer, Stephan Heim, Eleni Kosta, Georg Kramer, Marek Kumpošt, Vashek Matyas, Karsten Radatz, Johann Schrammel, José Luis Vivas

(ATOS, BRNO, CURE, DTAG, GUF, HP Labs, ITO, K.U.Leuven, UMA)

Reviewers:

Jean-François Coudeyre, Hewlett-Packard Centre de Competence, France (HPF)

Stefan Eicker, IT-Objects GmbH, Germany (ITO)

Erik Heimann, IT-Objects GmbH, Germany (ITO)

Editor:

Eleni Kosta, ICRI – Katholieke Universiteit Leuven, Belgium (K.U.Leuven)

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

Table of Contents

Summary **1**

The PICOS Deliverable Series **3**

Foreword **4**

Table of Contents **5**

List of acronyms **7**

1 Introduction **8**

2 Assurance **10**

2.1.1 Assurance methodology 10
2.1.2 Analysis of the platform prototype implementation 11
2.1.3 Analysis of the first community prototype 13
2.1.4 Recommendations based on the assurance evaluation 18

3 Evaluation of the Platform Design & Architecture (WP4) **19**

3.1 Summary presentation of the Platform Design & Architecture ***19***
3.2 Legal Evaluation ***21***
3.2.1 Methodology used 21
3.2.2 Evaluation of the requirements and functionalities of the Platform design and architecture 22
3.2.3 Summary of findings and recommendations 24
3.3 Technical evaluation ***25***
3.3.1 Trust, Privacy & other technical elements 25
3.3.2 Community focus 30
3.3.3 Location based services and communication features 33
3.4 Economic evaluation ***37***
3.4.1 Methodology used 37
3.4.2 Documentation used 37
3.4.3 Evaluation of the requirements and functionalities of the Platform design and architecture 38
3.4.4 Summary of findings and recommendations 41

4 Evaluation of the Platform Prototype (WP5) **42**

4.1 Summary presentation of the Platform Prototype ***42***
4.1.1 Overview 42
4.1.2 Implementation 42
4.1.3 Client – platform interaction 44
4.2 Legal evaluation ***44***
4.2.1 Methodology used 44
4.2.2 Documentation used 44
4.2.3 Evaluation of the requirements and functionalities of the Platform Prototype 45
4.2.4 Summary of findings and recommendations 49
4.3 Technical evaluation ***49***
4.3.1 Trust, Privacy & other technical elements 49

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

4.3.2 Community focus 53
4.3.3 Location based services and communication features 57
4.4 Economic evaluation 61
4.4.1 Methodology used 61
4.4.2 Documentation used 61
4.4.3 Evaluation of the requirements and functionalities of the Platform Prototype 61
4.4.4 Summary of findings and recommendations 65

5 Evaluation of the Angling Community Prototype (WP6) 66

5.1 Summary presentation of the Angling Community Prototype 66
5.2 Legal evaluation 69
5.2.1 Methodology used 69
5.2.2 Documentation used 69
5.2.3 Compliance with data protection principles 69
5.2.4 Location Based Service (LBS) 73
5.2.5 Summary of findings and recommendations 74
5.3 Technical evaluation 74
5.3.1 Trust, Privacy & other technical elements 74
5.3.2 Community focus 78
5.3.3 Location based services and communication features 81
5.4 Economic evaluation 85
5.4.1 Methodology used 85
5.4.2 Documentation used 85
5.4.3 Evaluation of the requirements and functionalities of the Angling Community Prototype 85
5.4.4 Summary of findings and recommendations 88
5.5 Usability evaluation 88
5.5.1 Methodology used 89
5.5.2 Documentation used 92
5.5.3 Installation – Functionality & Operation 93
5.5.4 Evaluation of the requirements and functionalities of the Angling Community Prototype 93
5.5.5 Summary of findings and recommendations 101

6 Conclusions and recommendations for the developers 102

7 Appendix I 106

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

List of acronyms

ABD	*Assurance Based Development*
API	*Application Programming Interface*
CA	*Certification Authority (X.509)*
IDE	*Integrated Development Environment*
J2ME	*Java 2 Mobile Edition*
LBS	*Location Based Services*
OTA	*Over The Air*
PET-USES	*Privacy Enhanced Technology – User's Self Estimation Scale*
PUC	*PICOS Use Case*
RPC	*Remote Procedure Call*
SDK	*Software Development Kit*
SSO	*Single Sign On*
SUS	*System Usability Scale*
SVN	*Subversion*
UML	*Unified Modelling Language*
WSDL	*Web Services Description Language*

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

1 Introduction

The objective of the present PICOS Deliverable 8.1 “Legal, economic and technical evaluation of the first platform and community prototype” is, as it is clearly indicated by the title of the deliverable, to provide a legal, economic and technical evaluation of the work performed during the first cycle of the PICOS project. More specifically the aim of PICOS D8.1 is to conduct a multi-disciplinary evaluation of the PICOS Platform Design and Architecture v1, the PICOS Platform Prototype v1 and the PICOS Angling Community Application Prototype v1, focusing on trust and privacy elements, as implemented via the PICOS project, and more specifically on the determination of trust and privacy needs in the context-rich mobile communication services. The outcome of this evaluation is on the one hand the assessment from a legal, technical, economic and usability (where applicable) point of view of the privacy and trust aspects of the PICOS project and on the other hand the drafting of recommendations that will be taken into account for the design and the development of the PICOS platform and application prototypes during the second cycle.

The work of this present deliverable is complemented by the work conducted in WP3 “Assurance of Technical Trust and Privacy Properties”. One of PICOS main goals is to ensure that assurance is an integral constituent of the PICOS solution[1]. Therefore the PICOS project has dedicated a separate Workpackage -WP3- to the assurance of technical trust and privacy properties of the platform and application prototypes[2]. WP3 aims at ensuring that the PICOS platform architecture and design achievements, as well as the platform and application prototypes developments of the project, are accurate and consistent with the trust and privacy technical objectives planned. The work conducted in WP3 during the first cycle of the PICOS project focuses on the assurance evaluation of (a) the PICOS platform design and architecture v1, (b) the PICOS Platform Prototype v1 and (c) the PICOS Angling Community Application Prototype v1. The outcome of the assurance evaluation is included in three respective deliverables, i.e. D3.1.1 “Trust and Privacy Assurance for the Platform Design”, D3.2.1 “Trust and Privacy Assurance Evaluation of the Platform Prototype” and D3.3.1 “Trust and Privacy Assurance of the Community Prototype”. Given that the aforementioned WP3 deliverables are currently confidential, a summary of the main findings of the assurance evaluation are presented in Chapter 2 of this present deliverable. In this way the reader can be informed about the main results of the assurance evaluation during the first cycle of the PICOS project.

Methodologically, the evaluation for the needs of PICOS D8.1 “Legal, economic and technical evaluation of the first platform and community prototype” was conducted on the basis of Workpackages, in conformity also to the structural analysis of WP3, as described above. Therefore the evaluators were asked to conduct their evaluation in three parts: evaluation of (I) the PICOS Platform Design and Architecture v1, (II) the PICOS Platform Prototype v1 and (III) the PICOS Angling Community Application Prototype v1, assessing the work conducted in Workpackages WP4, WP5 and WP6 during the first project cycle respectively. The present deliverable D8.1 mirrors this structure and is divided into three main chapters: (I) Chapter 3: “Evaluation of the Platform Design & Architecture (WP4)”, (II) Chapter 4: “Evaluation of the Platform Prototype (WP5)”, and (III) Chapter 5: “Evaluation of the Angling Community Prototype (WP6)”. Each evaluation is divided into the following parts: (i) Legal evaluation, (ii) Technical evaluation (comprising of Trust and Privacy related evaluation, evaluation with a community focus and finally an evaluation of Location Based Services functionalities and Community features) and (iii) Economic evaluation. A usability

[1] PICOS ANNEX I – “Description of Work” (Amendment 2), v4.15, 11.01.2010, p.59.
[2] PICOS ANNEX I – “Description of Work” (Amendment 2), v4.15, 11.01.2010, p. 34 ff.

evaluation is also conducted for the PICOS Angling Community Prototype, something that would not be feasible or meaningful with regard to the PICOS Platform Design and Architecture (WP4) and the PICOS Platform Prototype (WP5).

These evaluation tasks aim at the identification of the strengths and the weaknesses according to the goals set up by the PICOS project. The multi-disciplinary evaluations will be used as a measure for goals that have already been achieved and as source for improvements to be made for the second iteration of the PICOS project. Finally, a quick usability report of the PICOS Angling Community Prototype is presented in Appendix I.

The evaluation of the PICOS platform design and architecture v1 (WP4) was conducted in a first phase. The evaluators prepared their evaluation by the beginning of December 2009, so that their findings could be provided to the WP4 developers in time for the second version of the PICOS platform design and architecture. The evaluation of the PICOS Platform Prototype v1 (WP5) and the PICOS Angling Community Application Prototype v1 (WP6) were completed in the beginning of February 2010 and again an early draft of the findings of the evaluators was sent to the respective Workpackage leaders, so that they are taken into account for the development of the second cycle.

The evaluators worked in close cooperation with the technical partners and the development team (WP4, WP5 and WP6). An internal evaluation/validation workshop took place in Vienna on the 25th of January 2010. The evaluators were provided with a PICOS enabled Nokia 5800 XpressMusic and they were given tasks in the form of a lab test. Moreover the evaluators were also taken on the streets of Vienna and they tested the PICOS Angling Community Prototype in a simulation of field tests. This valuable experience helped the evaluators in completing their task and in conducting a more comprehensive evaluation of the Angling Community Application Prototype v1.

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

2 Assurance

As already mentioned above, one of PICOS main goals is to ensure that assurance is an integral constituent of the PICOS solution. Therefore the PICOS project has dedicated a separate WP3 to the technical evaluation with regard to assurance of technical trust and privacy properties of the PICOS platform and application prototypes. During the first phase of the PICOS project, WP3 prepared three confidential deliverables, i.e. D3.1.1 “Trust and Privacy Assurance for the Platform Design”, D3.2.1 “Trust and Privacy Assurance Evaluation of the Platform Prototype” and D3.3.1 “Trust and Privacy Assurance of the Community Prototype”.

In the following sections, an overview of the work carried out in WP3 with regard to the assurance evaluation will be presented. For a complete description, the reader is referred to the document identified in the previous paragraph. In the present document, the reader will first be introduced to the assurance methodology adopted by the WP3 team and a summary of the main results of the assurance work in the first phase of PICOS will be given. The following part includes two sections that provide a comprehensive summary of the assurance evaluation results, carried out in WP3. Mainly the focus lies on the analysis of how well the PICOS platform and community prototypes meet the needs of trust and privacy in PICOS, with special emphasis on those aspects which the WP3 team considered that needed a closer attention in the second phase of the project. Finally some core recommendations that should be taken into account for the second phase of the PICOS project are presented.

2.1.1 Assurance methodology

An assurance methodology inspired by the Assurance Based Development (ABD) approach[3] has been developed in the context of PICOS WP3 (Assurance) in order to provide trust and privacy assurance of the PICOS results. A requirement of PICOS is that assurance should be an integral constituent of the PICOS solution and must be pursued in a holistic manner. Assurance should address the requirements, design, architecture, and implementation phases of the development of the PICOS platform. To this end, we propose a methodology enabling an integration of security engineering and assurance with the aid of the notion of security assurance case. Assurance is seen as an integral security engineering component, not simply as a documenting task for external review.

Security engineering as a discipline is concerned with building dependable and secure systems that resist not only error or mischance, but also malicious behaviour. The best way to acquire confidence that a system meets its requirements is by the application of sound system engineering methodologies and procedures. Assurance can be best achieved by focusing on these procedures, documenting them, extracting from them the evidence and argumentation needed to build the assurance case, showing how they contribute to the achievement of the established security goals, and acting upon the decisions taken during the whole system development effort. Assurance should not be simple documentation exercise separate form security engineering.

In its analysis WP3 makes an evaluation of the trust and privacy aspects of the platform design and architecture, the platform prototype, and the community prototype. They defined 24 privacy principles and 8 trust principles that were relevant for PICOS according to the established PICOS requirements. This work resulted in a series of observations about the components, their functionality and

[3] Graydon Patrick J., Knight John C., Strunk Elisabeth A., Assurance Based Development of Critical Systems. In 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN ’07), pp. 347-357, 2007.

dependencies, both in the architecture and in the platform prototype. Several observations about possible omissions and inconsistencies were put forward, intended to become the main input of the assurance work to developers in the subsequent stages of development of the PICOS platform, as it will be further elaborated below.

2.1.2 Analysis of the platform prototype implementation

In this section we give a summary of the main recommendations for developers, after the assurance evaluation of PICOS first prototype implementation, concerning some of the PICOS trust and privacy principles (presented in D3.1.1), which we considered needed special attention.

2.1.2.1 PrP1 Notice of collection

Notice of the purpose of collection must be provided, eventually by Registration component, before any data collection during registration.

2.1.2.2 PrP2 Policy notification

Notice of the policy enforced by the community must be provided, eventually by Registration component, before any data collection during registration.

2.1.2.3 PrP6 Informed Consent

It must be ensured that informed consent is provided by the user during registration, suitably by the Registration component, either through the terms and conditions, or immediately before the collection of personal information.

2.1.2.4 PrP8 Consequences of Consent Denial

Where relevant, the member must be made aware of the consequences of denying consent to the provision of certain personal information.

2.1.2.5 PrP10 Collection of Personal Data by Fair and Lawful Means

This principle should be enforced during registration, at least by providing notification of collection, policy notification, and informed consent. Collection of profile data during creation of new partial identities should not involve further collection of personal information, as this would contradict the principle that personal data must be collected fair and legally. It is therefore not appropriate to collect personal data during the creation of a partial identity. For PICOS this implies that personal data that has been disclosed by a member, as part of a partial identity profile or as imported content, shall never be used in the personal profile of the member, i.e. the profile of the root identity, since this would amount to collection of personal information without the consent of the data subject and without having previously provided notice of collection. It is also important to ensure that all personal information contained in the profiles has been collected by fair and lawful means. Mixing personal

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

information with partial identity profile information may be a source of problems and obscurities with regard to the legal aspects of data collection and processing.

2.1.2.6 PrP11 Acceptable Uses

The use of personal data in order to control access to services must be in accordance with the purposes stated at the time of collection. The new access control functionality must be specified in more detail, as well as the role of the Web proxy server, in order to ensure that this principle is being enforced. Furthermore, it must be guaranteed that the integration of a sub-community into a member's profile does not contradict the stated purposes for data collection.

2.1.2.7 PrP13 Third-party Disclosure

Members must be able to express how imported content can be exported, and their view in this regard must be upheld. Tagging was used in the architecture to express a member's wishes with regard to disclosure, but in WP5 tagging is not mentioned. Ways to enforce this principle should be provided. The same policies concerning Third-Party Disclosure and data flow for personal information must be applied to sub-community profiles if the latter are associated with the corresponding member's profile.

2.1.2.8 PrP15 Access to Information

Data management functionality allowing users to access personal information should be provided.

2.1.2.9 PrP17 Correcting Information

Data management functionality allowing users to correct personal information should be provided.

2.1.2.10 PrP18 Safeguards

It is necessary to provide mechanisms to secure the registration process, so that data is not tampered or eavesdropped, the member is not impersonated by a malicious user, etc. Safeguards are included in the description of the register call flow. No mention is made in the description of the Registration component about possible safeguards to ensure secure communication and authentication during the registration process. This issue must be given special attention in the next cycle, as its impact on trust, accountability, privacy, etc, is considerable. This is a complex issue, involving several security requirements, including trust.

2.1.2.11 PrP20 Public Policies

Privacy policies must be clearly published and publicly available.

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

2.1.2.12 PrP21 Data Management

The community must allow members to set their preferences for the use of their personal data and to establish at least the basic principles for sharing content data during registration. Tagging was used in the architecture to express a member's wishes with regard to data management, but in WP5 tagging is not mentioned. Ways to enforce this principle should be provided, even with regard to partial identities. There is no description in the WP5 PDD document about how the Profile manager may enforce the Data Management principle. It seems that this functionality has been inadvertently left out due to the lack of a data management use case. The same policies concerning data management of personal information should apply to sub-community profiles if the latter are associated with the corresponding member's profile.

2.1.2.13 TrP1 Openness and Transparency

The user should be alerted when presence information is activated, suitably by the Presence manager. If the creation of a sub-community involves the use of personal information, either about the creator of the sub-community or about the members participating in the community, it is important that this fact is clearly notified to the involved parties.

2.1.2.14 TrP8 Accountability

It is important to ensure accountability during registration, which may be enforced with the help of the Registration component and event logging. The fact that part of the registration functionality is performed by the client application might have important consequences for accountability. Further details about the registration functionality must be made available in order to facilitate evaluation of how well the principle is enforced. It must be assured that the terms and conditions, the privacy policies, notification of collection of personal information, and informed consent, are provided and in the right order. The whole registration process should be logged in a secure way by the platform. Mechanisms to check the authenticity and accuracy of the user, and his or her personal information, should also be provided.

2.1.3 Analysis of the first community prototype

In this section we give a summary of the main recommendations and findings of the assurance evaluation of PICOS first prototype implementation concerning each the PICOS trust and privacy principles. We were able to establish that the final specification and implementation of the PICOS community prototype conforms in a satisfactory way to the initial trust and privacy requirements, itself a result of the close interaction between WP3 and WP6 before and during the development of the prototype.

2.1.3.1 PrP1 Notice of Collection

The community terms and conditions explain the global community policies related to data collection and data retention. They are displayed during the registration before any data is collected, and are always available for any inspection.

2.1.3.2 PrP2 Policy Notification

The community terms and conditions provide an explanation of the global community policies concerning data collection and retention. They are displayed during registration before any data is collected. A successful registration process requires the acceptance by the registering user of the PICOS privacy policies.

2.1.3.3 PrP3 Changes in Policy or Data Use

The terms and conditions cannot be changed in the first version of the platform. Hence this principle is not supported by the platform and consequently neither by the prototype.

2.1.3.4 PrP4 Timing of Notification

In the prototype, notification of purpose is given before the user enters any personal data.

2.1.3.5 PrP5 Sensitive Information

No sensitive information is collected in the first prototype.

2.1.3.6 PrP6 Informed Consent

Informed consent is guaranteed by the Terms and Conditions made available before registration.

2.1.3.7 PrP7 Change of Use Consent

The terms and conditions cannot be changed in the first prototype.

2.1.3.8 PrP8 Consequences of Consent Denial

In the first prototype, denying consent amounts to not becoming registered into the community, a consequence which should be readily understood by the user.

2.1.3.9 PrP9 Limitation of Collection

The community application restricts the collection of personal information to the minimum: a login name, a password, and a first partial identity pseudonym.

2.1.3.10 PrP10 Fair and Lawful Means

The first Picos prototype clearly enforces this principle.

2.1.3.11 PrP11 Acceptable Uses.

The prototype enforces this principle. The user has always full control from the mobile device on his/her personal data. The application allows the user to set the rules and conditions concerning how his personal data is shared and with whom.

2.1.3.12 PrP12 Data Retention.

When a user account is deleted, all corresponding personal data is also deleted.

2.1.3.13 PrP13 Third-Party Disclosure

No user data is disclosed outside the community, and within the community only with the consent of the data subject.

2.1.3.14 PrP14 Third Party Policy Requirements.

Strictly external services are not included in the first prototype.

2.1.3.15 PrP15 Access to Information

Members can access at any time their profile information by clicking the Settings icon [D6.1 D.3 and D6.1 2.2.9].

2.1.3.16 PrP16 Provision of Data

Access to a user profiles and the terms and conditions is provided immediately upon request.

2.1.3.17 PrP17 Correcting Information

The user is always able to update or to correct personal information. The data is accessible from the mobile device applications when the user logs in and can be modified any time during a session.

2.1.3.18 PrP18 Safeguards

It is necessary to provide mechanisms for securing the registration process, to prevent data from being tampered or eavesdropped, impersonation of a member by a malicious user, etc. For instance, SSL can be used for securing commutation, and CAPTCHA mechanisms for ensuring that only "humans" can register to the community. No safeguards are mentioned explicitly in the description of the registration use case. However, SSL is intended to be used here, a secure protocol in widespread use today for securing internet transactions that do not require client authentication. In PICOS, all terminals and access are controlled in the user trials, so no further client authentication was deemed necessary.

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

Access control is enforced by the use of authentication and a session token. However, how personal data is protected within the platform is not revealed, and thus the eventual presence of vulnerabilities that may be exploited by a malicious user must be further investigated during phase 2 of the Picos project.

2.1.3.19 PrP19 Data Accuracy

Appropriate mechanisms will be provided to the end users' mobile devices which will enable checking that all personal information provided by a user is entered (e.g. uniqueness of pseudonyms, login name), and which on request will be kept accurate and up-to-date.

2.1.3.20 PrP20 Public Policies

The terms and conditions contain the required summary of PICOS community policies. The client may access the terms and conditions any time during a session (available in the setting options screen).

2.1.3.21 PrP21 Data Management

The user may change his or her profile, as well as the corresponding privacy rules using the policy manager. Moreover, data is never disclosed against the wishes of the user.

2.1.3.22 PrP22 End-to-End Privacy

This principle is not particularly supported by the community application. End-to-end privacy is aimed to be reached on a global level, considering all involved artefacts.

2.1.3.23 PrP23 Authentication

The first prototype supports only one form of authentication, namely username/password.

2.1.3.24 PrP24 Multiple Persona

The partial identity manager of the community application allows one to create and manage multiple independent identities (partial identities). The principle is enforced throughout in the prototype. Users always interact through one active partial identity.

2.1.3.25 TrP1 Openness and Transparency

The CA enforces this principle in a satisfactory way. The user is always in control of his/her own personal data, policies are easily accessible, and the treatment of personal data is easy to understand.

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

2.1.3.26 TrP2 Trust Between Communities

Sub-communities have a reputation attribute. External communities, however, are not part of the first prototype.

2.1.3.27 TrP3 Provenance

Provenance is enforced in the prototype with the help of password based authentication mechanism.

2.1.3.28 TrP4 External Services

The first prototype does not provide links to real external services.

2.1.3.29 TrP5 Audit

Auditing in Picos is based on logging, which is performed by the PICOS platform.

2.1.3.30 TrP6 Objective and Subjective Trust

Objective trust is based on rating of content and contributions uploaded into community or sub-community repositories. Rating is supported by the CA. The prototype allows also the assessment the reputation of an individual member before establishing communication.

Subjective trust in PICOS communities is specifically supported by the private room and private sub-community concept. Only invited members may access a private sub-community, implying that content keeps its private character and is uploaded to the public community only by request of the content owner. Regarding chat rooms, only members invited to participate in the chat may take part in it. Chats can be used to foster subjective trust between community members. Finally, asynchronous messages, which are handled privately via user inboxes, also contribute to trust within the community.

2.1.3.31 TrP7 Consensus

Since in PICOS communities only provided content is directly rated, not users, there is no consensus functionality at the level of the end user’s device.

2.1.3.32 TrP8 Member Accountability

Users cannot interact in the community without a valid login. The event logging performed by the platform, as well as the access control mechanism, enables a step-by-step control of any user action. The event-logging platform component is intended to follow a search event model that allows fast access to the required information.

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

2.1.4 Recommendations based on the assurance evaluation

From our experience in the assurance evaluation of D4.1, D5.1 and D6.1, we would like to make the following suggestions/recommendations for the second cycle:

- A detailed description is given of an updated set of specific requirements, both functional and security requirements, taking into consideration what was learned in the first cycle.
- A new specification is made of the uses cases and reflecting the external behaviour of the final system, intended both for defining the architecture of the system and validating all technical results of the second cycle; it is desirable that the system design should include an architecture-free description of this revised set of use cases with the purpose of establishing the main functional features of the system, rather than to validate the components; these use cases should thereafter guide the development of both the platform and the prototypes, thus staving off for the need for community prototype developers to make major decisions about its functionality.
- A clear link is made and documented between the architecture and the platform prototype, particularly the components and their functionality.
- A clear alignment is produced between the specifications of the WP4 architecture, the WP5 platform, and the WP6 prototypes; it should for instance be possible to link elements of the architecture, e.g. features, components, or other functionality, to the requirements that justify their inclusion in the architecture.
- In order to complete the evaluation of the WP5 platform, the functionality and internal interfaces of the platform components, functions and services should be provided and documented, not only their signature or external interfaces.

3 Evaluation of the Platform Design & Architecture (WP4)

3.1 Summary presentation of the Platform Design & Architecture

The first version of the PICOS Architecture (D4.1) was derived from the needs of the reference community, namely the Anglers, but more specifically the needs on a generic mobile community. Requirements were gathered, and from these a set of PICOS Principles and PICOS Features were prepared. The Principles provided the high-level design goals that the architecture would follow. The twenty-three Principles covered:

- Law
- Trust
- Privacy
- Control
- Identity
- Other

Fifteen PICOS Features were considered, covering the needs of privacy, trust and identity management, and other functions that a community – and specifically a mobile community – would require. Each feature was categorised as:

- PICOS Enhancing
- PICOS Distinguishing

the objective, being to show how the PICOS community has been differentiated from existing general purpose 'social networking' communities.

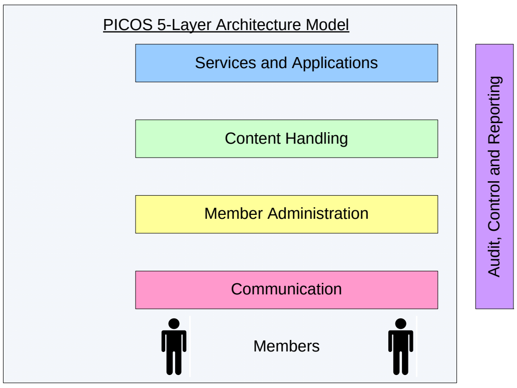
An additional category called PICOS Research was used to highlight features that at the time of the design were not fully understood and which require further research.

The design process also defined a trust model that established fundamental understandings that were essential in making key design choices.

Use cases, fifteen in total, and an angling scenario helped to validate the design. The use cases reveal some of the key operating modes of the PICOS community; they include: Registration, Revocation, Reputation, External services, Content sharing, Presence, Offline working, Real-time communication and Audit.

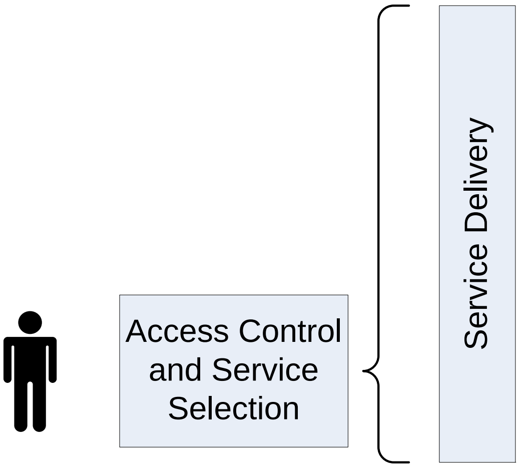
Several topologies were considered before settling on the standard client-server arrangement, which in fact was the most appropriate fit for the angling community that had to be represented in the first prototype.

The architecture is built on a set of components. The components perform a range of functions that support the privacy, trust and identity management objectives of PICOS. The components extend to over 50, but can usefully be grouped into 5 categories, represented by the PICOS five-layer model:


PICOS 5-Layer Architecture Model
Services and Applications
Content Handling
Member Administration
Communication
Members
Audit, Control and Reporting

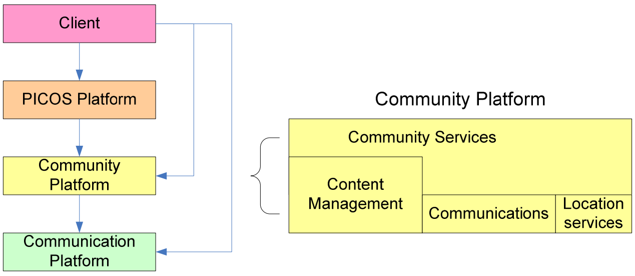
The PICOS architecture is complex and dependent on a large number of inter-related components. The use cases provide a useful entry point to the understanding of the design.

At its highest level the architecture consists of components that (1) support access to the community and (2) deliver a range of services. The architecture is essentially services-based:



To assist implementers, the Architecture provides example and discusses aspects of implementation. Although D4.1 was not primarily concerned with implementation, two interpretations emerged that provided a useful insight into how PICOS might be built.

For the first prototype, client-server was the chosen topology because it is a good fit for the target angling community, but more specifically met the immediate needs of a mobile community. The preferred way to visualise this arrangement was to consider a platform-centric implementation, such as that shown below:



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

As mentioned previously, the Architecture highlights several features and components that warranted further research. Research was necessary because some features that appeared in components were either not well understood, or had the potential to make a significant contribution to PICOS if developed beyond their current implementation.

Eight components required additional research: Accountability, Data Minimisation, Linkability, Partial Identity Management, Policy Management, Privacy Advisor, Reputation Management and Trust Negotiation.

Furthermore, new challenges anticipated beyond the needs of the first prototype arose, including: stronger trust models, independent identity endorsement, independent law enforcement, transfer of sensitive 'privacy preserving' functionality to the client, and privacy from community operator.

3.2 Legal Evaluation

3.2.1 Methodology used

The legal evaluation of the First Platform Design and Architecture specification, and more specifically of PICOS Deliverable D4.1 "Platform Architecture and Design V1" is based on the European legal framework on data protection. In the field of European Union law, the Charter of Fundamental Rights of the European Union (hereinafter EU Charter)[4] provides for the respect for private and family life (Art.7) and the protection of personal data (Art.8), while the Data Protection Directive (1995/46/EC)[5] has been adopted to guarantee efficient data protection. The principles included in this Directive have been transposed as a set of requirements in Chapter 6 "Legal Requirements" of PICOS Deliverable D2.4 "Requirements", a summary of which can be found in its Appendix B (Summary of Legal Requirements). Furthermore, the general overview of the legal and regulatory framework (PICOS Deliverable D2.3 Contextual Framework, Ch.4) has been used as a source of this evaluation.

The main goal of this evaluation is to ensure compliance of the defined architecture with the European data protection legislation and the relevant applicable principles. It has been noted (Ch. 6, D4.1) that PICOS opted to follow the "privacy by design model" thereby ensuring continuous cooperation of the technical partners with the legal team and taking into account privacy principles at the earliest stage of the creation of the architecture. This "privacy by design model" ensures privacy as a central design feature, and not merely a last-minute attempt at ensuring the compliance of the system with the relevant legislation. This evaluation will assess the adequacy of the proposed policies, and ensure compliance with the defined legal requirements (Ch.6, D2.4) and principles of Appendix B (D2.4). The defined architecture principles (Ch.7, D4.1), along with the initially proposed PICOS features (Ch. 8, D4.1) will be critically assessed vis-à-vis the aforementioned legal framework, as presented and analysed.

[4] Charter of Fundamental Rights of the European Union, O.J. 2000, C 364/1 (18.12.2000).

[5] Directive 2002/58/EC (ePrivacy Directive) and Directive 2006/24/EC (Data Retention Directive) are not directly applicable to PICOS as they only apply to "publicly available electronic communications services offered via a public electronic communications network", which is not the case for the PICOS platform nor for the PICOS application prototype.

3.2.2 Evaluation of the requirements and functionalities of the Platform design and architecture

3.2.2.1 Compliance with data protection principles

A general overview of the legal and regulatory framework on privacy and data protection has been provided for in PICOS Deliverable D2.3 Contextual Framework, Ch. 4. The legal principles on privacy and data protection contained in the aforementioned framework were translated into requirements in Chapter 6 “Legal Requirements” of PICOS Deliverable D2.4 “Requirements”. This section will evaluate the aforementioned principles and address the extent to which these principles have been implemented in the Design and Architecture document, PICOS Deliverable D4.1. So all the references to chapters and section refer to Deliverable D4.1

a. Principle of fair and lawful processing.

According to Article 6(a) of the Data Protection Directive, the first principles relates to the requirement of fair and lawful processing. In determining whether any processing of personal data is ‘fair’, particular regard must be paid to the method by which data were obtained. In PICOS, this principle is reflected in PP2, regarding Data Ownership, in which members explicitly grant “the right to store and process their data according to the Member’s stated privacy and data handling preferences”.

b. Principle of obtaining data only for specified and legitimate purposes.

Data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes (Article 6(b) of the Data Protection Directive). This principle thus has two components: (1) the data controller must specifically inform the data subject of the purposes for which data has been collected; and (2) once data has been properly collected, it must not be used for further purposes incompatible with the original purposes. Article 7 Data Protection Directive sets out the criteria for making data processing legitimate, one of which is the unambiguous consent of the data subject.

The PICOS Design and Architecture platform specification adheres to this principle with its inclusion of the “PP3: Use of personal information” of the PICOS principles in which the members state the conditions that dictate how their personal information can be used by other Members and these conditions are then enforced by the Architecture. Furthermore, a *Consent Management* component allows members to grant consent for their personal information to be used in the way members wish. It therefore enforces user-defined policies with respect to the sharing of members' profile information (and other member data) with other members and with external services. It indicates whether the member gave consent for this data to be shared with others and, if so, what terms and conditions apply, also allowing member to modify or withdraw their consent, if they desire.

c. Principle of data minimisation

Article 6(c) of the Data Protection Directive requires a data controller to hold only personal data that is “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”. It is therefore a legal obligation for the data controllers to store only a bare minimum of data for the purpose of running PICOS (data minimisation principle). Moreover, the

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

design and technical devices of the data processing systems must be oriented towards collecting, processing and using either no personal data or as little as possible ('data avoidance')[6].

Pursuant to section 7.1.8, PICOS adheres to this principle with PP8, where it is stated that the PICOS Architecture must support the concept of data minimisation, by only collecting data absolutely necessary for the provision of the service.

The PICOS Architecture also supports the use of pseudonyms, as per PP11, where members who wish to interact with other members and services, can still do so whilst still being able to restrict how much identifying information is shared.

d. Principle that personal data shall be accurate and, where necessary, up-to-date

According to Article 6(d) of the Data Protection Directive, and as further elaborated in PICOS D2.3 section 6.2.1, this principle creates an obligation for the data controllers to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, are either erased or rectified. In practice, a data subject is likely to complain of a breach of this principle in cases where there has been some detriment to the individual as the result of the information being incorrect. It is therefore advised that the data controllers set up a mechanism whereby the data subjects are able to update their personal data or notify the data controller about the inaccuracies of the present information.

The PICOS Design and Architecture ensures compliance with this principle via "PP15: Data controllers", whereby the data controller (the entity that determines the means and purpose of the data processing) is identified and can be contacted in circumstances regarding the accuracy of his personal data. In addition, via PP2, "Data ownership", the PICOS architecture recognises that personal information belongs to the member, and therefore the members are able to update their personal data directly.

e. Principle that personal data shall not be kept for longer that is necessary for the purposes

This principle, outlined in Article 6(e) of the Data Protection Directive, states that data should be destroyed or rendered anonymous when the specified purpose for which they were collected has been achieved. This principle is translated into a specific feature in the PICOS Design and Architecture specification with the "Revocation" component which is called whenever a member wishes to leave the community (or is asked to leave the community), or when a member wants to terminate a partial identity.

As described in section 9.7.11 of D4.1 "PICOS Design and Architecture", Revocation "requests the Anonymisation component to pseudonymise (in a reversible way, such as encryption) all references in all databases to the identity of this individual, and then after a second period of time, all these reversible pseudonyms are converted to irreversible pseudonyms (for example a hash of the previous pseudonym). Additionally, after a period of time, all sensitive data belonging to this individual must be erased".

It has been stated in this section that "it is unlikely that this information can simply be deleted from the community (or even removed) since it may be shared or required for legal purposes." It is recommended that when personal information can not be deleted it should be made anonymous.

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

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

f. The principle of data security

Article 17 of the Data Protection Directive outlines the principle regarding the issue of data security: it requires data controllers to take 'appropriate technical and organizational measures'. This principle has been transposed into PICOS policies with the existence of the *Network Security* component (as per 9.4.4 of PICOS Deliverable D4.1) which is responsible for creating a secure channel between communication entities. An *Intrusion Detection* component (section 9.6.7) is responsible for detecting attacks on the PICOS community. It is stated that this component should work alongside various other security safeguards such as network firewalls. A *Secure Repository* component (section 9.8.7) provides a safe location to store personal sensitive information.

3.2.2.2 Pseudonymous data in the architecture

As detailed in PICOS Deliverable D2.3 on Contextual Framework which analyses the regulatory framework on privacy and IdM, and the proposed list of requirements in PICOS Deliverable D2.4, there is a need to assess the applicability of the data protection legislation to pseudonymous data. According to the Data Protection Directive in Article 2(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'). It is arguable whether pseudonymous data is personal data for the purposes of the data protection legislation, and this depends to some extent on the method used for achieving pseudonymity. Furthermore, Recital 26 of the Directive states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person".

The Article 29 Working Party in its opinion 4/2007 on the concept of personal data,[7] expressed the opinion that "retraceably pseudonymised data may be considered as information on individuals which are indirectly identifiable", as "using a pseudonym means that it is possible to backtrack to the individual". As such, the conditions of Article 2(a) of the Directive are met.

Whilst few details of a technical nature exist at the Design and Architecture phase as to how the pseudonyms will be generated and managed, we reach the conclusion that for the purposes of PICOS, pseudonyms can be linked to the user and therefore qualify as personal data.

3.2.3 Summary of findings and recommendations

The PICOS Design and Architecture v1 (WP4) is meant to create technical architecture and design for the PICOS identity management platform. The legal evaluation covers the basic data protection issues that relate to the use of personal data. It critically assesses the privacy principles defined and which shall be respected and applied both during the design phase of the platform and also in future implementations of the platform architecture.

Many of the Architecture Principles listed in Ch. 7 (D4.1) have as their root the data protection principles appropriately considered in the aforementioned documentation and legal framework. However it is impossible at the design and architecture phase to effectively evaluate all the Architecture Principles and assess their compliance with the data protection principles and legislation, since they are still in a very abstract form of implementation with little detail as to how these principles will in practice be implemented.

[7] Article 29 Working Party, opinion 4/2007 on the concept of personal data, WP 136 (adopted on 20th June)

Features evident in PICOS such as the *Privacy Advisor*, which informs members if the action they are about to perform will place their privacy at risk, and the ability of members to have *multiple personas* (as per PP18) safeguard the members' privacy over-and-above the minimum requirements of data protection legislation.

It is evident that the pertinent privacy issues and in particular the issues relating to the processing of personal data have been taken into account at the earliest stage of the creation of the architecture, with the resulting defined architecture fulfilling, or at least addressing, many of the legal requirements as set out in the European legal framework on data protection. Although it is evident from the analysis conducted above that the setting out of the legal requirements and their translation into clear principles for the developers at a very early stage of the PICOS project, as well as the continuous cooperation with the legal team during the designing phase of the architecture, following the "privacy by design model" has resulted in an architecture complying in theory with the relevant legal framework, it is difficult to certify true legal compliance until a more detailed prototype is created. It is however safe to conclude that all the data protection principles have been adequately addressed for the purposes of the Design and Architecture specification, and translated into specific features. A more concrete evaluation will be conducted in the frame of the evaluation of the PICOS Platform Prototype v1 (WP5) and the PICOS Angling Community Prototype (WP6).

3.3 Technical evaluation

3.3.1 Trust, Privacy & other technical elements

3.3.1.1 Methodology used

In this part of (technical) evaluation we will focus mainly on the issues relevant to trust and privacy principles. Trust and privacy are critical objectives in the PICOS Architecture. The evaluation of the PICOS Architecture will be done in a way we will discuss scenarios, features and components relevant to trust and privacy their relevancy and technical aspects. The main source of documentation for this part of evaluation was D4.1.

3.3.1.2 Evaluation of the requirements and functionalities of the Platform design and architecture

Community topologies and community trust models

Proposed community topologies and respective trust models play the key role in the trust building process within the community with respect to the service providers. The PICOS architecture is going primarily towards client-server implementation (D4.1, section 4) topology. In this topology there is one central server (in case of multiple communities, we can have multiple central servers) which must be trusted by all community members. Client-server topology does not explicitly require trust between individual members of the community (on the service-provider level). If members within a community trust the central server then this trust turns as a building block used for building trust between other members of the same community and trust to the community as a whole. This level of trust plays the key role in content sharing, communication with other members of the community and privacy protection.

Section 5 in D4.1 discusses different community trust models and user attitudes towards trust and risk – Every community, and every community member, has a different attitude to risk. Some are risk accepting, while others are risk averse. The list of different perspectives from both members' and community operators' side are discussed; but what is not discussed clearly is the PICOS proposal for the process of building such trust. How does PICOS attract members who enter the community with "complete distrust" in order to convince them that they can trust the system.

PICOS principles

PICOS principles are used for architecture design. These principles are based on requirements gathered from real-world potential online community members. There are seven basic PICOS principle categories – one of these categories addresses directly trust (PICOS principles: PP5, PP6, PP12, PP13, PP14, PP16, PP21, and PP23) and another one addresses directly privacy (PICOS principles: PP8, PP9, PP17, PP18, and PP19). It can be seen that the majority of PICOS principles fall into either trust or privacy category. This is an indication that these two aspects are of great importance for the PICOS architecture. In the following text we will discuss these trust and privacy related PICOS principles in more detail.

PP5 – Openness and transparency (PP_trust)

The PICOS Architecture must offer services to Members in an open and transparent way.

This PICOS principle aims to increase Members' trust in the Architecture by providing them with information how their private data will be processed, stored and used. This information should be formulated in well-understandable fashion (instead of huge technical documentation) so that Members will be motivated to read such text and understand it.

PP6 – Trust between Communities (PP_trust)

The PICOS Architecture must recognize trust as a common currency when exchanged between PICOS Communities.

The goal of "trust between Communities" is to allow Members from different Communities to "transfer" trust (or reputation) from one Community to another. The goal of this feature is therefore to build trust between Members from different Communities. This feature does not directly help to build trust in the Architecture.

PP8 – Data minimization (PP_privacy)

The PICOS Architecture must support the concept of data minimization. Only data absolutely necessary for the provision of the Service should be collected.

Data minimization is a principle that Members are required to provide only the necessary information for getting access to the Service. This is a natural privacy-related principle and can also help to build Members' trust in such systems. As Members' trust in the system grows, they may become willing to provide further personal information that is shared within their Community.

PP9 – End-to-end privacy

The PICOS Architecture must support end-to-end privacy.

End-to-end privacy (as defined in the PICOS Architecture) is a way for protecting private information in the PICOS Architecture. It's accomplished by legal obligations placed on the

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

Community operators, who may have access to private information. End-to-end privacy can help to increase trust in the Architecture.

PP12 – Provenance

The PICOS Architecture must ensure that Members can rely on the provenance of information that they receive from other Members/PICOS Communities, subject to the Member choosing to state the provenance and there being no conflict or risk of undermining other privacy principles.

The goal of this property is to increase Members' trust in information received from other Members or PICOS Communities. Because it may be difficult to guarantee the accuracy of information, this property may provide information about the level of trust (based on reliability of the source, or reputation score).

PP13 – External services

The PICOS Architecture must ensure that externally hosted services are delivered in as trustworthy a way as an internally hosted Service, or that Members are aware when an external service is (potentially) less trustworthy than an internal service.

Trustworthiness of externally provided services is a problematic issue if Members must have trust to the whole. PICOS will solve this issue by an explicit indicator to the Members that a service is provided externally.

PP14 – Audit

The PICOS Architecture must allow all services to be fully auditable by an entity trusted by all Members.

Sufficient auditing of services (by an entity trusted by all Members) must be applied and enforced in order to support Members' trust in the system and for being able to prevent and recover from privacy intrusive events.

PP16 – Objective and subjective trust

The PICOS Architecture should support both objective and subjective methods for assessing trust.

Subjective trust is assessed by Members based on their experience and, e.g., reputation management services. Objective trust, on the other hand, is presented as being based on objective methods including trusted computing base and reputation management system or hard facts. This description is not very specific and, especially in case of the objective trust, should be clarified in a more precise fashion.

PP17 – Authentication

The PICOS Architecture should support multiple forms of Member authentication, while continuing to respect privacy.

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

The PICOS Architecture specifies three possible methods for authentication (know/possess/are). It is not clear which one will be implemented as mandatory and which of them will be implemented as optional (if any). Health-related information must be adequately protected if such authentication method is available.

PP18 – Multiple persona

The PICOS Architecture should allow Members to have multiple persona.

This property allows Members to define and use different identities. This is a privacy-enhancing issue which helps to protect Members' real identity and limit linkability between user identifiers and performed actions.

PP19 – Sub-groups

The PICOS Architecture must support the creation of sub-groups within the Community.

Support of multiple sub-groups within one Community is natural and may help to protect private information that is share only within such sub-group(s).

PP21 – Diversity

The PICOS Architecture should be designed in such a way that no single entity can act in a way that might compromise the trust and privacy of the community.

Privacy and trust related principle that ensures that single entity cannot harm privacy and trust of the Community. Communities rely on community operators that must be trusted (see PP9 and PP14).

PP23 – Trust

The PICOS Architecture should ensure that Members are accountable for their actions while a member of the Community.

This property should work together with audit (see PP14) in order to acquire information about all activity within the system, communities and sub-communities. It should be clearly stated how the gathered information will be protected and who has access to it.

PICOS features

PICOS features consist of a list of features that will create the main benefit for community members. PICOS features are categorized in three levels – PICOS distinguishing (introduces new community feature); PICOS enhancing (enhances this traditional community feature); PICOS mobility (enables mobility through this feature).

The list of PICOS features is the following:

1. Reputation – PICOS enhancing
2. Content sharing – PICOS mobility, PICOS enhancing

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

3. Registration – PICOS enhancing
4. Personalization – PICOS enhancing
5. Messaging – PICOS enhancing
6. Searching – PICOS enhancing
7. Sub-communities – PICOS enhancing
8. Presence – PICOS mobility, PICOS enhancing
9. External services – PICOS mobility, PICOS enhancing
10. Content tagging – PICOS distinguishing
11. Communication services – PICOS mobility, PICOS enhancing
12. Notification – PICOS mobility, PICOS enhancing
13. Inter-community interaction – PICOS enhancing
14. Mobility – PICOS mobility, PICOS distinguishing
15. Non-repudiation – PICOS distinguishing

Trust, privacy and identity management related issues are discussed individually for each PICOS feature – called "How PICOS will address the privacy/trust/IdM concerns". These descriptions are very detailed for each PICOS Feature and can be found in document D4.1, section 8 – PICOS Features. Roughly counted, there are around 60 privacy, trust and identity management concerns for building trust and privacy protection. This number greatly supports the primary objectives of the PICOS Architecture – trust and privacy in online/mobile communities.

3.3.1.3 Summary of findings and recommendations

How does PICOS attract community members so that their trust in the system increases? Such description or its relevant parts are discussed in different sections of the document, but for better understanding, it would be advisable to put all these descriptions together.

It should be clearly stated (where relevant) that PICOS supports the data minimization principle. Members have explicitly be informed they do not need to provide more private information than requested.

PP16 – Clearer clarification of methods for building objective trust.

PP17 – Clearer clarification of methods of authentication that will be mandatory and those that will be optional.

PP14 and PP23 – Clearer clarification of how the acquired information will be protected and who will have access to it.

Trust, privacy and identity management concerns discussed in section 8 – PICOS Features, provide a detailed specification how the PICOS Architecture will address these principles. These descriptions are crucial in order to build a trustworthy system that also allows members to build trust and maintain privacy regarding other members or regarding (sub-) communities. Therefore a special care must be taken during the implementation phase in order to have all these principles properly implemented and documented.

3.3.2 Community focus

The focus of this part of the technical evaluation is on the PICOS requirements, principles and components of its architecture, which have a community focus. Because PICOS wants to research, develop, build, trial and evaluate a platform that supports the provision of community services, principally every requirement, principle and component of the architecture has a “community-focus”. As in chapter 2.3.1 trust, privacy and other technical elements are evaluated and in chapter 2.3.3 location information and location based services, this chapter 3.3.2 will get down to one of the key concepts of the PICOS platform. Obviously the discussion of identity management components and of the sub-community component cannot be strictly separated from trust and privacy aspects.

3.3.2.1 Methodology used

Components of a software architecture have to be evaluated at least regarding three questions:

(1) Are the components suitable to fulfil the requirements?

(2) Are the components appropriately cut to size?

(3) Are the relationships/interactions between the components appropriately constructed?

For answering question (1) the platform design and architecture (as described in the deliverable D4.1) has to be evaluated in the light of the gathered requirements (described in the deliverable D2.4). D4.1 “Platform Architecture and Design” follows a user-centric and scenario-based proceeding for eliciting the requirements from D2.4 “Requirements”: A heavyset user story describes features of the Angler Community which has been selected for the first prototype; then PICOS Principles, PICOS Features and finally the PICOS Components are specified.

The innovative concepts of the PICOS Platform, especially in form of the Sub-Community Concept (and additionally the Private Room Concept) cannot be derived directly from the requirements gathered in D2.4. In fact they are aiming at providing useable, user-friendly and convenient concepts which meet the requirements best.

Therefore the correlation between the gathered needs and requirements for the community focus on one side and the platform design and architecture on the other hand will be evaluated "forward" (from the requirements to the user story, to the principles, to the features, to the components) as well "backwards" (from the user story, to the principles, to the features, to the components to the corresponding requirements).

For answering question (2) the specification of the components is relevant, too.

For answering question (3) the description of the interactions between the components, the picture of the overall PICOS Architecture and the discussion of the use cases are relevant.

3.3.2.2 Documentation used

As mentioned above, the documentation used for this evaluation are Deliverable 2.4 “Requirements” and Deliverable 4.1 “Platform Architecture and Design”. D2.4 addresses the requirements and needs for the PICOS platform, D4.1 the current state of the platform design and architecture.

3.3.2.3 Evaluation of the requirements and functionalities of the Platform design and architecture

The identity management requirements are discussed in chapter 3.3.1 of D2.4. In that chapter nineteen requirements were identified: (R3.1) Accountability, (R3.2) Reliability, (R3.3) Context Information, (R3.4) Partial Identities, (R3.5) Subsequent Release of Identity Attributes, (R3.6) Lifecycle Management of Identities, (R3.7) Inactive Accounts and Their Deletion, (R3.8) Measuring of Linkability, (R3.9) Intended Linkability, (R3.10) Openness of Identity Attributes, (R3.11) Protection of Personal Data, (R3.12) Interoperability of Identity Management Systems, (R3.13) Cross-community Identity Management System, (R3.14) Unique Identifiers, (R3.15) Identification of Communication Partners , (R3.16) Authorisation and Delegation, (R3.17) Authentication and Access Control, (R3.18) Import and Export of Credentials, (R3.19) Different Identity Management Providers.

A mapping of the functionality being described in the user story (D4.1) to the requirements is not explicitly specified. A corresponding evaluation determined that the story directly factors in all relevant requirements (which are listed in D2.4) beside the requirements R3.1, R3.2, R3.3, R3.5, R3.6, R3.7, R3.8, R3.9, R3.10, R3.12, R3.13, R3.14, R3.17, R3.18, and R3.19. Additionally the story addresses the requirements R1.1, R1.11, R4.5, R4.8, R5.4, R5.7 and R5.10 (which also are listed in D2.4).

The story itself is plausible and comprehensible, and is without doubt based on profound knowledge and experiences about the Angler Community.

A mapping of the PICOS Principles (D4.1) to the requirements (which are listed in D2.4) is not explicitly specified. The principles PP2: Data Ownership and PP11: Use of Pseudonyms are related to identity management.

A mapping of the requirements (which are listed in D2.4) to the PICOS Features (D4.1) - which only are the key features - is not explicitly specified. A corresponding evaluation identified the following features that are directly related to the community focus:

1. (PF1) Reputation
2. (PF2) Content sharing
3. (PF3) Registration
4. (PF7) Sub-Communities
5. (PF9) External services
6. (PF13) Intra-community interaction (comment: this feature is called *intra*-community interaction, but discusses *inter*-community interactions)

A corresponding evaluation identified the following requirements (from D2.4) that are related to these PICOS Features:

1. (R1.11) Reputation Management
2. (R5.4) Ad hoc P2P Communication, (R5.10) Integration of Communication, Cooperation and Content Sharing Services
3. (R4.5) Authorisation and Authentication Infrastructure, (R3.1) Accountability, (R3.15) Identification of Communication Partner - lead to a registered Member
4. (R1.1) Personal Trust, (R1.3) Trustworthy Content, (R2.3) Confidentiality, (R2.6) Classification of Sensitive Data, (R2.10) Unlinkability, (R3.4) Partial Identities, (R4.3) Management of Community Data - the sub-community makes use of

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

5. (R5.7) External Information Services, (R5.8) External Transaction Services, (R4.8) Integration of External Interfaces
6. (R1.2) Inter-Community Trust, (R3.13) Cross-community Identity Management System

As a result it has to be determined, that the PICOS Features factor in all relevant requirements (which are listed in D2.4) beside the requirements R3.2, R3.3, R3.5, R3.6, R3.7, R3.8, R3.9, R3.10, R3.11, R3.12, R3.14, R3.16, R3.17, R3.18, and R3.19. Additionally the features address the requirements R1.1, R1.2, R1.3, R1.11, R2.3, R2.6, R2.10, R4.3, R4.5, R4.8, R5.4, R5.7, R5.8, and R5.10 (which also are listed in D2.4).

A mapping of the PICOS Components to the requirements (which are listed in D2.4) is not explicitly specified. A corresponding evaluation identified the following components (from D4.1) that are directly related to the community focus:

1. (9.5.3) Access Control
2. (9.5.6) Authentication
3. (9.5.7) Authorisation
4. (9.5.16) Partial Identity Management
5. (9.5.18) Preparation Area
6. (9.5.21) Reputation Management
7. (9.6.3) Accountability
8. (9.7.10) Registration
9. (9.7.11) Revocation
10. (9.7.12) Sub-Community Management
11. (9.8.2) Content Sharing

The following requirements (which are listed in D2.4) were identified as being related to these PICOS Components:

1. (R3.15) Identification of Communication Partner, (R3.17) Authentication and Access Control
2. (R3.17) Authentication and Access Control
3. (R3.16) Authorisation and Delegation
4. (R3.4) Partial Identities
5. implied by: (R2.5) Privacy in Processes and Transactions, (R2.3) Confidentiality, (R3.11) Protection of personal Data
6. (R1.11) Reputation Management
7. (R3.1) Accountability
8. implied by: (R3.15), (R3.16) and (R3.17)
9. -
10. implied by: (R1.1) Personal Trust, (R1.3) Trustworthy Content, (R2.3) Confidentiality, (R2.6) Classification of Sensitive Data, (R2.10) Unlinkability, (R3.4) Partial Identities, (R4.3)
11. (R5.4) Ad hoc P2P Communication, (R5.10) Integration of Communication, Cooperation and Content Sharing Services

As a result it has to be determined, that the PICOS Components factor in all relevant requirements (which are listed in D2.4) beside the requirements 3.2, 3.3, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.12, 3.13,

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

3.14, 3.18, and 3.19. Additionally the features address the requirements 1.1, 1.3, 1.11, 2.3, 2.5, 2.6, 2.10, 4.3, 5.4, and 5.10 (which are also listed in D2.4).

Regarding the second question that has to be answered a corresponding evaluation identified no component that is not appropriately cut to size. That is, the individual components each have an adequate independence and thus possess an adequate delineation of the other components of the architecture.

Regarding the third question that has to be answered a corresponding evaluation concluded that the discussion of the relationships/interactions between the components in chapter 9 of D4.1 shows some feasible relationships, but surely is not complete. The same is true for the picture of the overall architecture.

A corresponding evaluation has determined, that use cases (PUC 1) Registration, (PUC 2) Accessing the Community, (PUC 3) Revocation, (PUC 4) Multiple Partial Identities, (PUC 5) Reputation, (PUC 7) Content Sharing, and (PUC 9) Sub-community are of relevance for the community focus. The description of each of these use cases includes more details regarding the interaction between the components; the relationships are plausible, but not quite complete.

3.3.2.4 Summary of findings and recommendations

D4.1 has used state-of-the art artefacts to design an architecture: a user story, design principles, features, a component model and use cases. The interactions between the components are described in the component model and – with more details – in the use cases.

The artefacts are plausible and comprehensible; this is especially true for the components of the component model and the use cases with community focus. The interactions between the components are not completely discussed; this has to be done during the next steps of the development process.

PICOS is not a commercial software development project, but a research project. For this reason and because “only” prototypes have to be developed, design patterns were not used to design the architecture. Furthermore it was not possible to directly derive the architecture principles and features and especially the components from the requirements. Rather the knowledge and the experiences of the experts of the PICOS team had to be used to overcome the gap between the identified user needs and innovative concepts of the PICOS platform especially aiming at providing useable, user-friendly and convenient concepts. Therefore an evaluation of the concepts by the users during the trials is of particular importance.

Based on the results of the trials regarding the first cycle it should be possible to reveal a more comprehensible connection between requirements on one side and components of the architecture on the other hand during the second cycle.

3.3.3 Location based services and communication features

3.3.3.1 Methodology used

The design and architecture of a platform supporting communities are mostly complex and involve many challenges and tradeoffs. Different methods exist for the evaluation of such platforms. The method followed here targets the technical evaluation of WP4 (Platform Architecture and Design), is twofold and consists of:

1. comparing the **as-is state** of the platform design and architecture (described in the deliverable D4.1) with respect to fulfilment or at least consideration of the gathered needs and requirements (addressed in deliverable D2.4) *and*
2. a review of the proceeding followed in WP4 for fulfilling the gathered needs and requirements in terms of design and architecture derivation e.g. components, their interaction, and how they are aligned in a given architecture either primarily with respect to LBS and communication functionalities in PICOS as well as some aims[8] **implicating/needing potential extensions** (also mentioned in D4.1).

3.3.3.2 Documentation used

For the design and architectural analysis related to the consideration of LBS and communication functionalities we used mainly the deliverable D4.1 “Architecture v1” which is the first outcome produced by WP4 since WP4 was responsible for defining the PICOS platform design and architecture. Latter were implemented in successive work packages, principally WP5 and WP6. We compared the deliverable D4.1 with the deliverable D2.4 “Requirements” (gathered needs and requirements), because the role of D4.1 was to consider D2.4 and to derive a technical description of the components that address the needs and requirements of the PICOS community.

3.3.3.3 Evaluation of the requirements and functionalities of the Platform architecture and design

3.3.3.3.1Fulfilment and consideration of the gathered needs and requirements

For the technical evaluation, aspects such as which components are foreseen and which interaction take place among them as well as how such components are aligned in a given architecture are essential. Thereby, the main focus of the evaluation is set on how technical aspects fulfill the requirements.

When considering PICOS Requirements, twelve main requirements were identified in D2.4, which are related to and explicitly involving the location and presence contextual information as well as messaging/communication, and notification functionalities:

1. R2.7 (Definition of Privacy Settings - p.58)
2. R2.8 (Visibility and Reachability of Users - p.58)
3. R2.11 (Fine-grained Disclosure and Sharing of Data and Information - p.59)
4. R.2.12 (Control over Data and Information Flows - p.59)
5. R3.15 (Identification of Communication Partners - p.65-66)
6. R3.16 (Authorisation and Delegation - p.66)
7. R5.4 (Ad hoc P2P Communication – p.73)
8. R5.6 (Context-dependent Service Provisioning – p.73)
9. R5.7 (External Information Services – p.74)
10. R5.10 (Integration of Communication, Cooperation and Content Sharing Services – p.75)
11. R5.11 (Integration of Information and Recommendation Services – p.75)
12. R5.12 (Integration of (Geo)location Services – p.76)

[8] One of the aims mentioned in D4.1 was to be as topology agnostic as it is practicable. Because every community will have a different trust model, D4.1 mentions that PICOS plans to ideally support multiple trust models, and also mentions that is important to align the architecture with a trust model.

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

All needs and requirements identified in D2.4 were categorized in form of a key features list in D4.1. This list includes 15 PICOS (main system) Features (PFs)[9]. From these PFs, seven PFs explicitly involve the location and presence contextual information as well as messaging/communication, and notification functionalities:

7. PF2 (Content sharing – p.58)
8. PF8 (Presence – p. 68)
9. PF10 (Content tagging – p.71)
10. PF11 (Communication services – p.72-73)
11. PF12 (Notification – p.74)
12. PF13 (Intra-community interaction – p.75)
13. PF14 (Mobility – p.76)

Based on the 15 PICOS Features 49 components were defined. These components were categorised according one of five “components groupings” (Services and Applications, Content Handling, Member Administration, Communication, and Audit, Control and Reporting) and assigned to “tiers”. According to our review of the component functionality descriptions we assess that these descriptions consider the twelve requirements cited above needed for LBS and communication functionalities.[10] Especially when we review the PICOS Use Cases (PUCs 2, 5, 7, and 8) and evaluate how each component is involved or interacts with other components to satisfy the “user requirements”, we can assess that at least for those PUCs, the LBS and communication means requirements and needs can be fulfilled with the help of the current Platform design and architecture. For example, there are specific components for location handling (location sensor component), presence (social presence component), and notifications (notification component) which are explicitly invoked through other components (e.g. authorisation and policy management components). For this, a semi-formal representation (in form of block diagrams and enumerated interaction arrows) was used. The initial architecture is essentially services-based and the overall architecture diagram is depicted in Figure 73 on p.198.

We also generally could assess that such approach supports a very high-level of abstraction and delegates the assignment of the technical components to a given topology (e.g. Client-Server or P2P topology) as well as different trust model etc. to further steps. Thus, such design approach supports adequately i.e. high-level generality, one of the main aims of PICOS.

We also recognized, that the approaches described in Ch.14 (i.e. PICOS features have to be seen as services that can be hosted locally or centrally) should support these aims, namely, different topologies as well as different community trust models as described in D4.1 with the help of the PICOS toolbox. When considering the description of the PICOS service toolbox in Ch.10, this toolbox is intended to primarily support community designers by building community-specific solutions. Ch. 10 describes that the toolbox can be seen as a set of APIs within a SDK, which provides building blocks to community developers for (1) creating or (2) customising their communities as well as associate privacy and trust management features according to their needs through the interfaces provided (e.g. using service orchestration). For instance, the PICOS implementation will need to integrate functions

[9] See D4.1 subsection 8.1.3 p. 54

[10] In addition to the clearly related components to LBS and communication functionalities, the components Application Orchestrator, Authorisation, External Service Delivery, Importer/Exporter, Reputation Management, Service Selection, Event Logging, and Secure Repository describe how they handle location as presence information as well as trigger notifications and support communication/messaging.

in order to enable privacy and trust into existing community management and identity management systems. This case is briefly described in Ch14 (example implementation) for the client-server topology. However showing how a PICOS toolbox could be reached needs in our opinion further explanation in the text of Ch. 14 with more concrete examples how to perform this (e.g. by describing concrete steps to carry out such integration and possible deployments).

3.3.3.3.2 Review of the proceeding of WP4 for deriving the design and architecture based on the needs and requirements

The next evaluation step consists of a review of the proceeding followed by designing and architecting the platform based on the gathered needs and requirements, because it affects the results in terms of functionality and therefore the evaluation criteria (such as satisfying the aim of reaching "a generic PICOS toolbox" as mentioned in the previous section). Indeed, the design and architecture of the platform were partially achieved by eliciting scenarios from the stakeholders which state the needs and requirements in terms of functionality to be supported.

D4.1 follows a user-centred and scenario-based proceeding for eliciting the requirements from D2.4 (such as user stories, interviews and questionnaires). In general, PICOS user scenarios are artificial scenarios describing some interactions of the users with the system. Therefore, the scenario-based description of PICOS use cases (PUCs) is one of the main concepts upon which the design and architecture of the PICOS platform are built (see D4.1 Ch.3.1: Relationship between scenario, the architecture and the prototype). Use cases have become state of the art to sharp the focus and support design and architecture decisions. Another main concept consists of the 23 PICOS principles (PPs) described in D4.1 Ch.7 in terms of their contribution to the architecture where some principles contribute to more than one category.

In order to be more specific and to address concretely the end-user needs of the “Angler Community”, “user requirements” were derived. D4.1 mentions, *“We believe, that the best way to express members requirements is in terms of what they want from their community”*. The authors believe that members would say for example: *“We want to send messages to other members and, in general ,to have access to a range of different communication services, including real-time interactive instant messaging and push-pull-notification (e.g. voice/text messaging)”*. Eleven high-level requirements are expressed in this form based on this proceeding. Then, a set of 15 PFs as mentioned before is expressed in form of categories addressing these high-level requirements (see D4.1 subsection 8.1.3).

D4.1 also mentions that components groupings are referred to in PICOS as Tier-0 functionality while individual components are described as either Tier-1 or Tier-2 depending on their functionality. The general rule is that when a component relies on one or more other components for its functionality, it is called Tier-1 component and the subservient component are called Tier-0 components. There are five Tier-0 grouping, nine Tier-1, and four Tier-0 grouping components. In order to specifically address the needs of the “Angler Community”, D4.1 explains the functionality of those component groupings and their concrete components with PUCs.

Using user scenarios and related use cases for designing and architecting a platform is surely beneficial and very positive. However, the assessment of requirements fulfilment becomes so a tedious task, especially because D4.1 never establishes a link to the fulfilment to the requirements of D2.4 explicitly in the textual description. Considering in the textual description of the next deliverable D4.2 for the “Gamer Community” to show, which requirements are fulfilled/considered from which component will be certainly an enhancement. Another good point is to explain the different PUCs with

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

the help of diagrams. Here too, a possible enhancement can be attained by introducing a kind of legend or providing further explanations related to the kind of diagrams used and their (sub)elements (e.g. component representation as blocks, using arrows for information flow or communication, how different enumeration types have to be interpreted in the same diagram and so forth) . An improvement will be to use directly, widely accepted semi-formal notations such as UML that are adequate for all project stakeholders (i.e. user, architect and developers).

3.3.3.4 Summary of findings and recommendations

In general, we can assess that all requirements related to location based services and communication functionalities have been considered in D4.1 and are fulfilled by the platform design and architecture. A more explicit linkage between D2.4 and D4.1 would underline, how and where requirements have been realized in the architecture.

The approach chosen in D4.1 is viable to define the architecture. However some more concrete guidelines for further project phases, especially WP5.1 and WP6.1, are needed in order to turn the high level architecture and design into a real implementation. This is especially important against the background, that partners contribute existing knowhow and products which needs to be thoroughly integrated, to reuse as much as possible and at the same time to create a more general, product and community independent solution.

Some figures and notations are not self-explaining and should be substituted by more widely used notations like UML to avoid misunderstandings.

3.4 Economic evaluation

3.4.1 Methodology used

The following economic evaluation puts the PICOS Architecture in the context of business aspects of trust, IdM and privacy, as the collection, processing and exchange of information are key economical success factors for online and mobile communities. To keep a focus under the constraints of the scope of this evaluation this will not be a definitive analysis.

The aimed goal is to determine, how the PICOS Architecture copes with the economic aspects of the PICOS Requirements and with the economic view expressed in the PICOS Contextual Framework. The economic discussion and examination how well the architecture meets economic aspects of the PICOS Requirements and picks them up results in a much clearer understanding of the requirements. Additionally, this evaluation will result in recommendations on how and where to integrate economic aspects in the features and components of the 2nd cycle of the PICOS Architecture.

3.4.2 Documentation used

This evaluation is based mainly on documentation provided by the PICOS project. As we pick up the view from the PICOS Contextual Framework (D2.3) and the PICOS Requirements (D2.4), we examine how economic aspects of trust, IdM and privacy are covered and taken into account by the PICOS architecture (D4.1).

The PICOS Contextual Framework (D2.3) describes contextual aspects of online and mobile communities like technological and business aspects. The PICOS Requirements (D2.4) contains the collected, community specific and generalised requirements and thereby provides the basis on which the architecture was developed.

The PICOS Architecture (D4.1) documents the PICOS platform architecture itself, including features, components and their relations. It delivers a complete overview of the PICOS functionality and technological aspects.

3.4.3 Evaluation of the requirements and functionalities of the Platform design and architecture

As stated above, basis for the development of the PICOS architecture are the gathered requirements in the PICOS requirements deliverable (D2.4).This evaluation focuses on the economic requirements identified in the document (D2.4), speaking of the requirements on data brokerage especially advertising. Together with the PICOS Contextual Framework, which focuses on the collection, processing and exchange of information, the following requirements were identified as economic key factors for establishing an economic view on the Architecture:

- (R.A1) Considering Social Capital as Value of Communities

The control over personal data with regard to its release, processing and access to other parties plays an important role for most business models in online and mobile communities, as unintended and improper incidents could affect e.g., the acceptance of a community.

- (R.A2) Pre-filtering of Potential Advertisers

To ensure that community members identify themselves with the community and do not feel negatively touched, the community provider is responsible for selecting advertisers that respect official regulations and follow best-practice guidelines.

- (R.A3) Determining and Negotiating the Right Set of Necessary Personal Information

The goal is to support users in their sovereignty by providing the recipient of the advertisement the opportunity to assess that only the necessary subset of personal information is requested and that information are available why the data is requested in the particular context. The most difficult issue here might be to determine the necessary set of context information that an advertiser would like to gather and process. For achieving this, linking of different information sources, such as the presence information of a community member in his community environment and his location data might be necessary. However, being informed that both data sources get linked, to which degree and communicating choices to consent or object against are crucial for the acceptance by consumers.

- (R.A4) Finding the Advertisers of Interest

Assessing which needs can or even have to be satisfied by advertisements, respectively by offering services and goods, in an intuitive manner is crucial for their acceptance. Providing a fine-tuned subset of highly interesting topics could help to avoid this phenomena.

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

- (R.A5) Advertisement at the Right Point in Time and Place

Before giving any personalised information to advertisers, privacy users might have a demand that advertisers provide information that is relevant and of value for users. In reality, users normally start with data, which has a low level of sensitivity and offer more accurate and qualified data when they are convinced by the provided services. Consequently, the advertiser must be able to interpret the users' context, in order to be able to provide valuable ads. A problem occurs by applying this method because the advertiser has to make decisions based on partial and context-specific information. However, a positive reputation of an advertiser could probably weaken the problem if he has a sponsor in the community.

Evaluating Features of the PICOS Architecture

As the collection, processing and exchange of information are key economical success factors the focus in this evaluation of features first will be set on the Personalization concept (PF4) of the PICOS Architecture.

PF4 Personalization

The PICOS architecture allows a community member to personalize his profile by partitioning his personal information according to the current context. The personalization concept (PF4) in PICOS is suitable for making personal information selectively available to other community members but also to external services, e.g., advertisers, who use the personal data for placing personalized ads in the community. The question of who has access to what kind of user's personal information is therefore becoming more and more important also with respect to advertising. Thus, it is also accounted in the PICOS requirements to start with the pre-filtering of potential advertisers. And in a second step, to identify the advertiser of interest by determining and negotiating the right set of necessary personal information and place it at the right point in time and place.

However the personalization concept described there, focuses on a user centric view, regarding the user profile. It does not oppose the marketing perspective, by describing how marketers could particularly make use of the information provided, especially to configure and distribute personalised ads. Integrating the marketing / advertising view for retrieving personalized ads would help to leverage the potential of personalization within a community from an economic point of view.

As a recommendation for the Personalization, features for marketers and external service providers on how to get personal information, provided by community members, should be integrated. This could be done by a respective feature, which allows marketers, to e.g. analyse the personal data provided by the users with regarded to certain aspects and based on such analysis to configure criteria that should be addressed with which ads.

PF6 Searching

The PICOS Architecture describes the existing search functionalities currently in use on the Internet and identifies the key privacy and trust issues that occur and how they are technologically handled and solved within the PICOS architecture. It further describes a basic search functionality as a part of the PICOS architecture, allowing users to search for other users and contents.

The problem which can be identified here is, that there are no specific marketing mechanisms described in detail in the context of the PICOS search. But as long as marketing is not intended to be an integral part the PICOS search (as it is e.g. on Google), the benefit (from the users point of view) of the described features related to privacy and data protection remains extremely limited.

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

As a recommendation, it should be described in detail, how the PICOS search could integrate marketing mechanisms, which extend existing mechanisms (e.g. by providing ads not only based on keywords, but also on user profile and context information) and thereby also outline the possible benefits of the introduced privacy related features.

PF9 External Services

The external services form the basis for any kind of integration of 3rd party services, such as marketing and advertising services in a social community. By that no single specific requirements are addressed, but marketing and advertising as general requirement is enabled. However, it is not explicitly specified how such an interface could be used exactly by 3rd party services and the community provider.

As a recommendation, this should be outlined further. In addition, examples related to the angler and gamer community context should be added.

Evaluating Components of the PICOS Architecture

Payment Services (Component)

The Payment Services component is described as a component that provides access to different external payment services, e.g., Visa, MasterCard, and PayPal, to enable members to purchase services offered by the community.

Basically it is an external service, but is included as a specific component, to address privacy issues that arise through advertising. It does not become clear, to which degree, payment service differs from the simple integration of such a functionality as an external service.

Consequently as a recommendation, the privacy issues in the advertising context, and the difference between the Payment Service component and other external services should be described in more detail, to be able to assess its economic impact.

Profile Management (Component)

The Profile Management Component is a basis for the personalisation of the user profile as described before. The component describes the privacy preferences, allowing the community member to specify the level of privacy that applies to all or a part of the personal information. Thereby it covers also the requirement for Determining and Negotiating the Right Set of Necessary Personal Information (R.A3).

Thereby the architecture addresses an important aspect of the privacy related requirements in the context of marketing activities. It allows users explicitly to control the access to personal data, stored in their profiles. However, from an economic point of view, for the 2nd cycle the question will be interesting on how the user can create profiles for advertising and how he/she can differentiate between profile access for (individual or groups of) other users and 3rd parties.

Content Sharing (Component)

The Content Sharing component allows for making content available between members, e.g., by sharing or import/export. It thereby covers the economic aspect of exchanging information between community members and third parties. An interesting question in this context would be to what extent the content can be drawn on for marketing and advertising purposes, possibly combined with other personal (context) information. This could allow the provision of improved targeted ads for the user, with a further reduced risk of distraction and irrelevance. Thereby, the component could also further address the “Finding of Advertisers of Interest (R.A4)” requirement and the “Advertisement at the Right Point in Time and Place (R.A5)” requirement.

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

Especially with regard to upcoming questions and challenges regarding data protection / privacy, the question to what extent content can be drawn on for marketing purposes can prove as a valuable extension for the next version of the architecture.

3.4.4 Summary of findings and recommendations

In summary the focus of the well defined PICOS architecture on technical functions should be supplemented on certain key features and components with economic aspects, especially with a focus on marketing and advertising.

Regarding Personalization, features for marketers and external service providers on how to get personal information, provided by community members, should be integrated. The same counts for the search feature, which needs to be extended by marketing related mechanisms. Generally, it should also be reviewed on how to give the user transparency on the usage of his data (e.g. Privacy Advisor). Similarly applies for the Profile Management and the question on how the user can create and configure profiles for advertising.

Finally, the architecture could be extended with regard to content sharing and the consideration of personal content for marketing purposes. This would especially allow interesting new opportunities from an economic point of view. Together with the other mentioned recommendations, it could help to extend the economic potential of the PICOS architecture and outweigh its lack of consideration of aspects related particularly to marketing and advertising.

The principle of data minimization is protecting the user on the one hand, but might have negative economic impacts on the other hand. Goal of a second cycle PICOS Architecture from an economic view should be to point out how PICOS is able to balance these two controversy aspects.

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

4 Evaluation of the Platform Prototype (WP5)

4.1 Summary presentation of the Platform Prototype

4.1.1 Overview

The first version of the prototype PICOS platform consists of two main elements:

- PICOS platform (developed by WP5)
- PICOS trial application (developed by WP6)

The WP5 platform offers a community-agnostic service that supports the angling community that was involved in the first trial. The platform will also support future trials, albeit with additional -yet undefined - enhancements addressing the emerging requirements of the gaming community. While the requirements for the angling community have been used as the basis for the design, the implementation uses industry standard approaches, e.g. XML for data structures and meta-languages to describe user content.

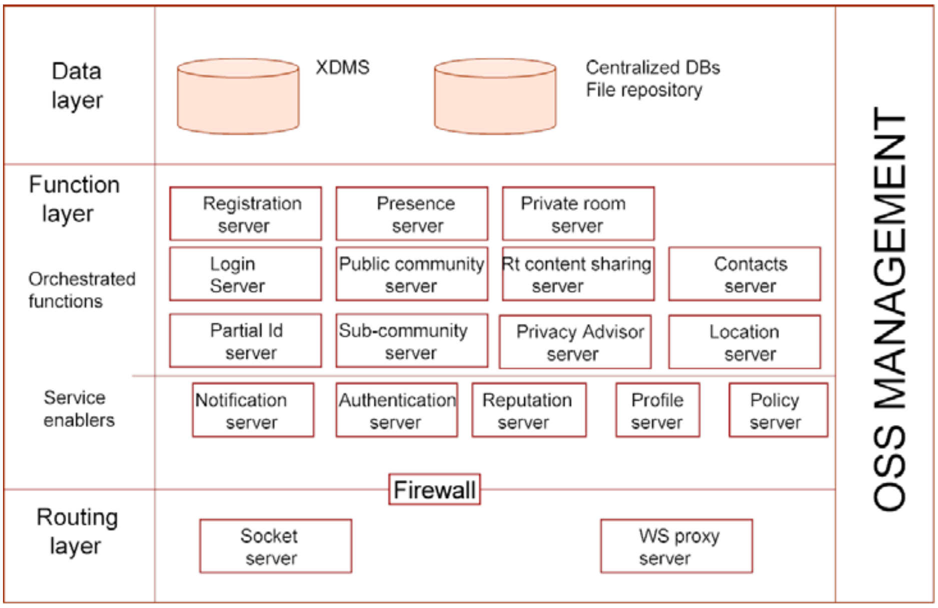
The design philosophy is that users orchestrate actions, typically from their mobile handset, the Nokia 5800 ‘Xpress Music’ smartphone touchscreen appliance. While the handset provides an interface and displays retrieved information, the logic that defines some of the application behaviour is provided by the ‘back-end’ platform. A design goal has been to minimize the processing required by the handset. In addition to centralize the operating logic, communication between server and handset is kept to an absolute minimum.

4.1.2 Implementation

The PICOS platform implements a set of components, as defined in the D4.1 architecture, in order to offer strong identity management, trust and privacy capabilities, including community management. Components are accessed by the application in line with the interactions defined in the PICOS use cases. These components can be separated into two categories:

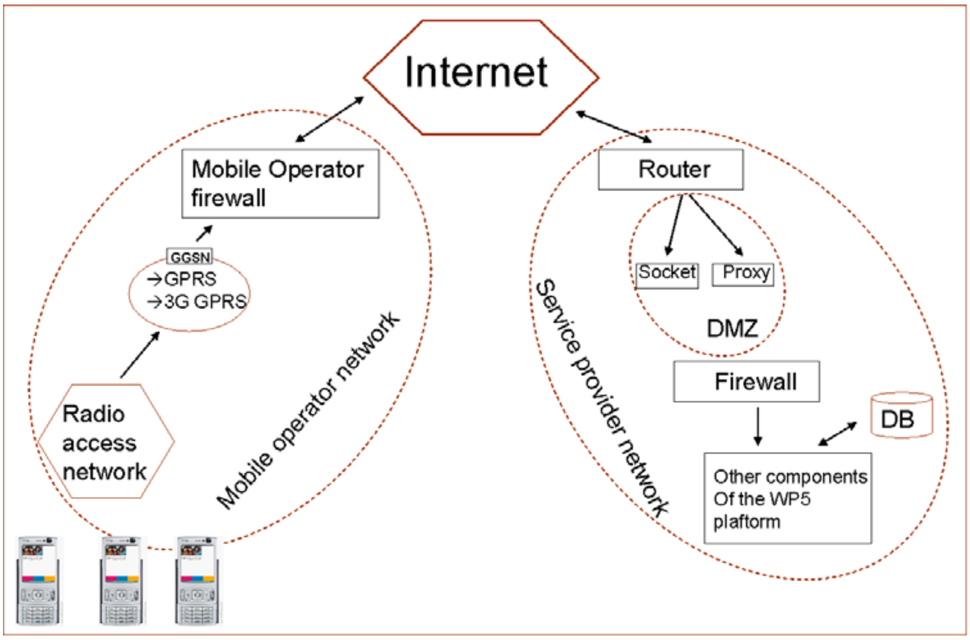
- Service Enablers – offering specific re-usable function
- Orchestrated Functions – offering sophisticated functional interactions between components

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



Most functionality is implemented as web services, and interfaces are defined to provide access by the client and other components. A client RPC (Remote Procedure Call) library is implemented using the Java 2 Micro Edition (J2ME) environment on the handset, which in turn interacts with platform support and communication services. At the platform, an RPC gateway (HP Opencall) acts as a front end for all mobile interactions. The gateway also manages access to the platform, using login credentials as a form of user authentication.

Since the PICOS platform connects to the Internet, protection against external attacks is essential. Thus, the RPC gateway server (being the front-end access of the platform for client RPC request) is installed in the DMZ encompassing the service provider network, all of which is protected by a firewall. This arrangement is summarised in the following figure:



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

4.1.3 Client – platform interaction

The Angler Application is composed of client-side and server-side components. As previously mentioned, the client side consists of a Nokia 5800 mobile phone on to which is installed the PICOS Angler application. On the server-side, the PICOS platform comprises of the platform components and the RPC Gateway (which acts as a proxy to provide a unified access to the platform). Communication and data exchange with the PICOS platform is by the Client API, using client implementation and RPC Gateway library.

The platform also implements an Orchestration Layer, which communicates with the other platform components in order to aggregate low level functions into application-specific features.

4.2 Legal evaluation

4.2.1 Methodology used

The legal evaluation of the PICOS Platform Prototype, as described in the PICOS Deliverable D5.1 “WP5 PICOS Platform Description document”, is based on the European legal framework on data protection. In the field of European Union law, the Charter of Fundamental Rights of the European Union (hereinafter EU Charter) provides for the respect for private and family life (Art.7) and the protection of personal data (Art.8), while the Data Protection Directive (1995/46/EC) has been adopted to guarantee efficient data protection. The prototype is evaluated against the data protection principles that are included in the Data Protection Directive (1995/46/EC). By taking into account the data protection principles already in the design phase of the PICOS prototype, PICOS is following and realising the “privacy-by-design” model, which is promoted by the European Commission.

The main goal of the legal evaluation of the PICOS Platform Prototype is to examine whether the PICOS platform prototype is built in compliance with the European data protection legislation and the relevant data protection principles. The focus of this evaluation lies within the platform and the implementation of the PICOS architecture in it. The legal evaluation will assess the adequacy of the proposed policies and the compliance with the defined data protection principles and the legal requirements as described in PICOS Deliverable D2.4 “Requirements” and in PICOS D4.1 “PICOS Architecture”.

4.2.2 Documentation used

The main document for the legal evaluation of the PICOS Platform Prototype naturally is the document where the PICOS Platform Prototype is described, i.e. PICOS Deliverable D5.1 “WP5 PICOS Platform Description document”, and more specifically Chapter 7 “How the WP5 PICOS platform implements the Privacy Principles”. The legal evaluation will also be based on PICOS Deliverable D2.4 “Requirements” and more specifically on its Chapter 6 – “Legal Requirements” and Appendix B (Summary of Legal Requirements), on the PICOS D4.1 “Architecture”, as well as on the analysis conducted in D2.3 “Contextual Framework”. The Data Protection Directive (1995/46/EC)[11] will also be taken into account, as referred to in the aforementioned PICOS Deliverables.

[11] Directive 2002/58/EC (ePrivacy Directive) and Directive 2006/24/EC (Data Retention Directive) are not directly applicable to PICOS as they only apply to “publicly available electronic communications services

4.2.3 Evaluation of the requirements and functionalities of the Platform Prototype

The fundamental data protection principles that apply to the processing of personal data are included in the Data Protection Directive and serve as obligations, with which the data controller needs to comply (Art. 6(2) Data Protection Directive). The way how the privacy principles are implemented in the PICOS WP5 platform, as described in Chapter 7 "How the WP5 PICOS Platform implements the Privacy Principles" of PICOS Deliverable D5.1 "WP5 PICOS Platform Description document", is evaluated on the basis of the principles on the processing of personal data as codified in Appendix B "Summarisation of Legal Requirements" of PICOS Deliverable D2.4 "Requirements"[12].

a. Principle of Fair and Lawful Processing

The principle states that the application shall collect and process personal data in a fair and lawful way and can be found in art. 6(1) (a) of the Data Protection Directive. This principle is further being specified in Articles 10 and 11 of the Data Protection Directive that specify the information that need to be given to the data subject, in order for the processing to be considered as fair and lawful.

The associated Privacy Principles ("PrP") are the following:

PrP1 "Notice of collection": The WP5 PICOS platform ensures that the data subject is informed about the collection of data, the types of data that are collected and the community policies related to data collection and data storage.

PrP2 "Policy Notification": The WP5 PICOS platform displays the information regarding the final registration of the user, so that he is informed about the applicable policies on consent, access and disclosure. In this way the lawfulness of the processing is promoted.

PrP3 "Changes in Policy or Data Use": The WP5 PICOS platform will enforce any customisation of privacy rules attached to user attributes. In order to ensure the fairness and lawfulness of the processing, no data mining function is integrated into the platform, nor is any external server allowed to access the user data.

PrP10 "Fair and Lawful Means": The data collected by the PICOS platform are entirely under the control of the end user. All information is collected via fair and lawful means, as the end user controls fully his information that is being processed.

PrP19 "Public Policies": The PICOS Terms and Conditions contain the PICOS community policies and the user can enable their display at any time during the log-in session. In this way he can be informed about the policies followed by the PICOS Community.

b. Legitimate Processing

offered via a public electronic communications network", which is not the case for the PICOS platform nor for the PICOS application prototypes.

[12] Principle LR.A.7 "Principle of security" of Appendix B "Summarisation of Legal Requirements" of PICOS Deliverable D2.4 "Requirements" is evaluated in detail by the technical evaluators in the respective parts of this deliverable. Principle LR.A.8 "Principle of Notification to the Supervisory Authority" is outside the scope of this analysis, as this is an action of the data controller that needs to be made in person to the Data Protection Supervisory Authority. With regard to the rights of the data subject, the Principles LR.B.5 "Right not to be subject to an Automated Decision" and LR.B.6 "Right to Seek Regal Relief" are not applicable to the WP5 PICOS Platform.

According to Article 7 of the Data Protection Directive the application shall process personal data only based on a legitimate ground. The collection and processing of the personal data requires the consent of the data subject (Art. 7(a) Data Protection Directive), unless one of the grounds for legitimate processing applies. In the PICOS applications the consent of the user will almost always be needed as a ground for legitimate processing.

Besides the general policy notification that notifies the users that their consent is needed for the processing of their personal information, the legitimate processing principle is also associated with the following Privacy Principles ("PrP"):

PrP5 "Sensitive Information": In principle, PICOS communities will not process any sensitive information. Shall there any PICOS application that enables the sharing of such information, then the user has to give his explicit consent via the privacy rules relating to these data, as offered by the WP5 PICOS platform.

PrP6 "Informed Consent": The WP5 PICOS platform allows the user to manage his consent via the policy rules that can be modified via the client application.

PrP7 "Change of Use Consent": The WP5 PICOS platform strictly enforces default community policies, so that every user attribute is private. The consent of the user is needed for the use of personal data for any purpose other the one stated at the time of the collection of the data.

PrP8 "Consequences of Consent Denial": Whenever the consent is denied by a user, the requester receives an error message that informs him about the denial.

PrP13 "Third-Party Disclosure": No user data is disclosed outside the community. Within the community, the disclosure of personal information is managed by the user via the privacy rules and is realised only after he consents to such disclosure.

c. Principle of Finality/Purpose Limitation

This principle of finality or else purpose limitation is established in Art. 6(1)(b) of the Data Protection Directive and states that the application shall use the personal data only for the specified and legitimate purposes. The data shall not be further processed in a way incompatible with those purposes.

The following Privacy Principles are implemented in compliance with this principle:

PrP1 "Notice of collection": The purposes for which data are processed are explicitly mentioned in the Terms and Conditions of the PICOS community.

PrP4 "Timing of notification": The data subject is informed about the purposes for which data are processed before the actual collection of the data and more specifically at the time of the final registration of the user, as the first screen before any data collection.

PrP11 "Acceptable Uses": The user can only treat the data within the uses that are allowed by the platform and thus only within the specified and legitimate purposes.

PrP13 "Third-Party Disclosure": No user data is disclosed outside the community and within the community the data are managed by the user via the privacy policies within the specified and legitimate purposes, in conformity to the purpose limitation principle.

d. Principle of Data Minimisation

The principle of data minimisation requires that the data are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 6(1)(d) Data Protection Directive).

This principle is implemented in the WP5 PICOS platform via the following Privacy Principles:

PrP1 “Notice of collection”: The Community Terms and Conditions inform the user about the types of personal data that are collected and processed by the PICOS community.

PrP9 “Limitation of Collection”: The WP5 PICOS platform has implemented the data minimisation principle in the most privacy-friendly way for the user, by only requiring a pseudonym. The pseudonym is the only user attribute that is essential to gain access to the platform. The addition of further attributes is thus left to the discretion of the user.

e. Principle of Data Quality

According to the data quality principle the application shall use accurate and, where necessary, up to data information (Art. 6(1)(d) Data Protection Directive). The user has full control of his information that is entered in the system and is given the needed tools to update his personal information. Therefore the existence of “Fair and Lawful Means” in the WP5 PICOS platform ensures compliance with the data quality principle:

PrP10 “Fair and Lawful Means”: The WP5 PICOS platform places all user information under his control and allows him to update the content of it.

f. Principle of Conservation

The principle of conservation requires that the application shall keep personal data only for the necessary purpose, for which data were collected (Art. (6)(1)(e) Data Protection Directive).

The associated Privacy Principles are the following:

PrP1 “Notice of collection”: The data subject is informed via the Terms and Conditions of the community, before any collection of his personal data is realised, regarding the period during which his information will be kept. This information is presented before the final registration of the user on the first screen before any data collection.

PrP12 “Data Retention”: The data are kept for the time that is required for the provision of the service offered by the PICOS community. The personal data of the user are stored until the time when a user is revoked. Upon revocation, all user attributes are deleted.

g. Rights of the data subject: Right to Information

In respect to the data subject’s right to information, before the processing of personal information, the data subject shall be given information at least regarding the identity of the data controller and the purposes of the processing for which the data are intended (Art. 10 Data Protection Directive). The information regarding the personal data that are being processed shall be given to the data subject in an intelligible way (Art 12(a)2nd section Data Protection Directive).

The Privacy Principles that are implemented in respect to this right of the data subject are the following:

PrP1 “Notice of collection”: The data subject is informed via the Terms and Conditions of the community, before any collection of his personal data is realised, regarding the identity fo the data controller, the typed of data that are processed, the purposes they are processed for and the period during which his information will be kept. This information is presented before the final registration of the user on the first screen before any data collection.

PrP2 “Policy Notification”: This principle is closely linked to the aforementioned PrP1. The WP5 PICOS platform displays the information regarding the final registration of the user, so that he is informed about the applicable policies on consent, access and disclosure.

PrP16 “Provision of Data”: In compliance to the principle that the data shall be provided in a clear way, the user can access his personal data when he logs-in to the service.

h. Rights of the data subject: Right to Object

In compliance with a fundamental right of the data subject, the application shall allow him to object to the processing of his personal data (Art. 14 Data Protection Directive).

The WP5 PICOS platform offers the possibility to the data subject to object to the processing of his personal information in two ways: By refusing to give his consent in the processing of his information (for instance by denying sharing specific information) or by modifying his preference via the privacy rules). The right to object is realised via the following Privacy Principles:

PrP8 “Consequences of Consent Denial”: A user can refuse to give his consent in the processing of his personal data, in which case the requester receives an error message that informs his about the denial.

PrP10 “Fair and Lawful Means”: The data collected by the PICOS platform are entirely under the control of the user. The user can revoke the permission he has granted to other members to his profile, presence, location or contact list. In this way he is withdrawing his consent and is exercising his right to object to the processing of his personal data.

i. Rights of the data subject: Right of access

A basic right of the data subject is his right of access, i.e. his right to be informed about his personal data that are being processed (Art. 12(a) Data Protection Directive).

The WP5 PICOS platform offers the possibility to the user to have a full overview of his data that are being available to the community and can be processed. This is realised via the Privacy Principle of “Access to Information”:

PrP15 “Access to Information”: Any data relating the user (user-profile, presence, location, contact-list, content in private room, forum contributions) is made available to the user through the client application. In this way he can exercise his right of access.

j. Rights of the data subject: Right to Rectify, Erase or Block

An application shall allow the user to rectify, erase or block his data (Art. 12(b) Data Protection Directive).

The WP5 PICOS platform allows the user to modify his data that are being available to the community and can be processed, to erase them or block access to them. This is realised via the following Privacy Principles:

PrP10 “Fair and Lawful Means”: The data collected by the PICOS platform are entirely under the control of the user. The user can erase his personal data or can block the permission he has granted to other members to his profile, presence, location or contact list.

PrP17 “Correcting Information”: The personal data of a user can be modified at any time by the user, so that they are corrected.

4.2.4 Summary of findings and recommendations

As illustrated by the analysis that was conducted above, the WP5 PICOS platform correctly implemented all the relevant data protection principles. The way the WP5 PICOS Platform has realised the PICOS Privacy Principles has been evaluated against the principles on processing of personal data, as they are codified and summarised in Appendix B of the PICOS D2.4 “Requirements Deliverable”. The PICOS WP5 Platform offers a legally compliant platform, with regard to privacy and data protection, for the development of future PICOS Communities.

4.3 Technical evaluation

4.3.1 Trust, Privacy & other technical elements

4.3.1.1 Methodology used

In this part of the technical evaluation we will focus mainly on the issues relevant to trust and privacy principles. Trust and privacy are basically critical objectives in the PICOS Architecture and therefore the evaluation of the PICOS Architecture will be done in a way we will discuss scenarios, features and components relevant to trust and privacy, their relevancy and technical aspects.

4.3.1.2 Documentation used

The main source of documentation for this part of evaluation was D5.1.

4.3.1.3 Evaluation of the requirements and functionalities of the Platform Prototype

We will start with the list of proposed privacy and trust related goals of the first prototype implementation:

- Implement the support of multiple partial identities per user so that the user has full flexibility to manage which identity profile fits the best which community context (forums; sub-community; chat...). The partial identity attributes are very rich and include presence, privacy rules, profile, contact list...
- Implement a very flexible policy engine to manage privacy and privilege rules attached to any attributes of users of community resources.
- Allow customization of non hard-coded privacy rules at fine granularity (presence, location, profiles...).
- Centralize the community policy management and allow rapid customization of these policies depending on the supported community (the application).
- Implement a privacy advisor component whose role is to advise the end user of any action that would endanger his privacy.
- Encrypted channel between the client and the server.

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

- Implement a reputation framework based on user (partial identity) contributions (content, forum contribution). At any time users can get user reputation information and use community facilities (contact creation, start sub-community, start chat...).
- Implement partial identities in such a way that generic user information cannot be hidden in the different identities enforcing trust about profile information.
- Allow correlation of identities at the platform administration level to user eliminate misbehaviours behind partial identities.
- Implement privacy advisor reputation management in sub-community to warn his administrator regarding a member with low reputation.

There are 16 architecture component based on the PICOS use cases[13] that were identified as candidate elements for the first PICOS prototype. We provide a list of components that are privacy and trust related:

- Access control
- Partial Identity Manager
- Privacy Advisor
- Location Sensor
- Sub-community management
- Reputation Manager
- Privilege Manager
- Profile Manager
- Privacy Manager
- Social Presence

In the following text, we will discuss how these components (with regard to privacy and trust) were implemented in the first PICOS prototype.

In order to meet the requirements of PICOS, the platform and the interactions within the platform were described with an object oriented model. Each component of the platform manages one or multiple objects, has access to its attributes and methods.

User object

User object is one of the root objects of the platform. Attributes of this object with regard to privacy and trust are:

- Private room – content repository attached to one user. Only this user can access that repository.
- User profile – is composed of a set of elements that characterize the user (17 elements). Only one attribute is mandatory to create a profile, namely the pseudonym.

[13] Use cases can be found in deliverable D5.1 on page 16 and 68-90.

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

- Presence – information about the current status of a user. Access to presence attribute is validated against privacy rules defined by the user.
- Location – current GPS position of a user. Access to location attribute is validated against privacy rules defined by the user.
- Contact list – a list of contacts that is associated to a partial identity of an existing member of the public community.
- Sub-community list – each user can join a (public) sub-community and can be invited to be member of a (private) sub-community. This attribute contains all the sub-communities, the user is part of.
- Partial identity list – list of user's partial identities.
- Reputation – number between 0 and 100 representing the average of all the ratings that all the members have sent.
- Privacy rules – a user has the ability to define access rules to some of his attributes (namely the user profile – on a per attribute level; presence; location; private room; contact-list).

Partial Identities

Partial identity is the way users manage their identity in PICOS. One user can have multiple partial identities with different reputation scores; they can share different personal data under different partial identities; they can be a member of different (sub) communities and so on. Attributes of the partial identity object are:

- Profile – each partial identity has an associated user profile. This is actually only a reference to the global user profile.
- Presence – each partial identity can have specific presence information and access to this information must comply with the privacy rules of the partial identity and the requester.
- Reputation – this reputation is separated from the root identity reputation. The reputation of a partial identity is always public.
- Privacy rules – ability to define access rules to some attributes of the partial identity (profile, presence and contact list).

Sub-community

A user can create a group of members of the public community. The creator of such a sub-community can invite other members to join his sub-community. Sub-community can be both private and public.

Relevant attributes of the sub-community are:

- Member list attribute – a list of the members of the sub-community.
- Sub-community reputation attribute – reputation attached to the sub-community, based on the reputation of its members.

4.3.1.3.1Implementation of platform components

Let's now take a closer look on how trust and privacy related component of the PICOS platform were implemented.

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

Public community server

This component is responsible for Category object, Forum object, Member object and related attributes. This component provides access to the forums and public repository and the possibility to create forums and forum threads. For both the forums and the public repository, the client application can decide to allow association of privacy rules to each content they publish via the policy manager. Privacy rules can apply to the content by itself or to sensitive attributes of the content (publisher information, location information, etc.).

Partial identity server

This component is responsible for managing identities of the user. Besides the primary identity created during the registration process, users can create additional identities, called partial identities. The primary goal of partial identities is to keep anonymity of users. User can use either the primary identity or partial identities to use the platform services. Users can also redefine some attributes of their primary identity under their partial identity.

Presence server

This component is responsible for managing identities of the user or partial identity. Presence attributes can be attached to the primary identity or to a partial identity. Users can see the presence information of other users if their privacy rules allow accessing it.

Location server

This component is attached to the primary identity. A user has the ability to update his own location and see location information of another user in case his/her privacy rule allows accessing it. User A can also subscribe to user B location so that he will receive location notification when the user B location is updated. Privacy rules allow defining rules that may request user B authorization when a user requests location or subscription to location information. Privacy rules may restrict location information access to a list of users or a sub-community or a role in a community context. The client application is controlling these “per instance” policy rules using the policy interface for the provision of these rules.

Policy server

This component is responsible for storing rules attached to various objects or attributes of objects and for evaluating user action based on the set of rules. Other components are responsible for asking the policy manager to evaluate action on resources (for example user attributes or community resources). Users can create various privacy policies on their attributes by specifying who has access to this information. The platform stores these policy rules and enforces them when a user decides to perform action on a particular resource. Overall policy server allows creating highly detailed privacy policies but this functionality must be delivered to the end users in a way that they will get to know how it works and what it is good for.

Reputation server

Users contributions in forum, public repository – on both community and sub-community level, can be rated by either the members of the public communities for public contributions or by the members of sub-communities for sub-community contributions. These ratings have a direct impact on the

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

reputation of a user. The reputation component also stores additional user related information such as the number of contributions as well as the number or ratings.

Privacy Advisor server (PA)

Privacy Advisor (PA) is a special assistant within the PICOS platform which role is to inform the user of non obvious possible consequences of his action on trust and privacy (typically via notifications). PA examines personal information contained in the content. The PA provides advices in three different scenarios:

- Content awareness – content is examined each time a member contributes to a forum, a public or private sub-community or to a repository.
- Sub-community dynamics awareness – PA of a creator of a sub-community “monitors” the reputation of other members of that sub-community and notifies the creator.
- Workflow awareness – when a member chooses to delete an identity or to leave the community, he decides what happens to the data that the community retains.

Private Room server

This component stores personal content in a private and personal repository. This repository is accessible only by the owner. Content from the private room can be copied in a sub-community repository or in a public community category/sub-category.

Profile server

This component is responsible for managing profiles attached to identities (either root or partial). The profile server enforces the policies defined in the policy server.

4.3.1.4 Summary of findings and recommendations

- Contact list attribute (user object) – the description does not cover who has an explicit access to this attribute (although this access can be defined in the privacy rules attribute).
- Sub-community list attribute (user object) – the description does not cover who has an explicit access to this attribute (although this access can be defined in the privacy rules attribute).
- Reputation attribute (user object) – definition of an algorithm used for computing reputation value.
- Member list attribute (sub-community) – definition does not describe who has access to this list (whether everyone can see a list of members of a sub-community or only the member of the sub-community can see this list and how this is influenced by the “visibility” attribute).
- Sub-community reputation attribute – there is no description of how this score is computed.
- Partial Identity server – more precise distinction of what can be updated on the partial identity level, what can be updated on the primary identity level and where the overlaps are.

4.3.2 Community focus

The focus of this part of the technical evaluation is on the implementation of the PICOS platform, especially the components which have a community focus. Chapter 3.3.2 “Community focus of the Evaluation of the Platform Design & Architecture” has identified the sub community features being the key features regarding the community focus. Therefore the implemented platform has to be evaluated regarding these features

4.3.2.1 Methodology used

The goal of the evaluation in this section is to provide information about how far the implemented platform prototype is able to fulfil the features, components and use cases in D4.1, which themselves try to put the associated requirements from D2.4 into practice.

In chapter 3.3.2 (Community focus) six features[14] have been identified from D4.1 which are directly related to the community focus. In addition eleven components[15] have been identified from D4.1 which are directly related to the community focus. And there are seven use cases[16] in D4.1 which are of relevance for the community focus. Therefore the implemented platform has to be evaluated regarding these features, components and use cases.

For the evaluation, a bottom-up approach has been used. Thereto for every single feature, component and use case it has been examined whether the platform realizes the corresponding specific PICOS concept in an appropriate way.

4.3.2.2 Documentation used

The documentations used for this evaluation are the Deliverables D4.1 Architecture and D5.1 WP5 PICOS Platform Description document. D4.1 addresses the current state of the platform design and architecture, D5.1 the implementation of the design and architecture, especially the chapters 3 (Mapping between WP4 Architecture and WP5 PICOS platform Components) and 4 (Platform Use Cases). D4.1 is used to evaluate to what extent the WP5 Platform meets the gathered requirements in this document. For looking at details of the implementation of the design and architecture the API descriptions of the internal document WP5 Platform Functional Specs[17] were used.

4.3.2.3 Installation – Functionality & Operation

Regarding the installation of the sub community component there were no special requirements. It was important that it fits the whole architecture, in detail that the overlaying web service can communicate with the component respecting the specification.

The open source social engine “Elgg” was chosen as a basis for the component as it offers many basic routines required by Picos, especially routines for private and public communities, for content sharing and for text pages. Elgg is written in PHP and bases on a MySQL database, and is referring to this compatible with the other components of the WP5 platform (the Elgg based component operates on the same system as the whole Picos platform). Elgg also offers an rpc interface; the Picos rpc gateway/web service is able to communicate with the Elgg component using this rpc interface. Therefore the Elgg compoment was integrated into the platform without greater problems. Especially a complete rpc interface was created that fits the defined web service interface.

[14] PICOS D4.1 “Architecture”: PF1 Reputation, PF2 Content Sharing, PF3 Registration, PF7 Sub-Communities, PF9 External Services, PF13 Intra-Community Interaction

[15] PICOS D4.1 “Architecture”: 9.5.3 Access Control, 9.5.6 Authentication, 9.5.7 Authorisation, 9.5.16 Partial Identity Management, 9.5.18 Preparation Area, 9.5.21 Reputation Management, 9.6.3 Accountability, 9.7.10 Registration, 9.7.11 Revocation, 9.7.12 Sub-Community Management, 9.8.2 Content Sharing

[16] PICOS D4.1 “Architecture”: PUC1 Registration, PUC2 Accessing the Community, PUC3 Revocation, PUC4 Multiple Partial Identities, PUC5 Reputation, PUC7 Content Sharing, PUC9 Sub-Community

[17] PICOS D5.1 “WP5 PICOS Platform Description document”.

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

4.3.2.4 *Evaluation of the requirements and functionalities of the Platform Prototype*

As mentioned above every single feature, component and use case which is relevant for the community focus has to be examined whether the platform realizes the corresponding specific PICOS concept in an appropriate way.

The following table shows, which feature, component or use case has been realised by which platform component. For the features and components the mapping from D5.1 chapter 3 and for the use cases the call flows and descriptions from D5.1 chapter 4 have been used.

Type	Feature/Component/Use Case identified in D4.1	Corresponding Platform Component in D5.1
Feature	PF1 Reputation	2.5.12 Reputation server
Feature	PF2 (Asynchronous) Content sharing	2.5.11 Sub-Community server
Feature	PF3 Registration	2.5.1 Registration server, 2.5.7 Partial Id server, 2.5.6 Public Community server
Feature	PF7 Sub-Communities	2.5.11 Sub-Community server
Feature	PF9 External services	not part of WP5, so it doesn't have to be evaluated here
Feature	PF13 Intra-community interaction	not implemented
Component	9.5.3 Access Control	2.5.4 Proxy Web Service server
Component	9.5.6 Authentication	2.5.3 Authentication server, 2.5.2 Login server
Component	9.5.7 Authorisation	2.5.1 Policy server
Component	9.5.16 Partial Identity Management	2.5.7 Partial Id server
Component	9.5.18 Preparation Area	2.5.14 Private Room server (mapping not mentioned in D5.1 chapter 3)
Component	9.5.21 Reputation Management	2.5.12 Reputation server
Component	9.6.3 Accountability	*Partially implemented in 2.5.19 Logging server (not mentioned in D5.1 chapter 3)*
Component	9.7.10 Registration	2.5.1 Registration server, 2.5.7 Partial Id server, 2.5.6 Public Community server
Component	9.7.11 Revocation	2.5.1 Registration server, 2.5.11 Sub Community server, 2.5.6 Public Community server (not mentioned in D5.1 chapter 3)
Component	9.7.12 Sub-Community Management	2.5.11 Sub Community server

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

Component	9.8.2 Asynchronous Content Sharing	2.5.11 Sub Community server
Use case	PUC 1 Registration	2.5.1 Registration server, 2.5.15. Contact server, 2.5.8 Presence server, 2.5.9 Location server, 2.5.3 Authentication server, 2.5.7 Partial Id server, 2.5.1 Policy server, , 2.5.12 Reputation server, 2.5.6 Public Community server, 2.5.14 Private Room server
Use case	PUC 2 Accessing the Community	2.5.2. Login server, 2.5.15. Contact server, 2.5.7 Partial Id server, 2.5.8 Presence server, 2.5.3 Authentication server, 2.5.6 Public Community server, 2.5.18 Notification server *Not part of the D5.1 Use case: 2.5.10 Policy server, 2.5.17 Profile server, 2.5.19 Logging server*
Use case	PUC 3 Revocation	2.5.1 Registration server, 2.5.15. Contact server, 2.5.8 Presence server, 2.5.9 Location server, 2.5.3 Authentication server, 2.5.7 Partial Id server, 2.5.10 Policy server, 2.5.6 Public community server, 2.5.14 Private room server *Not part of the D5.1 Use case: 2.5.17 Profile server, 2.5.19 Logging server, 2.5.12 Reputation server, 2.5.11 Sub community server*
Use case	PUC 4 Multiple Partial Identities	2.5.7 Partial Id server, 2.5.14 Private Room server, 2.5.17 Profile server, 2.5.9 Location server, 2.5.10 Policy server, 2.5.8 Presence server, 2.5.12 Reputation server *Not part of the D5.1 Use case: 2.5.19 Logging server*
Use case	PUC 5 Reputation	2.5.12 Reputation server, 2.5.17 Profile server, 2.5.19 Logging server *Not detailed specification in D5.1, which components are involved*
Use case	PUC 7 Content Sharing	2.5.6 Public Community server, 2.5.11 Sub Community server, 2.5.16 Real Time Content Sharing server, 2.5.17 Profile server, 2.5.18 Notification server, 2.5.1 Policy server, 2.5.13 Privacy Advisor server
Use case	PUC 9 Sub community	2.5.11 Sub Community server, 2.5.1 Policy server, 2.5.6 Public Community server, 2.5.7 Partial Id server, 2.5.18 Notification server *Not part of the D5.1 Use case: 2.5.17 Profile server, 2.5.19 Logging server*

4.3.2.5 Summary of findings and recommendations

On the one hand there are - due to the selection for the first prototype - components from D4.1 which are not or are only partially implemented. On the other hand there are because of technical reasons new components added (proxy web service, socket server) and components split/completed (split:

profile manager into profile server and privilege server; completed: public community server). Most of the components are renamed ("server" instead of "manager"; private room instead of preparation area)[18]. Additionally, because of the refinement of the use cases the D4.1 use cases do not contain the same components as the D5.1 use cases.

For the technical evaluation of the community aspects of WP5 the related components identified in the evaluation of the Platform Design & Architecture were reviewed against the results of WP5 (D5.1). For example, if you look at use case PUC 2 "Accessing the community" you can see in the right column the platform component used in D5.1 to implement this use case. Also, in italic font you see, which components were expected in D4.1, but not included in D5.1.These results reflect the status of the Design & Architecture in a good way, but in some minor points they differ. This happens mainly in the use cases. Components like the logging server may be left out in D5.1 due to readability.

4.3.3 Location based services and communication features

4.3.3.1 Methodology used

The methodology followed here for the evaluation of WP5 corresponds in general to the fact, that we are evaluating a technical product where a problem has to be solved in terms of requirements fulfilment (i.e. answering the question, were the design requirements mapped into the architecture?). Furthermore, the provided description has to meet the as-is state of the delivered product.

Hence the assessment verifies that

- the outcome of WP4 (first platform architecture described in the deliverable D4.1) is mapped into a real implementation with concrete architecture and components.
- the WP5 Platform description (described in the deliverable D5.1) corresponds to the as-is state of the WP5 platform implementation, deployment, as well as operation. The description has to address the requirements fulfilment and needs for the first prototype especially from the client perspective, namely, WP6 (i.e. providing the needed functionality and API usage description to the WP6 developers)

This verification is done based on the WP5 documentation and implicitly by using the WP5 platform for successfully developing the WP6 application.

4.3.3.2 Documentation used

For the technical evaluation of the WP5 Platform related to the consideration of LBS and communication functionalities, we used mainly the deliverable D5.1 (implementation description of PICOS architecture components in the first prototype), which role was to map D4.1 (Platform Architecture and Design) to a real implementation with a first concrete PICOS architecture. Thus, partially reconsidering the deliverables D4.1 and D6.1 (description of the first application prototype for the Angling community) was substantial.

[18] Please note that the list of implemented components in D5.1 is not complete and that there are naming issues in this document.

4.3.3.3 Installation – Operation & Functionality

4.3.3.3.1 Installation

The PICOS Platform developed in WP5 was hosted along the development period of the first prototype in Grenoble. An evaluation of the installation procedure at this stage of the project becomes therefore impossible. However, it has to be said, that such proceeding was favourable because the followed approach consisted of delivering WP5 functionality in a flexible way and in some cases on demand (e.g. for optimizing client interaction, the WP5 and WP6 developers agreed on sending contact and partial Ids info to the client in the login procedure besides a single response. This function was not foreseen in the initial design). This agile way of collaboration between the WP5 and WP6 partners would be negatively affected in the case of the distribution of installation packages to the different partners (i.e. due to the complexity of managing the distribution and update/upgrade processes etc.).

4.3.3.3.2 Operational Aspects

For operation, each PICOS partner had the possibility to remotely access various management and administration functionalities of its own PICOS instance while the maintenance of those virtual instances was carried out by the personnel of HPF. The HP personnel in Grenoble rapidly reacted to assistance requests and efficiently helped in solving the different problems. A short deployment description from the security point of view can be found on p.20-21 in D5.1. Figure 2 on p.21 (deploying the PICOS platform and the PICOS application) explains the security topology when deploying PICOS. In the case of the delivery of installation packages, detailed information to the security configuration has to be added to the installation and upgrade manuals. This is crucial because the first prototype follows a server-centric approach and therefore, all application and sensible user data are stored on the trusted PICOS platform.

4.3.3.3.3 Functionality

Related to the functionality described in D5.1, the WP5 leader decided to be community agnostic and to choose from the 49 components identified in D4.1 those components which are necessary to implement the selected PUCs. In Chapter 1, a brief description of the components selection process is given. D5.1 mentions that the selection was based on the analysis of the 9 PICOS use cases (PUCs) that were documented in D4.1 and summarizes required components for each PUC. The analysis itself is not deeply described and it seems – according to our understanding - to consist of establishing a link among each PUC and the components it requires (see table on p.16 of D5.1). This analysis determined candidate components to be implemented in the first WP5 prototype at the server side. In addition to this, D5.1 mentions on p.91 that a "*brainstorming has been conducted among partners to refine the value proposition select which uses cases had to be implemented in the first prototype and select the necessary components accordingly*". Furthermore, the concrete architecture is in our opinion a server-centric, service-oriented architecture since WP5 PICOS platform interface is defined as a web service interface reachable via a central server and the internal communication between the components is also carried through web services calls. In order to ease the client development, the WP5 developer team provided to the WP6 developers a client RPC library for the J2ME environment to access the WP5 PICOS platform using Remote Procedure Call (RPC) mechanisms.

D5.1 clearly differentiates between pure WP5 functionality and added server side components or servers provided by other PICOS partners. For instance, it clearly states that WP6 provides an orchestration server layer to optimize the client server exchange for some situations and that in those cases the application is responsible for invoking the platform components in the correct order and not

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

WP5 (i.e.WP5 provides a web services API to achieve the registration). However, to achieve the registration process as described in D4.1, the WP6 client application must call a sequence of functions of this API. D5.1 defines based on this the so called end user orchestration and function orchestration. While the end user orchestration is composed of a chained set of operations in order to support user scenarios, the function orchestration is the outcome of WP5 and consists of basic operations supporting community-agnostic functionalities. This strict separation of responsibilities is also reflected in the description of the PUCs in Chapter 4 of D5.1. There, the PUCs selected in D4.1 were again addressed from the WP5 perspective. Each PUC is accompanied with a detailed textual description of the interaction workflow between client and server as well as involved components at the WP5 server side (see for instance p.70 for PUC1).

In addition to the textual description, call flow diagrams were used for further explanation (see examples on p.71 for PUC1). Provided call flows are similar to UML sequence diagrams and were therefore helpful for the WP6 development team. The goal of these call flow diagrams was to support the validation of component needs against the proposed internal API.

The overall architecture of the first prototype is depicted in D5.1 on p.22 (see Figure 3, functional diagram of the WP5 platform). This Figure could be considered as concrete platform architecture since it introduces different layers (i.e. Function Layer and Data Layer). The access of the mobile client by using the RPC Gateway is also described. D5.1 Figure 1 on p.20 (Interfacing the WP5 platform) provides a detailed view on how the RPC mechanism is implemented. However, we have not found any overall architecture diagram including the Elgg Community Portal integrated in collaboration with ITO as well as the other server side components which WP5 integrates from WP6, namely, the IFM-Geomar FishBase database (see D6.1 p.116-132) and the WP6 orchestration layer (see D6.1 p.39-41). Since WP5 is still controlling the access to those components as well as their storage and establishes the interaction between them in the PICOS platform, providing such architectural information has to be considered in the next WP5 deliverables[19]. Such additional info should not explain the details of those added servers but address the common concerns such as how the data of the Elgg Community Server or AnglersBase server are stored at the WP5 server side and how they could be accessed. A good candidate figure for such additional info will surely be Figure 2 on p.21 (deploying the PICOS platform and the PICOS application) in D5.1.

4.3.3.4 Evaluation of the requirements and functionalities of the Platform Prototype

4.3.3.4.1WP4-WP5 requirements mapping and fulfilment

D5.1 and further distributed internal documentation provided good support to the WP6 developers. For instance, concrete code examples were made available for the developers showing how to use the client side RPC library. Another part included later as a part of D6.1 (see Community Application Prototype Functional Description in D6.1 p.203-307) provided a functional description of the signatures and available methods for client calls. However, some parameter names used in these signatures are confusing and inconsistent in respect to the delivered WSDLs. An improvement at this level is requested for the next implementation iterations.

For the WP6 Orchestration layer, WP5 provides additional functions on demand and helps to fulfil and optimize client side orchestration. For instance, "*a watercourse description was stored in the platform as a meta-content which first content is a text content that stores the XML angler specific data*

[19] Please note that WP6 provides a detailed description of the WP6 orchestration layer with installation and configuration instructions in D6.1. The installation in Grenoble was remotely performed with the help of HPF.

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

structure. The other content of the meta-content can contain multimedia content to illustrate the watercourse”[20]

The as-is-state of the WP5 functional support from the WP6 perspective is reflected in D6.1 Appendix C (p.203-307, Community Application Prototype Functional Description) and D6.1 Appendix G (p.395-400, Releases and Change of the Community Application Prototype 1). Functionality as well as known limitations and issues of the PICOS application from WP6 perspective can be found in Chapter 3 of D6.1 (p.133-139).

4.3.3.4.2 WP5-WP6 functional support for requirements fulfilment from the client perspective

D5.1 and further distributed internal documentation provided good support to the WP6 developers. For instance, concrete code examples were made available for the developers showing how to use the client side RPC library. Another part included later as a part of D6.1 (see Community Application Prototype Functional Description in D6.1 p.203-307) provided a functional description of the signatures and available methods for client calls. However, some parameter names used in these signatures are confusing and inconsistent in respect to the delivered WSDLs. An improvement at this level is requested for the next implementation iterations.

For the WP6 Orchestration layer, WP5 provides additional functions on demand and helps to fulfil and optimize client side orchestration. For instance, “*a watercourse description was stored in the platform as a meta-content which first content is a text content that stores the XML angler specific data structure. The other content of the meta-content can contain multimedia content to illustrate the watercourse*”[21]

The as-is-state of the WP5 functional support from the WP6 perspective is reflected in D6.1 Appendix C (p.203-307, Community Application Prototype Functional Description) and D6.1 Appendix G (p.395-400, Releases and Change of the Community Application Prototype 1). Functionality as well as known limitations and issues of the PICOS application from WP6 perspective can be found in Chapter 3 of D6.1 (p.133-139).

4.3.3.5 Summary of findings and recommendations

In general, we can assess that D5.1 delivers a real implementation of the D4.1 generic PICOS architecture. The WP5 PICOS implementation fulfils all requirements related to location based services and communication functionalities from the WP6 perspective.

The approach to choose a sub-set of components from D4.1 is realistic to define the concrete architecture. However, some more architectural information of the integrated components and servers of the other partners are missed. This information should show how the integration of these components and servers was carried out as well as describe their inter-communication at the server side. Further, the storage of the data has to be extended to cover those components and servers, too.

Again, as we stated in the WP4 evaluation, some figures and notations are not self explaining and should be substituted by well known notations such as UML to avoid misunderstandings. The delivery process of the APIs (WSLDs, API description etc.) has to be optimised for the next implementation work.

[20] See p. 19 in D5.1

[21] See p. 19 in D5.1

Finally, in the case of reaching a mature WP5 implementation of the PICOS platform, we propose to distribute installation packages to all partners with corresponding instruction for deployment, upgrades, and security configuration.

4.4 Economic evaluation

4.4.1 Methodology used

For the economic evaluation of the WP 5 PICOS platform, the requirements derived from a trust and privacy oriented perspective are tested against the implemented functionalities and if applicable put into a current context. To keep a focus under the constraints of the scope of this evaluation this will not be a definitive analysis.

The aimed goal is to determine, how the PICOS platform copes with the economic aspects of the PICOS requirements. The discussion examines how well the platform meets economic aspects of the PICOS requirements.

4.4.2 Documentation used

This economic evaluation of the PICOS Platform has been drafted by comparing PICOS Deliverable D5.1 “Platform Prototype 1”, and the PICOS Deliverable D2.4 “Requirements”, based on the PICOS principles in the PICOS architecture (D4.1).

4.4.3 Evaluation of the requirements and functionalities of the Platform Prototype

In chapter 2.4.3 the economic evaluation of the PICOS architecture went along the identification of requirements with an economic relevance, the PICOS features satisfying these requirements and at last the PICOS Components as virtual constructs to reflect the PICOS architecture itself. For the evaluation of the PICOS Platform Prototype, the corresponding implemented platform components are reviewed in an economic context, respectively their business relevance under consideration of the trust (TrP)[22] and privacy principles (PrP)[23].

The platforms initial intention was to bring a set of capabilities around trust and privacy that could be used by any mobile community platform. In order to fully support the identified capabilities a significant adaption of the adopting community platform would be required, as most of these platforms do have a hard coded more or less rich policy management and do not support PICOS concepts, like multiple identities or a privacy advisor. Especially Policy management affects numerous different components and functionalities within a community platform. This issue is addressed by the PICOS platform design, which is designed to interwork with external services to interwork with external services through well documented APIs. From a business perspective, the key to convince existing platforms to change their behaviour, and to integrate trust and privacy principles elaborated by PICOS in their community services, is to make the concepts valuable to the providers. Value for the providers is generated, by meeting the privacy demands of the users, and at the same time preserve the economic potential through marketing and advertising activities, gaining a competitive advantage.

[22] D5.1 Platfrom Prototype 1, p 94 f

[23] D5.1 Platform Prototype 1, p. 96 f

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

In order to create such an added value, in particular a close interplay between the possible integration of 3rd party services and trust and privacy related concepts integrated in the PICOS platform is needed.

Therefore the PICOS platform prototype was built to demonstrate the capabilities around trust and privacy, providing components like the Privacy Advisor, the Policy Server, the Profile Server and the Community Server (content sharing). The PICOS Architecture Feature “External Services”, implemented in the PICOS Architecture Component “External Service Delivery”, forms the basis for any kind of integration of 3rd party services, such as marketing or advertising services in a social community. However, this feature is not implemented by the platform as a component. Hence no single economic requirement (R.A1-R.A5) from the PCIOS requirements Deliverable (D2.4) is addressed, and marketing and advertising as general requirement is considered within the first implementation of the PICOS platform.

The fourth Trust Principle (TrP 4) states that PICOS ensures that externally hosted services are delivered in a trustworthy way, and that members are aware when external services are less trustworthy than internal services. The PICOS platform prototype states that this trust principle is fulfilled. No external services have been integrated into the PICOS framework that implies interactions between the WP5 PICOS platform and external possibly unsecure servers. But from the economic point of view an integration of external services is inevitable, especially when applying the platform in commercial scenarios. Therefore, possible security layer models for the data used by these external services should be evaluated. Further, it is recommended that depending on the results of the second cycle of the PICOS architecture a commercial scenario could be implemented, e.g. the voucher gratification system from the PICOS Use Case 6.

By an exemplary implementation of an external service, the PICOS Platform could give a strong prove that adhering trust and privacy principles does not necessarily mean the erosion of business models in social communities. The implemented PICOS Platform Components already ensure the integrity of the PICOS Privacy Principles. In particular the following principles are relevant in regards to the integration of external services:

- PrP9 Limitation of Collection: Only personal information relevant to the identified purpose may be collected. This rule is implemented in the platform by restricting mandatory entries to the very minimum (minimum pseudonym needs to be given), thereby limiting the collection.
- PrP10 Fair and Lawful Means: Information must be collected by fair and lawful means. By the platform’s design principle all user data (such as profile, presence, location, except pseudonyms of partial IDs) are by default private. Giving the user the possibility to decide which data should be public for which partial ID, the user has the control about his personal data. Information is collected either during registration, partial identity creation or user profile modification using screen. None of the handset information is sent to the platform except the location information as soon as the end user has decides consciously to enable other users to see his location information by customizing the privacy rules. By giving the user control over the data collection, PICOS meets the fairness principle.
- PrP11 Acceptable Uses: Personal data may only be used for the purposes stated at the time of collection. As the user can create profiles that he can decide to share, data are also then collected for remote storage. It is up to the user to decide what to do with the data in certain contexts (e.g., push content and share it, share user profile, presence or location).
- PrP13 Third-Party Disclosure: Notice and consent of the Data Subject is required to disclose information to third parties. The PICOS architecture must uphold the member’s wishes with regard to information flow. The disclosure is managed by the end user via his privacy rules.

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

No user data is disclosed outside the community and within the community. The platform fully meets PrP13 at the current stage. This privacy principle has to be taken into account, when designing the integration of external services and a potential usage of data subjects of users.

- PrP14 Third Party Policy Requirements: Organisations must ensure that any third parties are informed of their privacy policies and will enforce them or possess equivalent policies. Again, the platform at the current stage supports no external service and is thereby fulfilling the principle. If an External Service is integrated the integrity of this Privacy Principles has to be preserved.

Possible example implementations for external services might be as followed:

- Implementation of an example payment service
- The voucher gratification for users earning reputation in a community, described in PICOS Use Case 6 (D6.1) and
- Context sensitive placement of advertisements

Besides the economic relevance of external services for the PICOS Architecture, other already implemented components are relevant, such as the PICOS Platform Component controlling the handling of personal information and data subjects is the Policy server.

By TrP 1, PICOS offers services that handle personal information in an open and transparent way. This trust principle has to be maintained even in a business scenario. The implemented community policies define how personal data is stored and made available to other users. By default, all data related to users is classified as private and cannot be accessed by any member of the community unless the user defines it public through privacy rules. Thus, partial sharing of data is enabled. Any modification of the privacy rules is logged for audit purposes. All data entered by the end user is made available for modifications. The platform allows the modification of the user profile, published content as well as contributions. Further, more dynamic information about the user, such as presence, can be configured by him. The reputation of a user is always public and cannot be disclosed respectively hidden explicitly by him.

With the implemented privacy policies, the user is able to handle his personal data in the PICOS Platform in an open and transparent way, with the exception of the reputation attribute. This is defined by third users of the platform, which is according to the reputation principle in real life communities. Privacy policies thereby play an important role when it comes to enabling 3rd parties to access user data subjects, e.g., for marketing or advertising activities. To sustain the integrity of users' privacy policies on his data subjects, the privacy of a user is respected through the platforms design. By this, customization of privacy rules attached to user attributes is enforced. As no data mining function is integrated into the platform and no external server is allowed to access user data, the integrity of the users defined privacy rules is ensured. This reflects Privacy Principle 3 (PrP3) - Changes in Policy or Data Use: Notice must be provided if and when any changes are made to the applicable privacy policies or in the event that the information collected is used for any reason other than the originally stated purpose.

If external services would be connected with the platform, the external service provider has to be kept responsible for providing changes on the usage other than the originally stated purpose. And if personal information is collected, the data subject must provide informed consent, unless a law or regulation specifically requires otherwise (PrP6).

The Policy Server managing the policy rules together with the Notification server allows the user to manage consent via the policy rules that can be modified via the client application. Policy rule modifications are logged using the event logging. The notifications are an essential part for meeting the informed consent, where nowadays the user acceptance for such notifications is low. An integrative way of displaying the notifications in the user's workflow might be the key to establish this awareness in information processing by end users.

Thereby with the current implementation of the Policy server and Notification server, the platform complies with this requirement.

Last but not least, a change of use consent might occur, if external services are implemented. PrP7 Change of Use Consent states, that consent must be acquired from the data subject to use personal information for purposes other than those originally stated at time of collection. In the evaluated version of the PICOS Platform, a change of use consent will not occur in the platform, as it strictly enforces default community policies (every user attribute is private) unless the end user changes the use consent. As long as external services will have no access to the user data this rule is fulfilled by the platform design. As soon as external services do have access on the user data, mechanisms have to be provided to ensure this privacy principle, which will prove to be a technical challenge.

A solution for this challenge lies within the profile management implemented in the PICOS Platform Component "Profile server", which was specified for this purpose. The component allows the user to manage his root identity and his partial identities, in regards to his personal attributes. To give the user the possibility to manage the usage of data by third parties, an explicit release of certain attributes for advertising or marketing activities on attribute level needs to be available to the user. Alternativly, creating special advertising profiles, possibly in the form of discrete partial Ids for which the user can define which information he wants to share for marketing and advertising activities with third parties, reduces the complexity for the user, but increases the effort for configuration. Summarizing, in todays social networks and mobile communities, the user has no transparency which of his personal data is used by marketers, neither is he provided with a tool to manage his personal data on the level of personal attributes. Therefore an implementation in PICOS set a new reference.

Another economic potential of the PICOS Platform and a social community based on it, lies within the content generated by the community. In a business case, advertisements could be placed in context to the shown content. Therefore, now the PICOS Platform Component "Community server", responsible for content sharing is evaluated in this economic context.

If such content sensitive advertisement functionality would be integrated into the PICOS Platform, first the notice of collection needs to be covered. This is part of the community's terms and conditions, which explain the global community policies related to data collection and data retention. They are displayed before the final registration of a user as the first screen before any data collection. This is a standard covered by the platform. Second, data subjects must be informed of and give their explicitly consent to the collection, use and disclosure of sensitive information (PrP5), such as medical or health conditions, sex life, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, unless a law or regulation specifically requires otherwise.

The platform's content sharing server in connection with the policy server will offer a way to share personal information, if the user accepts that sharing model. The user could change his privacy rules, e.g., making a permission request for his personal presence and location information necessary, if another user wants to see this information. Same applies for other data subjects. This gives the user transparency and control over his data subjects, which is currently not available at that granularity in commercial platforms.

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

As the consequences and relevance of revealing certain personal information is not always apparent to the user, the Privacy Advisor Component of the PICOS Platform might be a solution to sustain the privacy of a person notifying the user upon posting personal information in a content sharing context, or giving advice upon the granularity of release of his data subjects.

4.4.4 Summary of findings and recommendations

In summary, the PICOS platform implements a set of capabilities around trust and privacy, without disabling business applications for the PICOS Platform. In opposite, current community platforms do not support such privacy features as multiple identities and privacy advisor. Particularly the implemented Profile server and Policy server are of a special relevance when it comes to business applications under trust and privacy preserving conditions. To prove the capabilities of the PICOS Platform and its applicability in business applications, an external service should be implemented as a use case. Several suggestions have been made, e.g., the implementation of a payment service, the implementation of the PICOS Use Case 6, or content sensitive advertisements.

To enable content sensitive advertisements, the concept of the partial identities implemented in the Profile server component, can be used to let the user configure advertising profiles by him, or at least define the extent of usage of personal information in personalised advertisements. Furthermore, adaptations to the Community server component are necessary to show content relating advertisements.

At last, the platform provides strong privacy mechanisms to put users into control over their data subjects and to give them full transparency over the data usage. In correspondence with the economic evaluation of the PICOS Platform Design & Architecture, the key point is to validate how functionalities for marketers and external service providers can interface with PICOS platform while preserving the trust and privacy principles at the same time. ,

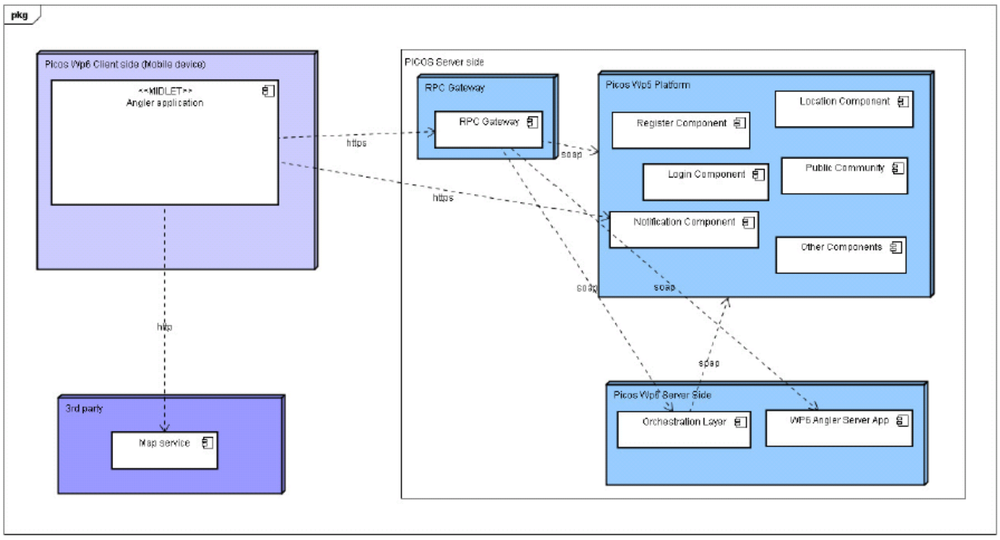
By that the PICOS Platform is able to take a role as a Intermediate in regards to sharing of personal data for marketing and advertising activities. It is capable via according matching, that on the one hand the privacy of the user is respected and his preferences are considered, while at the same time targeted advertising on basis of personal data of the user is possible. From the economic point of view, the platform by that is the basis for respecting and integrating the requirements of the user, 3rd parties and marketers. The goal for the second cycle should be to find an implementation solution for the adapted Architecture & Design of PICOS on these controversial aspects.

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

5 Evaluation of the Angling Community Prototype (WP6)

5.1 Summary presentation of the Angling Community Prototype

The PICOS Community Application Prototype 1 (as part of the PICOS open, privacy-respecting, trust-enabling identity management set of solutions that support the provision of community services) is, in essence, a mobile prototype which runs on a smart-phone touch-screen device (Nokia 5800 Xpress Music). It was developed using Java 2 Micro Edition (J2ME) and built on top of the services and communication infrastructure offered by the PICOS platform prototype 1. It also considered specific needs and expectations identified for the involved PICOS communities of anglers (i.e. by extending the core PICOS services provided by the platform with angler-specific functionalities, some of which are supported too on server-side like the Species Summary searches). The platform-centric, services-based overall architecture is depicted below in a high-level design diagram showing the integration model with the platform, which covers retrieval (including asynchronous notifications) and pushing of information between the server side and the client side:



The first PICOS Community Application Prototype (D6.1) is based on and provides a client side to the capabilities of the first PICOS platform. As fundamental input for its mission objectives and technical foundations, it has used the results from previous and on-going PICOS work, namely from work packages 2 (Requirements), 3 (Assurance of Technical Trust and Privacy Properties), 4 (Platform Architecture & Design), 5 (Platform Prototype Development). Additionally it has been oriented to produce the necessary input as required by work packages 7 (Community Prototype User Trials), 8 (Evaluation) and, again, 3 (in particular for the Trust and Privacy Assurance of the Community Prototype). It can thus be considered the culmination and practical realization of the concepts and principles laid out by the PICOS process in the first cycle of the project, as well as a major milestone required for such research and development results to be tested with real communities of PICOS technology users (private/leisure communities of anglers in this case) and comprehensively evaluated from complementary perspectives (assurance, technical, economic, usability and legal) in this deliverable. The outcome of this evaluation will be considered as a fundamental input (among others) for the evolution of the work of WP6 in the context of the second cycle of the PICOS project.

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

Well-documented and supported open standards and technologies are used extensively both in the implementation of the prototype and for the interfacing with the PICOS platform, as this will ensure several benefits, such as the reliability of the PICOS solutions and their future extensibility, reusability[24], interoperability and maintenance. Within this prototype, special attention was paid to the integration of basic features of privacy-enhancing identity management into a comprehensive trust-enabling, privacy-respecting community prototype, relying on the foundations of the first PICOS Platform prototype. During the realization of the application prototype, requirements on the PICOS Platform were refined, particularly with regard to the support for privacy enhancement based on PICOS technologies. In some cases, implementations of PICOS Principles are horizontal as they transversally affect the way many key operating modes of the PICOS community are offered and used; for example the identity management model based on multiple identities determines how PICOS services are consumed and how users in the community are perceived through any type of interaction. Key elements and targets of this approach are:

- - Providing a privacy-friendly community application with related functionalities on the mobile
- - Include community-specific features of special added value to users (i.e. allowing users to share and find angler information on fish, watercourses, fishing sites, catch reports, etc.) to ensure a realistic evaluation under real world scenarios (recreational fishing)
- - Support trust-building processes based on reputation and rating mechanisms
- - Offer users the ability to interact anytime, anyhow and anyplace
- - Multilateral security in a multi-party environment with advanced privacy and identity management options
- - Controlled access to private Sub-communities based on partial identity

The prototype focuses on features demonstrating the new approach of PICOS to identity management for meeting community user's needs for the enablement of trust by members of the community in other members of the community and in the service-provision infrastructure: the privacy of community member's personal information, the control by members of the information they share and the complexity / flexibility of overall service composition from component services. The implemented functionalities cover both basic core virtual community features (members and groups management, multiple forms of communications and content sharing, profiles, access control…), features specific to anglers (catch reports, watercourse advisor, species summary…) and PICOS-specific and distinguishing features (sub-communities, multiple identities, privacy advisor, reputation building based on content rating…). They can be short-listed as:

- Registration as a community member (includes creation of login credentials, root identity and first partial identity in a direct and easy manner) and access to the community (login)
- Multiple identities management (including profiles management)

[24] Re-usability has been a major design objective, considering the evolutionary approach of PICOS to facilitate future prototype work and assimilation of results by the research and ICT communities, trying to embed into the design trust and privacy principles which are core to the PICOS philosophy.

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

- Privacy rules management (for profiles, location and presence),
- Privacy advisor notifications
- Private room management (including diary entries/catch reports and content transfer)
- Contact management
- Sub-communities management (private and public, including forum, diary entries and files)
- Public community management (including public forums and public repository management)
- Asynchronous messages management
- Real-time communications (chat)
- Location based services:
    - Watercourse/ fishing spots management,
    - Locate myself,
    - Locate buddies in my area.
- Species summaries combined with catch reports
- Content rating and reputation management
- Revocation

The application prototype has been designed to be consistent with existing PICOS architecture and PICOS Platform and to cover as many of the PICOS requirements as possible, considering as a major goal to bring into the application the end-user perspective (facilitating access to PICOS technology to those new to privacy respecting communities) balanced with the intrinsic PICOS research and innovation goals. It provides to end-users an application context that allows to fully control and to minimise the collection of personal data on services side, maximizing privacy by means of a user-centric approach where users can keep track of rules established on their data (including profiles, location and presence). Being a collaborative environment, it has been an aim to give the user as much freedom as possible while selecting the most privacy-preserving default options.

The adequate balancing of multiple trade-offs has been a common and necessary procedural approach for the whole of task D6.1. for instance trying to achieve complementarity and a good compromise between two major drivers present in the PICOS project definition: research-driven and user community-driven goals (which becomes more relevant and challenging at the application prototype level, although the attempt to do so is necessarily largely oriented and determined by work in previous work packages).Together with the PICOS platform, the application follows many of the requirements in WP2 deliverables and of the architectural Principles and Features identified in D4.1. Naturally this was limited by the natural constraints of any software engineering process (following the iterative stepwise refinement cycles that lead from requirements to technical specifications, to design and finally to implementation, subsequently narrowing and clarifying the scope of the final software results).

The complexity of releasing a prototypical implementation (with the corresponding limitations),providing simultaneously an appropriate degree of usability, has centred most of the WP6 efforts, and has required extensive input from PICOS usability experts and end-user representatives in an iterative decomposition process (which has included validation with low fidelity prototypes), before actual implementation on the mobile device. It should be understood that the process lacked basic feedback of real user reaction to PICOS technical and conceptual propositions for the management of privacy, identity and trust in virtual communities. Therefore some of the implemented features are tentative in their nature in order to gather conclusions useful for a second phase comprising further end-user driven research and ultimately a set of more advanced and richer community application prototypes built on a second version of the PICOS platform.

5.2 *Legal evaluation*

5.2.1 Methodology used

This legal evaluation covers the first version of the PICOS Community Application Prototype for the Angling Community, as presented in PICOS Deliverable D6.1. In the field of European Union law, the Charter of Fundamental Rights of the European Union (hereinafter EU Charter) provides for the respect for private and family life (Art.7) and the protection of personal data (Art.8), while the Data Protection Directive (1995/46/EC) has been adopted to guarantee efficient data protection. The description of the specification and implementation work done in WP6 will be evaluated against the European Data Protection Directive (1995/46/EC)[25] and the privacy principles that have been identified in the legal evaluation of WP5.

The principles included in these Directives have been transposed as a set of requirements in Chapter 6 “Legal Requirements” of PICOS Deliverable D2.4 “Requirements”, a summary of which can be found in Appendix B (Summarisation of Legal Requirements). Furthermore, the general overview of the legal and regulatory framework (PICOS Deliverable D2.3 Contextual Framework, Ch.4) has been used as a source of this evaluation.

The main goal of this evaluation is to ensure compliance of the Application prototype with the European data protection legislation and the relevant applicable principles. It will ensure that the application prototype adheres to the legal principles and requirements detailed in prior PICOS Deliverables, mainly PICOS Deliverable D2.4 “Requirements”, and PICOS Deliverable D2.3 “Contextual Framework”. The Application prototype will moreover assess whether PICOS has correctly followed the “privacy by design model,” as noted in Ch.6 D4.1.

5.2.2 Documentation used

This evaluation has been drafted by considering PICOS Deliverable D6.1 “Community Application Prototype 1”, PICOS “Angler Mobile Application Prototype v1.0”, PICOS Deliverable D2.4 “Requirements”, PICOS Deliverable D2.3 Contextual Framework”, and the relevant legal framework relating to privacy and data protection, as referred to in the aforementioned documents.

5.2.3 Compliance with data protection principles

A dossier on the use of personal data in the first PICOS prototype has been provided for in Appendix F of PICOS Deliverable D6.1. This dossier details the general overview of the legal and regulatory framework on privacy and data protection which has also been extensively elaborated in PICOS

[25] Directive 2002/58/EC (ePrivacy Directive) and Directive 2006/24/EC (Data Retention Directive) are not directly applicable to PICOS as they only apply to “publicly available electronic communications services offered via a public electronic communications network”, which is not the case for the PICOS platform nor for the PICOS application prototypes.

Deliverable D2.3 Contextual Framework, Ch. 4. The legal principles on privacy and data protection contained in the aforementioned framework were translated into requirements in Chapter 6 "Legal Requirements" of PICOS Deliverable D2.4 "Requirements", however have also been transposed for the needs of the first PICOS prototype to specific obligations in Appendix C of PICOS Deliverable D6.1.

This section will evaluate the aforementioned principles and address the extent to which these principles and obligations have been implemented in the PICOS Community Application Prototype for the Angling Community, as presented in PICOS Deliverable D6.1. All the references to chapters and section refer to Deliverable D6.1.

a. Principle of Fair and Lawful Processing.

Principle: According to Article 6(a) of the Data Protection Directive, the first principle relates to the requirement of fair and lawful processing. In determining whether any processing of personal data is 'fair', particular regard must be paid to the method by which data were obtained.

Adherence: In the PICOS Application prototype, as per "PrP 1 Notice of collection" (Section 4.2.1, Chapter 5, D6.1), "Notice is provided to the data subject of the purpose for collecting personal information and the type of data collected." Without the confirmation of these terms and conditions, the user cannot register.

b. Legitimate Processing

Principle: According to Article 7 of the Data Protection Directive the application shall process personal data only based on a legitimate ground.

Adherence: In the PICOS Angling Community Prototype the processing of the personal data was based on the consent of the user. The users gave their consent by accepting the terms and conditions, which can be found in Appendix E of Deliverable D6.1. For the participation in the PICOS Angling Community Prototype lab tests and field tests the users also signed a user consent form, which can be found as Appendix I of Deliverable D7.1a "User Evaluation Plan".

c. Principle of Finality/Purpose Limitation

Principle: Data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes (Article 6(b) of the Data Protection Directive). This principle thus has two components: (1) the data controller must specifically inform the data subject of the purposes for which data has been collected; and (2) once data has been properly collected, it must not be used for further purposes incompatible with the original purposes. Article 7 Data Protection Directive sets out the criteria for making data processing legitimate, one of which is the unambiguous consent of the data subject.

Adherence: The PICOS Application Prototype, adheres to this principle with the inclusion of PrP 2 Policy Notification" (Section 4.2.2, Chapter 5, D6.1) where the data subject is notified of the applicable policies in terms of consent, access and disclosure. This displays the community terms and conditions which explain the global community policies related to data collection and data retention. The unambiguous consent of the data subject is collected.

Furthermore, in specific situations the Privacy Adviser requires the consent from the user (i.e. to expose to the public content that contains potentially sensitive information matching user profile attributes). This functionality is detailed in Section 2.2.12 of PICOS Deliverable D.6.1:

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

The Privacy Advisor (PA) is a special assistant embedded in the PICOS Platform whose role is to inform the End User of non-obvious possible consequences of his actions on trust (trust is potentially misplaced) and privacy (personal information is revealed).

d. Principle of Data Minimisation

Principle: Article 6(c) of the Data Protection Directive requires a data controller to hold only personal data that is “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”. It is therefore a legal obligation for the data controllers to store only a bare minimum of data for the purpose of running PICOS (data minimisation principle). Moreover, the design and technical devices of the data processing systems must be oriented towards collecting, processing and using either no personal data or as little as possible (‘data avoidance’)[26].

Adherence: This principle is embedded into section 7.1.9 and 7.1.12 of Deliverable D4.1 with PP8 (Data minimisation), supporting the concept of data minimisation (by only collecting data absolutely necessary for the provision of the service), and PP11 (detailing the “use of pseudonyms”) where members who wish to interact with other Members and services, can still do so whilst still being able to restrict how much identifying information is shared.

This functionality of data minimisation has been implemented in the Application Prototype of PICOS. As elaborated in Appendix F “Dossier on the user of personal data in the first PICOS Prototype” (D6.1):

“[…] only a login name, a password and a username (the first pseudonym) are mandatory for the registration and subsequent login process. For subsequent login, the user has just to provide his login name and password. He/she will then be able automatically to move around in the community with his username that was provided in the registration process. Anytime at a later stage the user may create an additional pseudonym that he/she may use for other purposes compared to the first username (first pseudonym). The user decides then in his further community life, which personal data shall be disclosed in relation to a certain pseudonym for what kind of purpose. Whenever the user is going to disclose data, he/she will be supported from a privacy advisor that dispatches an alert, specifically in a case where sensitive data shall be disclosed (e.g. disclosure of sex female/male).”

e. Principle of Data Quality

Principle: According to Article 6(d) of the Data Protection Directive, and as further elaborated in PICOS D2.3 section 6.2.1, this principle creates an obligation for the data controllers to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, are either erased or rectified.

Adherence: The PICOS Application Prototype adheres to this principle as a Policy Notification (as described in section 4.2.2 PrP 2 Policy Notification) which displays the community terms and conditions and that explains the global community policies relating to data collection and data retention is presented. The full privacy policy and terms and conditions, used for the data trials are presented in Appendix E of PICOS Deliverable D.6.1 “Community Application Prototype”.

Furthermore, the PICOS Application Prototype guarantees via the PICOS Angling Community Privacy Policy that “all personal data stored concerning yourself may be accessed directly via the

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

PICOS Angling Community Prototype”. Moreover, as per PrP17 “Correcting Information” (section 4.2.17), “those data [which] are accessible from the mobile device application when the user logs in … can be modified at any time during the session”. However, a caveat is made that states “some data which are entered into the profile (e.g. sex, age, zip-code, country) cannot be changed in an individual user’s partial identity profile but rather in the root identity profile. All other personal data entered by the users can be corrected directly by the owning users”.

f. Principle of Conservation

Principle: This principle, outlined in Article 6(e) of the Data Protection Directive, states that data should be destroyed or rendered anonymous when the specified purpose for which they were collected has been achieved.

Adherence: This principle has been translated into a specific feature in the PICOS Application Prototype, as evidenced in Section 4.2.12, where it is stated that “when a user account is deleted, the respective user is revoked and all user attributes and partial identities are deleted. The “MyAccount” Screen in the PICOS Community Application provides the necessarily functionality for this purpose (“Delete Account”).” It is stated that some limited information is retained for auditing purpose, however it is not clear whether this platform event logging is indeed required. It is nevertheless stated, that in regards to the Angling Community Prototype, all personal information shall be deleted at the end of the trials.

We reach the conclusion that the event logging that stores user pseudonyms, and which are capable of identifying the user should be purged upon an account deletion unless this storage of personal data is thoroughly explained and justified. This justification should include the necessary details as to why its storage is necessary in light of the circumstances.

g. Rights of the data subject: Right to information

Principle: In respect to the data subject’s right to information, before the processing of personal information, the data subject shall be given information at least regarding the identity of the data controller and the purposes of the processing for which the data are intended (Art. 10 Data Protection Directive). The information regarding the personal data that are being processed shall be given to the data subject in an intelligible way (Art 12(a) 2nd section Data Protection Directive).

Adherence: In the PICOS Application Prototype, this principle is adhered to via the information that is provided to the user of the service in the Terms and Conditions, as well as in the Privacy Policy, which as included in appendix E of Deliverable D6.1 “Community Application Prototype”. The data subject is indeed informed regarding the identity of the data controller (CURE), the purposes of the processing, the period during which the data will be kept etc in simple language and in an intelligible way.

h. Rights of the data subject: Right to object

Principle: The data subject has the right to object to the processing of his personal data (Art. 14 Data Protection Directive).

Adherence: The PICOS Angling Community Prototype enables the users to object to the processing of their personal data. This is realised in two ways: (a) the user can refuse to give his consent for the processing of his personal information. This is explained in Section 4.2.8 of D6.1 where it is stated that the “when a member requests to see the presence or location of a member this can be denied by the remote member and the requesting user will be notified accordingly"; (b) the user can modify the rules he has created via the Policy Manager (Policy Editor). As explained in Section 2.2.11.2 of D6.1, the user can revoke the permission (disallow) he has granted to other members to his profile, presence, location or contact list. In this way he is withdrawing his consent and is exercising his right to object to the processing of his personal data.

i. Rights of the data subject: Right of access

Principle: A basic right of the data subject is his right of access, i.e. his right to be informed about his personal data that are being processed (Art. 12(a) Data Protection Directive).

Adherence: As explained in Section 4.2.15 of D6.1, "only a minimal set of personal information is mandatory to be provided" for the PICOS Angling Community Prototype. Via the Private Room of the prototype (explained in Section 2.2.14 of D6.1), the user has an overview of his personal information that is stored or shared in the Prototype. The right of access can be exercised by the user to the data controller (CURE), as described in the PICOS Angling Community Privacy Policy, which explicitly guarantees to PICOS users that "All personal data stored concerning yourself may be accessed directly via the PICOS Angling Community Prototype installed on your mobile device and may be deleted or revoked or amended directly by you, the user. We do not reserve the right to refuse to provide you with a copy of your personal data" (Appendix E of D6.1). With regard to the user data collected and processed during the PICOS Angling Community Prototype lab tests and field tests the users were explicitly informed via the user consent form, which can be found as Appendix I of Deliverable D7.1a "User Evaluation Plan", that they "can have access to [their] personal data by contacting Ms Eva Ganglbauer at ganglbauer@cure.at, tel: +43.1.743 54 51.42 or fax: +43.1.743 54 51.30".

j. Rights of the data subject: Right to Rectify, Erase or Block

Principle: Of the rights of the data subject regarding the processing of his personal data is his right to rectify, erase or block his data (Art. 12(b) Data Protection Directive).

Adherence: The user can exercise his right to rectify, erase or block his personal data that are being processed and information he has entered to the community (into his profiles) via the mobile device applications, when the user logs in and at any time during the session. More specifically he can do this by modifying the rules he has created via the Policy Manager (Policy Editor). Moreover with regard to the user data collected and processed during the PICOS Angling Community Prototype lab tests and field tests the users were explicitly informed via the user consent form, which can be found as Appendix I of Deliverable D7.1a "User Evaluation Plan", that they can for the correction of [their] personal data "by contacting Ms Eva Ganglbauer at ganglbauer@cure.at, tel: +43.1.743 54 51.42 or fax: +43.1.743 54 51.30".

5.2.4 Location Based Service (LBS)

The ePrivacy Directive[27] aims to translate the data protection principles of the general Data Protection Directive into specific rules for the electronic communications sector. An extensive overview of the ePrivacy Directive has been provided for in PICOS Deliverable D2.3 "Contextual Framework", section 4.3. In this section, it has been explained that the ePrivacy Directive covers the providers of

[27] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), Official Journal L 201, pp. 37-47 (12.07.2002).

publicly available communications services or public communication networks. The PICOS Application Prototype does not come under this definition, however the telecom operator over which the PICOS Application Prototype is running over, does. Article 2(c) of the ePrivacy Directive states that location data means any data processed in an electronic communications network that indicates the geographic position of the terminal equipment of a user of a publicly available electronic communications service. The ePrivacy Directive does not make use of the term ‘Location Based Services’. In Article 2(g) of the Directive, however the term ‘value added service’ is defined as “any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof”. A conclusion is made in PICOS D2.3 that a Location Based Service (LBS) is a value added service which processes location data other than traffic data for purposes other than what is necessary for the transmission of a communication or the billing thereof. The PICOS platform and Application Providers do not fall under the obligations of the ePrivacy Directive. However, the legal evaluators decided to evaluate this specific functionality, as on the one hand the Mobile Operator that processes the location information falls under the scope of application of the ePrivacy Directive and on the other hand the protection of location data in the most privacy-enhancing way serves as an added value of the PICOS Angling Community Prototype.

In the PICOS Application Prototype, location data are turned off by default. As it is stated in the privacy policy of the Application Prototype (Appendix E, D6.1) “full location data may be accessed from your mobile handset, and sent to the PICOS platform however by default this functionality is turned OFF. **By turning ON the switch you consent to your location data being disclosed.** This functionality must be also be enabled in the general location policy and must be expressly “allowed” in order for the location data to be sent to the selected sub communities, a contact or to the whole public community. You, the user, are also able to specify the level of blurring in the partial identity (1 km, 5 km, no blurring), which is a global setting and effects all your identities.” The PICOS Application Prototype therefore ultimately assigns the choice to the *user* to consent to this feature being turned on, and to specify the level of ‘blurring’.

5.2.5 Summary of findings and recommendations

The PICOS Angling Community Application Prototype implements the data protection principles, ensuring a legally compliant application that respects the privacy of its users. Regarding the rights of the data subject the PICOS Angling Community Prototype makes use of the functionalities offered by the PICOS Platform regarding the creation of privacy rules. The provision of detailed information to the users that was realised via the PICOS Angling Community Terms & Conditions, the PICOS Angling Community Privacy Policy and the Consent form that was signed by the participants in the lab and fields tests and in the field tests ensures the maximum protection of the users and the adherence to the relevant data protection legislation.

5.3 Technical evaluation

5.3.1 Trust, Privacy & other technical elements

5.3.1.1 Methodology used

In this section we focus on issues concerning the trust and privacy principles established in D4.1, and present an evaluation of the community prototype (D6.1) with regard to those principles.

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

5.3.1.2 Documentation used

The main source of documentation for this part of evaluation is D6.1

5.3.1.3 Evaluation of the requirements and functionalities of the Angling Community Prototype

The Community Prototype provides a mobile interface for the platform services to the anglers. Its functionality is largely based on the functionality provided by the platform, on which it depends. As a result, if the platform prototype does not support a given functionally or enforce a given principle, it is hard or impossible for the community prototype to do it. In this sense, the underlying functionality related to *Public Community, Policies, Partial identities, Private Rooms, Profiles, Privacy Advisor, Presence, Reputation*, and *Location,* does not differ from the functionality provided by the platform prototype.

The main task of the community prototype is to present to the end user an interface to the functionality provided by the platform that respects the established trust and privacy principles.

In the first cycle, WP6 focused mainly on providing a more robust *Registration* process, improving the *Location Based Services* within the bounds of functionality provided by the platform, and integrating the FishBase via the *Species Summary*. Hence, in this section we focus on these three functionalities, evaluating their implementation in community prototype with regard to the trust and privacy principles.

Registration

The main difference with respect to the platform functionality can be found in the registration process, in which the community prototype adds an orchestration layer to the services provided by the platform. This adds also to the complexity of the community prototype with regard to the platform. For example, the privacy principles *Timing of notification* and *Informed Consent*, defined in D4.1, demand that the user should accept the policies before filling out the required data. The platform provides a pair of methods allowing the Client Application (CA) to retrieve the general policies of the community that are to be displayed and accepted, but when and how these methods are called, and when the policies are displayed (if at all) to user, is not specified in the platform prototype. The community prototype answers those questions in [D6.1 2.2.6] by describing a sequence of events that can be summarized as follows:

User presses the “register here” link in the LoginScreen presented by the CA

User accepts the terms and conditions (provided by Platform, according to the description).

CA displays the registration main screen to User

User fills the registration form (username, password, first partial identity)

Profile screen is displayed by CA

User fills the profile form (with non-compulsory data such as hobbies, data location, personal data and others).

CA sends the register request to Platform

Platform sends register response

In this sequence of actions we see that the display of terms and conditions takes place in step 2, before the display of the Registration screen, which should be considered, from the privacy standpoint, the correct order of events.

Apart from the registration process, the community platform also enriches other basic processes offered by the platform, in particular the location base services: fishing spots and watercourses; and the privacy rules editor.

The communication between the CA, which is part of the community prototype, and the server, which is part of the platform prototype, makes use of the SSL protocol in order to ensure confidentiality of the data exchanged between the user and the platform. However, no client authentication mechanisms are provided, which may allow a malicious and illegitimate CA to compromise the security of the system. This is solved in the first prototype by limiting access to the platform only to the devices used during the trials.

Location Based Services

With regard to the location based services, the community prototype had to solve some open issues. The main one was the fact that the location based services, and particularly the sharing of location and presence information with other members, might be used for linking the partial identities of a given member. In order to prevent it, the different partial identities of a user are allowed to be associated to different presence and location status. Otherwise, in case that only the active partial identity is shown to be online, when a user switches from one partial identity to another other members might be able to observe how the old active partial identity shifts to offline at the same time that the new active partial identity shifts to online. By showing the status of the partial identity as “online” for some random amount of time after going offline, this kind of linkability can be avoided. We consider this problem as partially solved in this way, although other solutions might be able to provide a higher level of privacy.

Location information included in the partial identity profile might enable the association of the different partial identities of a member, because it can be requested even when the user is not logged in or the partial identity is not active. This is only true if the user decides to share this part of the profile for more than one of the related partial identities. The user should be made aware of this issue, e.g. by the privacy advisor, when he or she wants to disclose the location information in the profile.

Another issue is related with the feature of showing contacts in a map. When two different partial identities belonging to the same member are in the contacts list of another member, the latter might see both partial identities in the same location and link both partial identities. In order to prevent it, all the partial identities of one and the same member are shown with the same coordinates, one over other. In this way, only one of them may be actually seen. Unlinkability is thus enforced. However, this solution is not an ideal one, since the partial identity concept is thereby partially compromised. Also, the member might notice that some of his contacts are missing, and thus deduce that it is linked to one of the shown partial identities.

Privacy Rules

The privacy rules can be managed by the users themselves with the aid of the policy manager. The latter provides a very intuitive interface for the creation of privacy rules that control access to the data associated to the members of the community.

In particular, both presence information and location data can be protected, using the same privacy rules associated with the profiles, by using the Policy Manager or the Policy Creator. The parameters for defining the privacy rules are:

- "*Scope of the Privacy Rule*", where the user has to select one or more partial IDs that will be the owner of the rule.
- "*Type of the Privacy Rule*", where the user can select the type of the rule to either Presence, Location, or Profile.
- "*Privacy Rule affects…*", where the user selects which members (in fact only partial identities can be selected) will be affected by the rule.
- "*Privacy rule for*" section, where the user finally selects which resource will be open for public view; the user may select "*Yes*" or "*Not*" in order to allow the affected partial identities to see the resource, or "*Ask Once*" and "*Ask Always*" if the user wants to be prompted before allowing someone else to see the resource.

Privacy rules can be edited in only one screen, which makes it easier to define them.

Species Summary

The Species Summary functionality allows the user to search for qualified information about a specific fish species. The information background comes from FishBase (www.fishbase.org). There are several options to search for a specific species: search with the common name, search with genus and species name, or search with only the genus.

The species summary can be seen as an external service, although it is hosted at the same location where the platform is hosted. It is important to highlight the fact that the services provided by the species summary do not require or collect any information from the members that use them, and thus can be considered to respect the established trust and privacy principles.

5.3.1.4 Summary of findings and recommendations

The main findings of the evaluation of the community platform are related to the impact of the trust and privacy requirements on the usability of the application. The community prototype tries to accommodate the services offered by the platform to the trust and privacy need of the end users. Unfortunately, the user is not able to find the mechanisms for enforcing trust and privacy intuitively. PICOS should focus either on giving some information to the final users about the trust and privacy features of the community prototype before the actual trial, or on refining the user interface according the members' wishes. The community prototype leaves some issues open that have to be solved in the second version:

- Most of the trust and privacy principles are currently enforced by the PICOS Angling community prototype.
- The PICOS Angling community prototype needs to provide other authentication mechanisms apart from user/password, such as Certificates or Federated access (OpenID), although this heavily depends on the functionality provided by the platform.
- In order to provide more friendly Location Based Services, enhancements may have to be done at the platform level.

5.3.2 Community focus

The focus of this part of the technical evaluation is on the implementation of the PICOS community prototype, especially the components which have a community focus. Again because of the intention of PICOS, principally every requirement, principle and component of the architecture has a "community-focus". The sub-community key features were already identified in chapter 3.3.2 Community focus of the Evaluation of the Platform Design & Architecture and were evaluated against the platform components (D5.1) in chapter 4.3.2. The identified platform components are now evaluated against the implemented community prototype (D6.1).

5.3.2.1 Methodology used

The goal of this evaluation is to provide information about how far the implemented community prototype, as described in D6.1, is able to make use of the platform components in D5.1.

In chapter 3.3.2 (Community focus) six features, eleven components and seven use case from D4.1 have been identified which are directly related to the community focus. In chapter 4.3.2 (Community focus) 17 components have been identified from D5.1 which realised it. These components are now evaluated against D6.1 and the implemented community prototype.

From this bottom-up point of view it will be evaluated if all components have been realized in a way to meet the PICOS specific approach.

5.3.2.2 Documentation used

The documentation used for this evaluation are the Deliverables D5.1 "WP5 PICOS Platform Description" and D6.1 "Community Application Prototype 1". D5.1 addresses the implementation of the platform design and architecture, D6.1 presents the first version of the PICOS Community Application Prototype for the Angling Community.

5.3.2.3 Installation – Functionality & Operation

Not applicable because the Anglers application is an integrated application, which cannot be installed modularly.

5.3.2.4 Evaluation of the requirements and functionalities of the Angling Community Prototype

For the evaluation of the requirements and functionalities of the Community Prototype, the sub-community related platform components were identified and have to be approved against the implemented community prototype.

The platform components which have been identified from D5.1 are:

2.5.1. Registration server

2.5.2. Login server

2.5.3 Authentication server

2.5.6 Public community server

2.5.7 Partial Id server

2.5.8 Presence server

2.5.9 Location server

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

2.5.10 Policy server

2.5.11 Sub-community server

2.5.12 Reputation server

2.5.13 Privacy Advisor server

2.5.14 Private room server

2.5.15. Contact server

2.5.16 Real time content sharing server

2.5.17 Profile server

2.5.18 Notification server

2.5.19 Logging server

The following table shows, how the community prototype uses platform components:

D 5.1 Platform Component	D 6.1 Community Prototype Design	D 6.1 Community Prototype Use Case	D 6.1 Community Prototype Functional Description
2.5.1. Registration server	2.2.6 Registration,	B.2 PUC 1: Registration	C.3 Access to the Community
2.5.2. Login server	2.2.7 Access to the Community	B.2 PUC 2: Access to the Community	C.3 Access to the Community
2.5.3 Authentication server	2.2.6 Registration, 2.2.7 Access to the Community and 2.2.17 Revocation	B.2 PUC 1:Registration, B.2 PUC 2: Access to the Community and B.2 Revocation	C.3 Revocation and C.3 Access to the Community
2.5.6 Public community server	2.2.13 Public Community, 2.2.17 Revocation, 2.2.5 Content Sharing, 2.2.6, Registration, 2.2.7 Access to the Community, 2.2.15 Sub-communities and 2.2.4 Fishing Spot / Watercourse Location Use Cases,	B.2 PUC 1:Revocation, B.2 PUC 7: Content Sharing, B.2 PUC 2: Access to the Community and B.2 PUC 9: Sub-community	C.3 Revocation, C.3 Access to the Community and C.3 Sub-communities,
2.5.7 Partial Id server	2.2.8 Partial Identities Management, 2.2.6 Registration, 2.2.7 Access to the Community, 2.2.17 Revocation and 2.2.15 Sub-	B.2 PUC 4: Multiple Partial Identities, B.2 PUC 1:Registration, B.2 PUC 2: Access to the	C3 Access to the Community, C.3 Revocation and C.3 Sub-communities

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

	communities	Community, B.2 PUC 3: Revocation and B.2 PUC 9: Sub-community	
2.5.8 Presence server	2.2.6 Registration, 2.2.7 Access to the Community, 2.2.17 Revocation and 2.2.8 Partial Identities Management,	B.2 PUC 1:Registration, B.2 PUC 2: Access to the Community, B.2 PUC 3: Revocation and B.2 PUC 4: Multiple Partial Identities	C3 Access to the Community and C.3 Revocation
2.5.9 Location server	2.2.6 Registration, 2.2.17 Revocation and 2.2.8 Partial Identities Management	B.2 PUC 1: Registration and B.2 PUC 3: Revocation	C.3 Access to the Community and C.3 Revocation
2.5.10 Policy server	2.2.11 Policy Manager 2.2.6 Registration, 2.2.17 Revocation, 2.2.5 Content Sharing, 2.2.15 Sub-communities and 2.2.8 Partial Identities Management	B.2 PUC 1: Registration, B.2 Revocation, B.2 PUC 7: Content Sharing, B.2 PUC 9: Sub-community and B.2 PUC 4: Multiple Partial Identities	C.3 Access to the Community, C.3 Revocation and C.3 Sub-communities
2.5.11 Sub-community server	2.2.15 Sub-communities , 2.2.17 Revocation and 2.2.5 Content Sharing	B.2 PUC 9: Sub-community, B.2 PUC 3:Revocation, and B.2 PUC 7: Content Sharing	C.3 Sub-communities and C.3 Revocation
2.5.12 Reputation server	2.2.4 Fishing Spot / Watercourse Location Use Cases, 2.2.13 Public Community, 2.2.15 Sub-communities, 2.2.5 Content Sharing, 2.2.6 Registration and 2.2.17 Revocation,	B2 PUC 7 Content Sharing, B2 PUC 10 Sub-community, B.2 PUC 1: Registration, B.2 PUC3: Revocation and B.2 PUC 4: Multiple Partial Identities	C.3 Revocation, C.3 Sub-communities
2.5.13 Privacy Advisor server	2.2.12 Privacy Advisor and 2.2.5 Content Sharing	B.2 PUC 7: Content Sharing	
2.5.14 Private room server	2.2.14 Private Room, 2.2.6 Registration, 2.2.17 Revocation and 2.2.8 Partial Identities Management	B.2 PUC 1: Registration and B.2 PUC 3: Revocation	C.3 Private Room and C.3 Revocation

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

2.5.15. Contact server	2.2.10 Contacts Management, 2.2.6 Registration, 2.2.7 Access to the Community and 2.2.17 Revocation,	B.2 PUC 1:Registration, B.2 PUC 2: Access to the Community and B.2 Revocation	C3 Access to the Community and C.3 Revocation
2.5.16 Real time content sharing server	2.2.5 Content Sharing	B.2 PUC 7: Content Sharing	
2.5.17 Profile server	2.2.6 Registration, 2.2.5 Content Sharing and 2.2.8 Partial Identities Management,	B.2 PUC 1: Registration, B.2 PUC 4: Multiple Partial Identities and B.2 PUC 7: Content Sharing	C.3 Access to the Community
2.5.18 Notification server	2.2.7 Access to the Community, 2.2.5 Content Sharing 2.2.15 Sub-communities	B.2 PUC 2: Access to the Community, B.2 PUC 7: Content Sharing and B.2 PUC 9: Sub-community	C.3 Access to the Community and C.3 Sub-communities
2.5.19 Logging server	Logging automatically by the platform		

5.3.2.5 Summary of findings and recommendations

For the technical evaluation of the community aspects of the community prototype the related platform components were reviewed against the results of community prototype (D6.1). The community prototype makes use of all evaluated platform components identified in D5.1. There are no platform components which are not used by the client application and there are no additional components realized in the client application. This is because the community prototype is dependent from the platform components and additionally implemented features cannot be used if they are not present on the server side.

5.3.3 Location based services and communication features

5.3.3.1 Methodology used

Similar to the WP5 evaluation, our methodology is based on a verification, that:

- the outcome of WP6 (the angler client application, that maps the outcomes of WP4 into a real client side implementation) interacts with WP5 and provides the required end user community features
- the WP6 prototype description (in the deliverable D6.1) corresponds to the **as-is state** of the WP6 (Angler) “Community Application Prototype 1” implementation, installation, as well as its usage in combination with the WP5 PICOS platform for fulfilling the user requirements and needs for the first prototype, and

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

- D6.1 provides essential information for developers (i.e. architectural hints, used technologies and development tools etc.) that are needed for further extensions or porting of the first prototype in next implementation work (i.e. Angler Gamer Community Prototype).

5.3.3.2 Documentation used

For the technical evaluation of the WP6 Platform related to the consideration of LBS and communication functionalities, we used mainly the deliverable D6.1 (Community Application Prototype 1), which role was to map the client side functionality for the end users requirements and needs of D4.1 (Platform Architecture and Design) and to implement a first prototype with consideration of D5.1 first concrete PICOS architecture (Implementation description of PICOS architecture components in the first platform prototype). Thus, partially reconsidering the deliverables D4.1 and D5.1 was substantial.

5.3.3.3 Installation, Deployment – Usage & Functionality

5.3.3.3.1Installation and Deployment

In general, WP6 provided detailed installation info for all stakeholders. This info considered different perspectives, namely, the developers as well as the testers and real users' perspectives. Because of this, the installation of the client was supported through different over-the-air (OTA) servers. For the developers and a restricted group of testers, an internal OTA server was used to release internal client installation packages. Internal releases are frequently needed, more than major test releases used by a wide range of testers (i.e. lab trials) and/or users (i.e. user trials). Therefore, major releases were made available through another OTA server in order to provide a good separation of these concerns. The release process was managed by TMO, which reacted promptly to the partners' requests. In addition to OTA installations, developers had the possibility to generate such installation packages each time from the common subversion (SVN) code repository[28] with the help of their own IDEs and to deploy them locally from their development machines. Furthermore, a detailed installation for OTA and the used IDE was distributed to other partners and made accessible for the WP6 stakeholders on the WIKI of the development collaboration tool TRAC, which is also used for instance for tracking opened tickets related to development issues or bugs. D6.1 reflects such information in various places for both, client device (p.139-141) as well as WP6 orchestration layer (p.39-41).

Concerning the AnglersBase used as part of LBS scenarios (i.e. fishing spots, watercourses), which is a part of the WP6 server side, and was made accessible through the WP5 RPC Gateway, we missed a description of the deployment procedure. While it was suggested that WP5 would have to generally describe the integration aspects of the AnglersBase, we expect in D6.2 a delivery of installation details to it. Another complementary aspect is the delivery of Release Notes for the first (Angler) Community Application Prototype, used in the lab and field tests. This is addressed in the following subsection.

5.3.3.3.2Usage

D6.1 describes in detail the features and limitations of the 1st Community Application Prototype in the Release Notes (s. Chapter 3 p.133-139). The release notes belong to the Community Application Prototype version 1.4 used in the lab and user trials that took place on the 27th/28th November 2009 in Vienna and 12th/13th December 2009 in Kiel. Furthermore, WP6 provides detailed changes history for all released versions (p.395-400). In addition to this, D6.1 describes with the help of Low Fidelity Community Application Prototypes the expected user interface (p.308-317).

[28] D6.1 p.416

5.3.3.3.3Functionality Overview

The functionality of the (Angler) Community Application (1st prototype) is described across D6.1 from different perspectives. The user perspective is reflected in the Release Notes addressed previously. The pure functional perspective can be found in the Appendix C of D6.1 (p.201-307) while the developers' perspective is reflected in Chapter 2 (p.29-129). The functionality from the WP5/WP6 perspective is spread over Appendix C (detailed description of the WP5 API, i.e. signatures and parameters etc.) and Appendix B (Preliminary Analysis of Input to D6.1). The Low Fidelity Community Application Prototypes cited above reflect the functionality from the usability perspective (p.308-317). The functionality from the testers' perspective is described in Appendix G (p.367-394). Related to the AnglersBase, the description of the functionality can be found on p.110-111 (Species Summary), p.118 (Angler specific services), and p.116-132 (Angler-specific Services Species, summary functionalities). For accuracy and space reasons, we address these functional aspects in details in the next section primarily for LBS and communication functionalities. Because LBS and Communication Features rely on various PICOS functionalities (i.e. those related contact, (sub)communities, reputation etc.), we address these functional aspects in details in the next section for WP6 in general and not only for LBS and communication functionalities.

5.3.3.4 Evaluation of the requirements and functionalities of the Angling Community Prototype

5.3.3.4.1Requirements mapping

Since D4.1 followed a user-centred and scenario-based proceeding for eliciting the requirements from D2.4 (i.e. user stories), D6.1 added the used Angler Story (p.155-164) and explained the relationship between the story and the prototype. Mapping the requirements from WP4 (described in D4.1) into WP6 (D6.1) is explained informally in Appendix B (p.166-200). However, no explicit requirements mapping from D4.1 is given (expect in the description of PUC 5: Reputation on p.174). There, PICOS use cases (PUCs) are addressed again from the WP6 perspective while the consideration of WP5 is more taken into account in Appendix C (p.201-291). For this, preliminary use cases were derived for the client application. Similar to WP5, the WP6 partners described this use cases textually and by using prototyping techniques (i.e. for the expected interface). Those prototypes helped later in compiling a common view of all the partners in respect to the expected user interface and related functionality (s. Low Level Prototypes in Appendix D on p.308-317 using homogenous UI prototypes). The description quality and used notations are very heterogeneous along the text of these Appendixes, which is surely due to the chronological progress besides WP6. By reviewing Chapter 2 for instance, the reader might note, that the used concepts and techniques (e.g. real screen shots from the prototype, UML as common notation etc.) are homogonous. Adding such chronological information will help external reviewers in understanding this.

We noted a discrepancy at the level detail of described UML diagrams in Chapter 2. Besides WP6, improvement at the level of the kind UML diagrams to be used and delivered as well as their detail level have to be reached (e.g. some partners provided more than others and in different level of detail). It is preferable to agree on this before the beginning of the next implementation work. This is surely easier now due to the common understanding of all partners reached through the successful collaboration in the development of the first prototype.

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

5.3.3.4.2 Requirements fulfilment and developer information for future extensions

In contrast to WP5 of which the license situation has to be clarified (i.e. if the WP5 Platform will be available after the end of PICOS or not), the Community Application Prototype WP6 client has to be seen as a candidate PICOS outcome for (re-)distribution in this respect. This is reflected in Appendix H, especially by the choice of the open-source implementation technologies (such as J2ME s. p. 402-413) and the selection criteria for the mobile device (s. Appendix H p.401-413), which matches the PICOS needs (p. 409).

Concerning the fulfilment of the agreed requirements for the first prototype, we conducted intensive internal functional tests at different levels. At the development level, our development methodology is test-driven. Therefore, we developed our client side classes, so that they can be used with the WP5 Platform or with local Mock Up test classes (local test classes e.g. used for the simulation of the components being developed by other partners). This allowed us to check the fulfilment for our requirements from the beginning in those test classes while the WP5 platform was in development and/or not available. After the integration of the WP5 platform, we conducted functional tests by using mobile devices with the installed prototypes. For the LBS scenarios and communication requirements, such tests are described in Appendix G (Inbox and Chat p.367-370 and LBS p.370-376) for the 1st Community Prototype. Finally, we conducted internal peer code reviews to assure the quality of the delivered code. Such proceeding helps in detecting hidden failures or errors (i.e. at the architectural level) which can arise and could not be easily covered by functional tests.

Chapter 2 includes all relevant information for future extensions to any developer interested in extending our code[29].WP6 followed a state-of-the-art design and implementation at the level of used technologies at the client as well as WP6 orchestration side. In our opinion, we met so the agreed requirements for the LBS scenarios and communication functionality for the first PICOS prototype.

5.3.3.5 Summary of findings and recommendations

In general, we can assess that D6.1 delivered a real implementation of the client side which interacts with WP5 together and fulfils (in our opinion) the functionality required for the 1st Community prototype. According to our various internal tests, the functionality for LBS scenarios and communication functionalities are fulfilled from the WP6 perspective. Like in WP5, the approach to agree on a sub-set of requirements from D4.1 is realistic in order to focus on studying privacy and trust research topics in PICOS. An explicit mapping from selected requirements remains open for all work packages we evaluated in this document (WP4, WP5, and WP6). The document is well structured and described. It used state-of-the-art technologies and provided deep hints and information for any future extensions. The next implementation iteration will profit from this especially because it foresees the provision of two prototypes (Angler as well as Gamer Community Prototype).

The good quality of the document could be surely increased if the WP6 partners agree on the detail level of the used UML diagrams, their kind, and their detail level. The latter will not be difficult when considering the fruitful cooperation that took place by implementing the mobile client application among all partners.

Providing information related to installation and user guides using real device screen shots in WP6/WP7 as well as providing detailed information to the installation/deployment of the AnglersBase will conclude D6.1. Also beneficial is the provision of more information for the integration of the

[29] Please note that also here, the release or licensing of the WP6 code has to be clarified.

Privacy Advisor integration in WP5 and its usage possibilities in WP6 will help in studying new privacy-enhancing and privacy-preserving solutions.

5.4 Economic evaluation

5.4.1 Methodology used

The following economic evaluation puts the PICOS Community Application Prototype 1 for the Angling Community in the context of business aspects of trust, IdM and privacy, as the collection, processing and exchange of information are key economical success factors for online and mobile communities. To keep a focus on the constraints of the scope of this evaluation this will not be a definitive analysis.

The aimed goal is to determine, how the PICOS Community Application Prototype 1 for the Angling Community copes with the economic aspects of the PICOS Requirements and with the economic view expressed in the PICOS Contextual Framework. The economic discussion and examination how well the Application Prototype meets economic aspects of the PICOS Requirements and how the way it picks them up results in a much clearer understanding of the requirements.

5.4.2 Documentation used

This evaluation has been drafted by considering PICOS Deliverable D6.1 “Community Application Prototype 1”, PICOS Contextual Framework (D2.3) and D2.4 “Requirements”, based on the PICOS principles in the PICOS architecture (D4.1).

5.4.3 Evaluation of the requirements and functionalities of the Angling Community Prototype

Corresponding to the PICOS platform prototype evaluation, the PICOS Angling Community Prototype is reviewed along its implemented components in an economic context, respectively their business relevance under protection of the trust (TrP)[30] and privacy principles (PrP)[31].

The Angling Community Prototype focuses on the end-user perspective for the realisation of requirements of the Angling Community in order to validate the acceptability of the concepts and approach chosen by PICOS. The focus lies on mobility aspects for a leisure community of anglers picking up the broader issues of privacy and trust in virtual communities by realising a framework of multiple identities management for users to build rich relationships and interactions. Due to this objectives, no business application processes like, for example, the voucher example described in the PICOS Use Case 6 were implemented in this first Angling Community Prototype. Therefore, no business related external services are available in the first version of the Angling Community Prototype. If external services are part of the 2nd Cycle, the following privacy principles will have to be taken into account for the Angler Prototype:

- PrP9 Limitation of Collection: Only personal information relevant to the identified purpose may be collected. The Angling Community Prototype achieves this Privacy Principle by a minimum of mandatory fields that need to be filled in for a partial identity. Therefore only information a user is willing to share is available to External Services.

[30] D5.1 Platfrom Prototype 1, p 94 f

[31] D5.1 Platform Prototype 1, p. 96 f

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

- PrP11 Acceptable Uses: Personal data may only be used for the purposes stated at the time of collection. The application allows the user to set the rules and conditions which data are shared with whom in the community, including customised order level of detail (e.g., for location). This has also to apply to a future implementation of External Services. The treatment of an External Service like another community user, which needs authorization by the user himself, might be a solution.

- PrP13 Third-Party Disclosure: Notice and consent of the Data Subject is required to disclose information to third parties. The PICOS architecture must uphold the member's wishes with regard to information flows. Disclosure is managed by the user via the privacy rules. Data will not be distributed to third parties without the explicit consent of the user.

- PrP14 Third Party Policy Requirements: Organisations must ensure that any third parties are informed of their privacy policies and will follow them or possess equivalent policies. If personalised services will be supported in the application prototype a consistent process through notification and policy management must be established to sustain the privacy of the user.

Possible example implementations for external services for the second version of the platform prototype as well as the Angling Community Prototype version 2 might be as followed:

- Implementation of an example Payment Service,

- The Voucher gratification for users earning reputation in a community, described in PICOS USE CASE 6 (D6.1), and

- Context sensitive placement of advertisements.

The integration of a business process into the PICOS Prototypes could be a way to show the applicability of PICOS concepts in the context of commercial community services (e.g., advertising).

With the retrieval of information from FishBase (an external database on species summaries), the PICOS Prototypes implemented an example how the integration of external data into the platform and client could look like. The interfaces to Fishbase can be considered as an external link to information and data which were not produced primarily from community members. The Angling Community Prototype at its present status only provides indirect access to external services from quality checked sites (such as FishBase). However these information are retrieved from FishBase (and updated frequently), adapted to the use in the mobile environment and subsequently hosted on a server which is owned by the PICOS consortium. The client applications access the information from there and thus, the trust into such information is at the same level as any other internal service.

The implementation of this Service gives a good example of how PICOS is able to provide added value to the community members by integrating external data, and preserving trust and privacy principles at the same time. Nevertheless, the PICOS Angling Community prototype lacks the implementation of External Services, which are the basis for any kind of integration of 3rd party services, such as marketing or advertising services. By that no single economic requirement (R.A1-R.A5) from the PICOS requirements Deliverable (D2.4) is addressed, and marketing and advertising as general requirement is not implemented. For the 2nd Cycle a integration of Point of Interest via a location based service for the gaming or the angler client should be investigated.

With regards to Trust Principles, WP6 states in the deliverable D6.1, that the fourth Trust Principles (TrP 4), should be part of the platform prototype. TrP4 states that PICOS ensures that externally hosted services are delivered in a trustworthy way and that members are aware when external services are less trustworthy than internal services. Nevertheless the integration of the FishBase database,

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

shows that the client prototype is playing an important role when it comes to consistent trust and privacy concepts in the client server architecture.

Another aspect of the client prototype with economic potential is content sharing, including asynchronous messages. The client prototype enables the Privacy Principle of correcting information (PrP17): Data Subjects are able to update or correct personal information held by the organisation. The user has the possibility to change data subjects via the graphical user interface of the client. The integration of content sensitive advertisements or the voucher gratification concept described in the PICOS Use Case 6 would plug on the content sharing service, respectively the reputation service. The integrity of the users' privacy in such a scenario could be sustained by the policy manager and notification server of the platform prototype.

One special aspect in the context of content sharing is that some data subjects can only be changed in the root identity (e.g., gender, age). A change in the root ID also implies a change in the partial IDs, if the attributes are released. Such a change in attributes of the identity might lead to a certain level of linkability as the change in several partial IDs is visible to other users or the external service provider.

The PICOS concept offers a powerful tool to the user to map the privacy need of the user by means of the Policy Manager. As for the platform, the user is able to change his policy settings via the client. This allows the user to define fine-grained policies for profiles, presence and location. By that the Client Prototype is fulfilling the Privacy Principle on Changes in Policy or Data Use (PrP3). This principle states that notice must be provided when any changes are made to the applicable privacy policies or in case that the information collected is used for any reason different from the initially stated purpose.

In terms of integrating marketing or advertising functionalities, the Policy Manager gives the user transparency and control at very high granularity. As Privacy Policies are getting more and more complex with the integration of external services, the already existing component of the Privacy Advisor will support the user in understanding the consequences of his actions regarding his personal expectation of privacy. For example, the implemented Privacy Advisor functionality notifies the user about possible risks with regards to the disclosure of personal data and sharpens the awareness of the user, by that implementing the Privacy Principle "timing of notification" (PrP4). The purposes for which personal data are collected should be specified at the time of collecting the data at the latest.

Furthermore, the Privacy Advisor compares uploaded information with information stored in user profiles. Profile information is thus considered to be sensitive. No case could be identified where the PICOS Community Application Prototype requests the collection of sensitive information as defined above. The fulfilment of the underlying Privacy Principle on sensitive (PrP5) is in current commercial community platforms nonexistent. The implementation of an External Service would allow investigating the applicability of the Privacy Advisor in a business application while providing the PICOS platform and client with a unique and state-of-the-art feature.

Last but not least, the Privacy Advisor requires consent from the user, i.e., to delete a partial identity, to confirm unregistering from a community, or to publish content that contains potentially sensitive information that matches user profile attributes. By that, the client application gives the user guidance and transparency on the privacy implications of his actions. In a business scenario with external services providing marketing or advertising functionalities, the Privacy advisor again provides transparency to the user. This Privacy Principle is called Informed Consent (PrP6) and states that the Data Subject must provide informed consent to the collection of personal information unless a law or regulation specifically requires otherwise.

Unlike the platform prototype the client prototype provides a search feature on content by title, description, author, location, or type of file. The search button is on top of the Public Repository that can be accessed from “Community” in the navigation bar. The implemented search is a basic search, which identifies matching content and showing it to the user. Giving the search feature a commercial relevance could e.g., mean to implement an advertising engine. This would allow 3rd parties to drop advertisements into such an advertising engine, which then delivers a search related ad. Key question upon such an implementation would be whether the strong trust and privacy requirements in PICOS would make it necessary that such an advertising engine is provided by the platform itself or whether such a feature could be integrated as an external service via the Platform APIs while respecting the privacy settings of the user and preserve the usage of his data subjects.

5.4.4 Summary of findings and recommendations

In this chapter, we have presented an analysis and evaluation of the business potential and economic functionalities of the community prototype 1, described in D6.1. In summary, the PICOS Application Prototype in its current state and its user centric view complies with the set of trust and privacy principles, but at the same time does not provide functionalities to make use of the social capital as value of the community, which was not a requirement for the first cycle of the PICOS project, but is investigated in the second phase as it as a strong requirement of community providers.

In the process of the evaluation the distinction between the functionality of the platform and the application was not always clear. A clearer definition which component of the PICOS Application Prototype is just a visualisation of a platform component or has itself the logic in it would make it easier to evaluate the economic effects. Regarding the strong privacy mechanisms, the key question for the PICOS client accounts the same as for the PICOS platform: How to integrate features for marketers and external service providers to make use of personal information provided by the community. A concrete scenario is already described in PICOS Use Case 6, i.e., the voucher gratification for users earning reputation in a community. Context sensitive advertisements would be another example of implementation. The mentioned advertisement engine could gather anonymous cross-sectional data from the platform, which then is provided to the marketers in form of different target groups. Marketers can then adapt their advertisements and transfer them to the platform. The platform itself proceeds the matching with the users which are part of the target group and delivers the advertisement. But in this scenario the anonymous cross-sectional data collection might state an issue in regards to privacy policy agreements. Last but not least, the implemented search feature can be extended by marketing related mechanisms.

In summary the client prototype holds some economic potential yet not accessed. Implementation of such features always has to be subject to the PICOS trust and privacy principles.

5.5 Usability evaluation

The general procedure of the evaluation activities in the first phase of the PICOS prototype included an expert evaluation on usability and functionality during the implementation phase and lab and field tests. The aim of both lab and field tests was the evaluation of the PICOS concepts on trust, privacy and identity management in virtual communities and the application prototype. For this purpose, lab and field test with 12 participants in Vienna and respectively Kiel have been conducted. Participants had to complete several tasks, which will be described in section 5.5.1.

The tests took place on the 27th /28th November 2009 in Vienna and 12th /13th December 2009 in Kiel. Lab test in November took place at the lab of CURE in Vienna and the according field trials took place at a fishing lake in Groß-Enzersdorf near Vienna. Tests in Vienna were conducted by Eva Ganglbauer (CURE, Vienna), Bernd Ueberschär (IfM-Geomar, Leibniz Institute of Marine Sciences, Kiel) and Markus Tschersich (Johann Wolfgang Goethe-Universität, Frankfurt).

Lab tests in December took place at the lab of Leibniz Institute of Marine Sciences in Kiel and the according field trials were conducted at two fishing lakes in Jevenstedt, close to Kiel. The Kiel trials had been conducted by Eva Ganglbauer (CURE, Vienna), Bernd Ueberschär (IfM-Geomar Leibniz Institute of Marine Sciences, Kiel), Katja Böttcher (Goethe University Frankfurt) and Philipp Kropp (IfM-Geomar Leibniz Institute of Marine Sciences, Kiel).

5.5.1 Methodology used

The expert evaluation was carried out based on the experience of an expert. This included the analysis of the PICOS angling application regarding usability and major problems. The analysis of central usability problems included also encountered bugs. The following methods common in the field of human computer interaction have been applied:

- Usability quick expert review through criteria relevant for usability and common guidelines.
- Adoption of expert methods such as heuristic evaluation, cognitive walkthrough and mobile user interface principles.

The methodology for the tests involved all in all 24 test participants. Participants for the first tests in Vienna had been recruited via online announcement at an Austrian job portal for students. For the tests in Kiel an already existing angling community was recruited. The recruiting had been done with respect to the following characteristics:

- Being an active angler
- Interested in innovative and mobile technologies
- Experienced in using mobile phones
- Participants can deal with an application in English
- Diverse demographic background
- Some anglers should already know each other

For Vienna and Kiel, finally 24 persons, 21 male (75%) and three female (25%) in the age of 18 - 55 years (M = 27,12) took part. For their participation at two test days they got an allowance of 130€ (60€ for the lab test and 70€ for the field test) to compensate the time and effort they invested for the tests.

Test participants had been asked to complete three different questionnaires: PET-USES, SUS and a pre-test questionnaire including questions about demographics, interests, angling experience and experience with online communities as well as questions about privacy concerns. The questionnaire furthermore asked for previous experience with mobile devices, online communities, angling community, expectations regarding an angling community and the subjective importance of privacy, trust, identities and security for the user.

The pre-test questionnaire for Vienna showed that the participants had different angling experience ranging from 1 - 25 (M = 13,83) years. The participants stated that they are mainly interested in "sports" (75%) and "travelling" (66,76%). On average the participants go fishing Z = 1-3 times per

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

month. They spend on average one day (M = 11,77 hours) with fishing. The majority of the participants answered to the question what could be a reason to deter them from angling: “having not enough time” (91, 67 %) followed by “no friends with the same interest” (16, 67%). Participants rated their English comprehensive skills as “well”. All participants were owners of a mobile phone. The majority of the participants use their mobile phone for “calls” (100,00 %), “SMS” (100,00 %) and the “calendar” (75%). The pre-test questionnaire showed that 66, 76% of the participants had been already member of an online community and stated that they are using online communities on average 1-3 per week. The majority participants are member of Facebook[32] (41,67%), StudiVZ[33] (33,33%) and MySpace[34] (25, 00%). Only one participant (8,3 %) had been already part of a mobile online community. Concluding, results of pre-test questionnaire showed that the twelve participants met the recruiting criteria.

For Kiel, the pre-test questionnaire showed that the participants had different angling experience ranging from 12 - 49 (M = 21,75) years. The participants stated that they are mainly interested in “sports” (75%) followed by “Computer” (50%), “education” (50%) and “travelling” (50%). On average the participants go fishing Z = 1-3 times per month. They spend on average 5, 5 hours with fishing. All participants (100%) answered to the question what could be a reason to deter them from angling: “having not enough time”. They rated their English comprehensive skills as “very good”. Only one participant has no own mobile phone. The majority of the participants use the mobile phone for “calls” (91,67%), “SMS/MMS” (83,33%) and as a “calendar” (41,67%). The pre-test questionnaire showed that 83,33% of the participants had been already member of an online community and stated that they are using online communities on average 1-3 times per week. The majority participants are member of StudiVZ (66,67%), Facebook (50%) and Xing[35] (33,33%). Additionally the participants mentioned participating at angling specific online communities (“Leidenschaft Meerforelle”, “Anglercommunity”, “angler online”, “IFish”). Already 3 participants (25%) had been part of a mobile online Community. In sum results of pre-test questionnaire showed that the 12 participants met the recruiting criteria.

The Tasks for the lab and field tests were almost the same for Vienna and Kiel. The differences between tasks in Vienna are not really worth mentioning, therefore only the tasks for Kiel will be presented. For the lab tests nine tasks had to be carried out:

- **Task 1**: Please register and log into the angler application. Please enter at least your age interval at the profile.
- **Task 2**: Please explore the application freely. You have 2 min for this.
- **Task 3**: Please create a further identity to your account and use the new identity.
- **Task 4**: Please search for the contacts “test lead” and “Cure.eva” and add them to your contacts.
- **Task 5**: Please send a message to “test lead” with reference to “test message 1” containing short greetings.
- **Task 6**: Within the angler application you have the opportunity to create public and private sub communities with different access right as well as public community. Find the forum “lab test” of the public community and post in the thread “Put & Take Seen:-)”

[32] http://www.facebook.com/
[33] http://www.studivz.net/
[34] http://www.myspace.com/
[35] http://www.xing.com/

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

- **Task 7**: The default settings of the application protect all your personal data. You can show the data of your profile (e.g. age) to specific members if you want to. Create a privacy rule, which show your age to the contact “test lead”.
- **Task 8**: Go to Catch Reports of the public community, rate and add a comment the post “fast trout”.
- **Task 9**: Logout and exit the application.

The test facilitator sat next to the participant and presented one by one the written task to the participant. If necessary test facilitator explained the task once again in his/her own words therefore it has been ensured that every task had been understood right by the participant. The participant was asked to think aloud while s/he was solving the task. Events, problems and comments of the participant were listed and written down by the test facilitators.

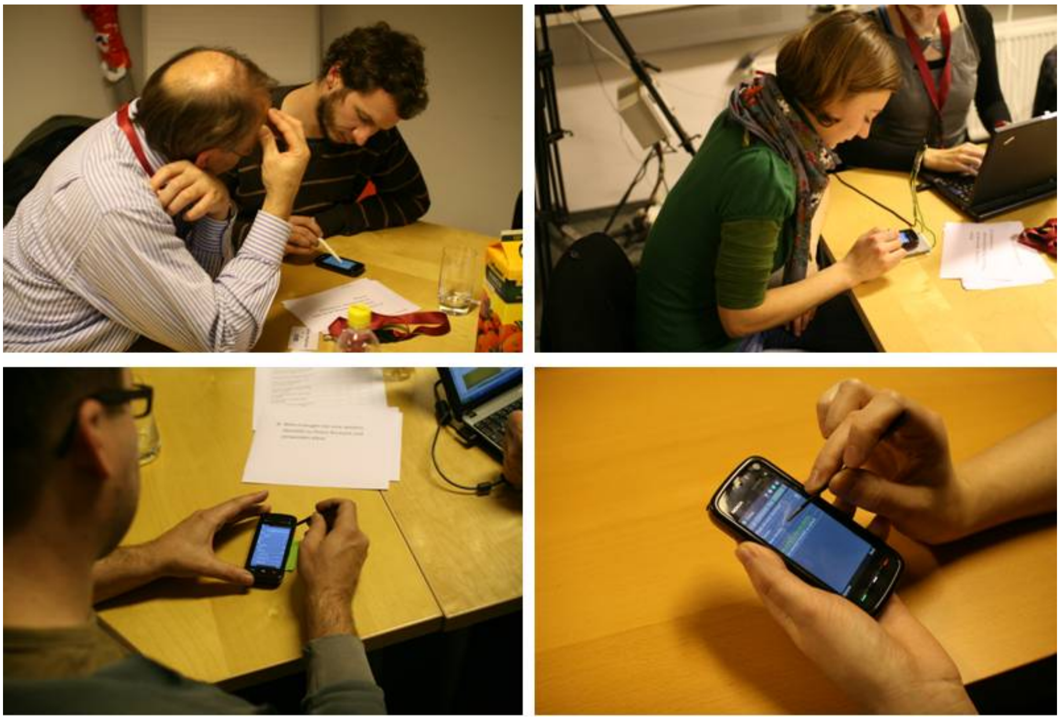


Figure 1: Participants during lab tests in Vienna using the PICOS angling application

For the field tests, 6 tasks were carried out in a real-world context at angling lakes. The tasks have been sent as messages to their mobile phones.

- **Task 1**: Find the watercourse “Jevenstedter angling lake”on the map.
- **Task 2**: Try to locate all your angling colleagues on the map who are contacts on your list.
- **Task 3**: Please “blur” (approximate display) your position for your contacts (1km).
- **Task 4**: You caught a fish. Please create a new catch report and insert a picture (of the caught fish). Make your entry available for the public community. Alternative: You haven’t caught a fish. Create a private sub-community and invite your friends to discuss about successful lures of the present day.

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

- **Task 5**: Please comment and rate the watercourse “Angling lakes Jevenstedt”. Enter your favorite angling spot of this angling lake as fishing spot at the watercourse advisor.
- **Task 6**: Please check exactly which fish species you caught and find out about the scientific name.

The participants in the field have been asked to deal with the tasks on their own. Every participant received the following tasks by asynchronous messaging on his/her device: One field test task (4) was replaced compared to the field tests in Vienna based on the experiences there. After the field tests, participants and trial facilitators moved back to the lab and carried out the questionnaires on paper and personal interviews.

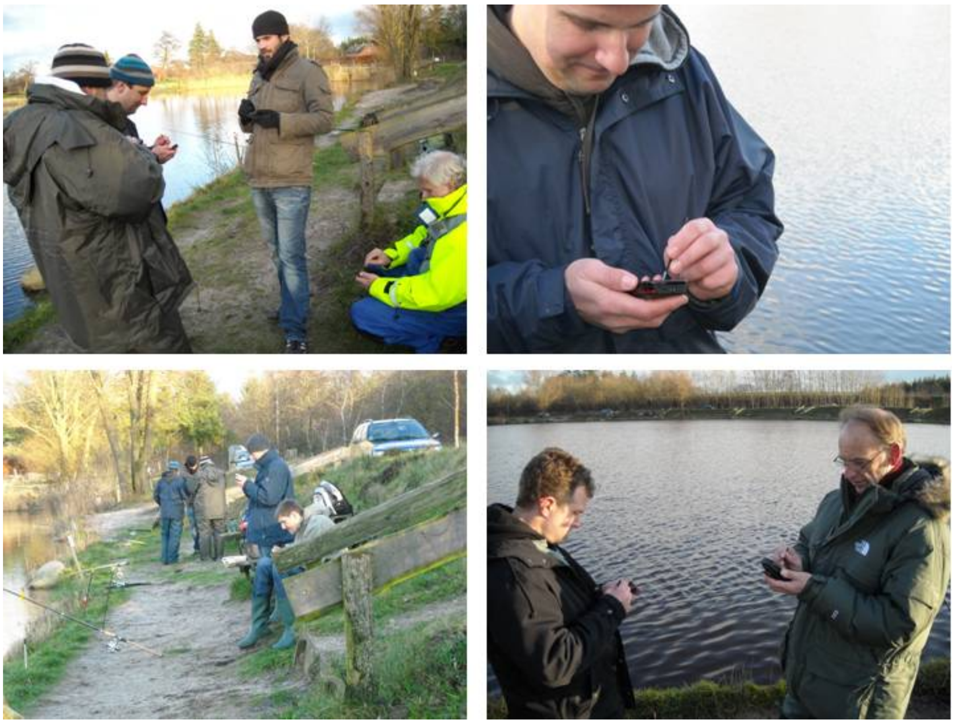


Figure 2: Participants during the field tests in Jevenstedt near Kiel while using the PICOS angling application.

5.5.2 Documentation used

In order to analyse the usability during the lab and field tests, various documentation was used. The test facilitators were writing down observations, problems and processes of interactions during the lab tests. Questionnaires and pre-questionnaires had to be filled out, which not only provided analysis, but also some form of documentation. Of some participants the face and his/her detailed interactions with the mobile device were recorded concurrently for later analysis, as illustrated in the figure below.

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

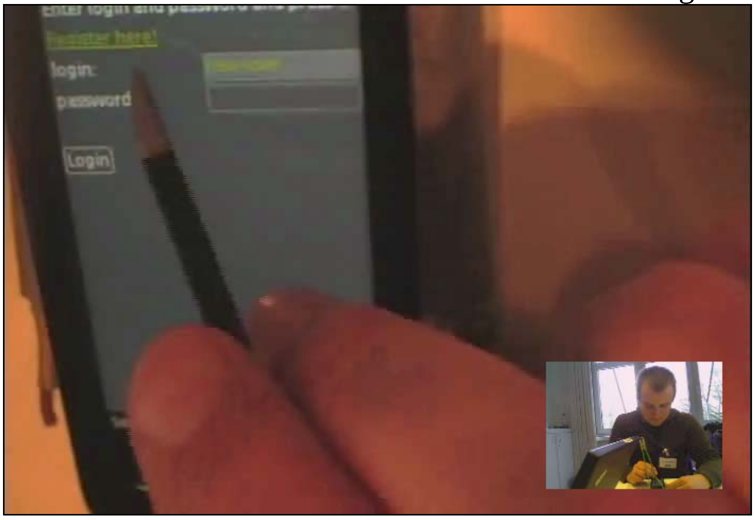


Figure 3: Snapshot of a video recorded during the lab tests.

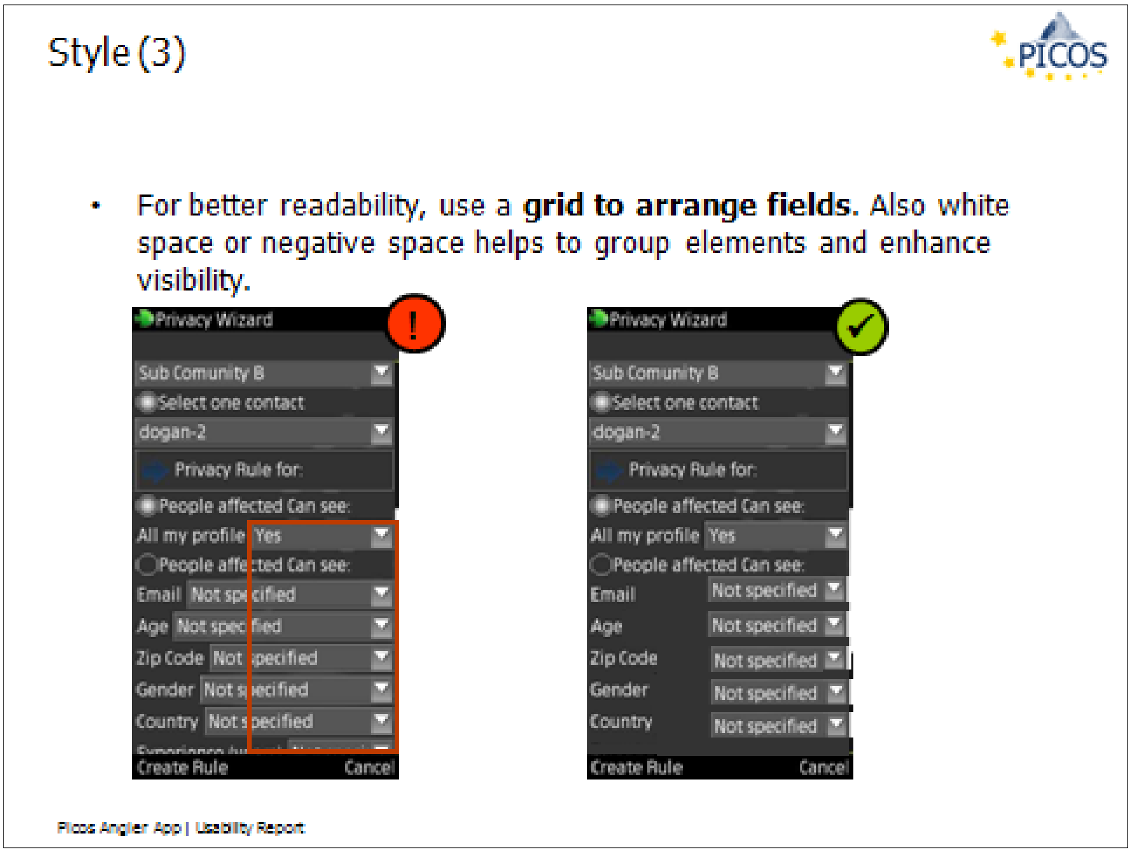
For qualitative analysis personal interviews were carried out, which have also been documented as the answers have been written down by the trial facilitators. The detailed scheduling and arrangement of the tests was documented as well to support the process of planning.

5.5.3 Installation – Functionality & Operation

In order to be able to carry out the tests, installation was conducted before the lab and field tests. The usability of the installation process was not a matter of analysis with members of the community. Only the usability of the application itself was intended to be evaluated, the installation process was not included in the usability evaluation. The focus was rather on the usability of P privacy enhanced technology (PET) than on the installation processes.

5.5.4 Evaluation of the requirements and functionalities of the Angling Community Prototype

Before the tests during the implementation phase, expert usability feedback on the actual application has been conducted by the Center for Usability Research & Engineering. A presentation was sent to all partners to discuss different topics and addressed usability problems. An example slide from the report is shown in the figure below:



Style (3)

- For better readability, use a **grid to arrange fields.** Also white space or negative space helps to group elements and enhance visibility.

Privacy Wizard

Sub Comunity B
Select one contact
dogan-2
Privacy Rule for:
People affected Can see:
All my profile Yes
People affected Can see:
Email Not specified
Age Not specified
Zip Code Not specified
Gender Not specified
Country Not specified
Create Rule Cancel

Privacy Wizard

Sub Comunity B
Select one contact
dogan-2
Privacy Rule for:
People affected Can see:
All my profile Yes
People affected Can see:
Email Not specified
Age Not specified
Zip Code Not specified
Gender Not specified
Country Not specified
Create Rule Cancel

Picos Angler App | Usability Report

Figure 4: Example slide from expert usability feedback on application to support implementation process.

5.5.4.1 Lab and Field Tests

For the lab and field tests, various instruments have been used to collect data, observe, analyse and evaluate the usability. The usability with a special focus on PICOS PET concepts will be described in Section 5.5.4.2.

The "System Usability Scale" (SUS) was filled out by the participants after carrying out the tasks of the lab tests and the interviews that followed the tasks. The SUS is a questionnaire which measures the subjective satisfaction of users who rate the usability of a technical system. The 10 items are formulated as statements. The user can express his/her extent of agreement on a 5 point agreement scale (ranging from 1 = "I agree very much" to 5 = "I disagree"). The SUS is a rough measurement of the usability of a system. A SUS score ranging from 100 to 80 is declared as "very good", from 79 to 70 as "good", from 69 to 60 as "acceptable" and below 60 as "not acceptable".

The SUS rating was between acceptable and good for the lab tests in Vienna and Kiel. After the field tests in Kiel, data from another SUS questionnaire was gathered, and showed different results, as indicated in the figure below.

The 12 participants in Vienna rated the PICOS prototype as "acceptable" on average. In Kiel, the angling application was rated between "acceptable" and "good" after the lab test and between "acceptable" and "not acceptable after the field test. The SUS questionnaire was carried out a second

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

time after the field tests only in Kiel. During field tests naturally more problems occur as it is a setting with uncontrolled conditions, which is an explanation for the inferior SUS rating after the field test.

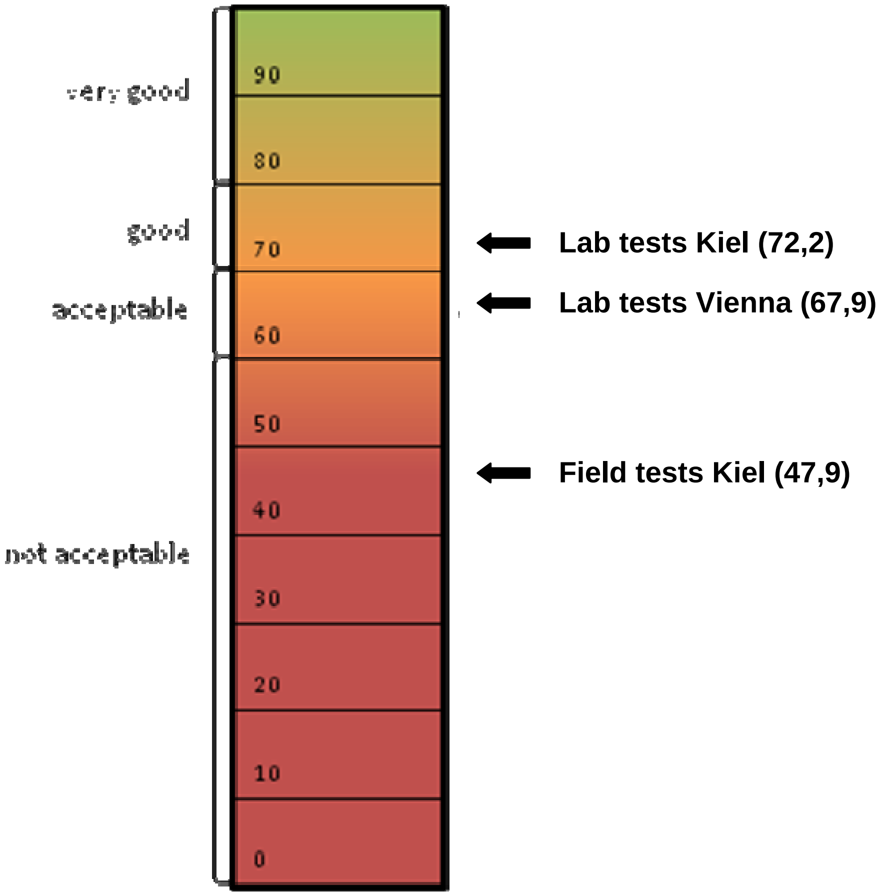


Figure 5: SUS score of PICOS angling application after lab tests in Vienna.

The test participants have been interviewed after the lab and field tests. After the lab tests on the first day of the tests, the general impression of the application was "good" and "interesting". Some statements are listed below:

> *"My impression is very good; the application offers a very fast way to exchange information with friends. There are many possibilities to choose and many topics available."*
>
> *"Very interesting, but I would need more experience to say more."*
>
> *"I would need more overview and would desire more pictures where you can click something. Maybe you need more time to get a better overview if you deal with it a longer time."*
>
> *"It's implemented very basic and not really fun to use. But I know that it's difficult to do something like that on a mobile device."*

The user comments gathered in the interviews after the field tests were less positive. Most of the trial participants embraced the general concept of the angling application and the privacy functionalities, but criticized the implementation, the feedback it provides and the design. Most of them had concerns using it during angling, as their fingers would be very dirty.

> *"The application offers very good approaches, but many things can be improved. At the moment, you wouldn't use it during angling, as it takes up a lot of time because of error messages and slow reactions"*
>
> *"The application is hardly viable for a practical context. Many things and actions last for a long time, which results in less time for angling. I think that this would deter most users from using it directly during angling. You never know exactly if the program understood a click or not, because nothing happens then."*
>
> *"In principal my impression was very good, the application would be used in general, but the navigation of the menu needs some time and effort getting used to. All in all my rating is positive, as there are very interesting functions after getting used to the application"*
>
> *"For a mobile application it offers too many possibilities. You can enter details that are very complex, and this deters the users from angling"*

Based on the user's comments, interviews and the observation during the lab and field tests the following problems were identified respectively recommendations and suggestions. The results on usability problems after the tests in Vienna have been summarized as follows:

1. Most probable **next steps** should not be hidden in the context menu "Options". Test participants always had to search again and again to find the next step and told us repeatedly to **have the most probable option visible**.
2. Navigation has to be **more consistent**. Different programmers have obviously chosen different types of navigation.
3. **Improved feedback times** for the angler application: there was EDGE during the field tests, but test participants even complained about slow reaction times during the lab tests with WIFI). Add an indicator which indicates that the application is working, such as an hour glass.
4. **Improved touch feedback-visualisations:** Highlight different options from the "Options"-Context menu when they are clicked or touched. The Nokia 5800 typically vibrates if a button is clicked.
5. No test participant could find the **diary entries in the repository**, so these options should be on the first level of the community screen. We recommend discarding the "Repository" as first level." Make "**catch reports**" a dedicated button in the menu and in general, add more generic buttons in the main menu for important resources (user wanted to have a more direct success instead of working down in sometimes confusing sub-menus).
6. Add **"send a message" to the Options in the Contact screen**. The participants did not understand that the "write message" was hidden behind the "Home" button; It would improve the angling application to add the "write message" to the "contacts" also because the option to start a "chat" is possible. It's positive if a process for carrying out an action is provided on several occasions.
7. The meaning of the little icons on the top right were not obvious for many user.

8. Some participants couldn’t find where to write a message, therefore **Inbox should be an item** in the menu bar

9. **Consistency:** Buttons and Links are sometimes used interchangeably, it’s not clear for test participant where buttons or links are used.

10. It was not clear for participants where they can scroll (horizontally or vertically) **visible scroll-bars** would be very helpful for that.

11. The **layout** of many screens needs to be rearranged to be more logic and graspable. (E.g. a lot of participants needed some time to understand the catch diary entries layout)

12. **Wording** (people really had problems to understand the “**policy creator**”, the “**repository**” and the “**private room**”)

13. **Context sensitive help** was several times required from the participants.

14. Many participants use the phone in **landscape mode** over the whole time. So some pop-ups had been out of the screen. (e.g. the announcement after login)

15. Make **all elements** (also the watercourse advisor) **editable** and allow to replace an instantaneous snapshot with a photo taken later with the mobile device and allow more text.

16. Make **OK-buttons** visible in horizontal position of the screen (users were worried what to do when they have joined the community, since the ok-button is not visible in the horizontal position.

17. When **rating and commenting** an entry in the watercourse advisor, there should be an indication, that rating and adding a comment are in the same place (only "rating" is seen at present)

18. The "**Option"** button below left: changes the available items, in context to the function which was called, that made the user a bit worry because there is no instant feedback if the option was clicked or not. Furthermore, sometimes the **"Exit"** command appears there, sometimes not.

19. Most anglers preferred to **use the application with the fingers** and not with the stylus, for which the application was designed.

Some adaptations that were easy to carry out happened between the first set of tests in Vienna and the second in Kiel. Some changes of PICOS prototype have been implemented. These changes concerned the screen of the partial Identities, which has been restructured and textual links received the appearance of a button. An hour glass function was added when the application was loading content, the term “Repository” was replaced by “Public Community Content” and received the appearance of a link.

The methodology for the tests remained the same, except some minor changes in the tasks and a second SUS questionnaire after the field tests in Kiel.

Results after the tests in Kiel have been summarized as follows:

1. **Long response times** and **reaction times** were named as major problems during usage of the system. Additionally, often feedback was missing if the application is working or an abnormal system end has occurred.

2. For many actions, **feedback** after carrying out actions is missing (e.g. after creating and publishing a post or after creating a privacy rule with the policy editor). Feedback is also missing regarding the participants don’t know if the application is working or has crashed. Users should always be able to know what the angling application does and in which state it is

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

3. **Registering** often couldn't be carried out, therefore the trial conductors had to tell the participants to connect to the internet before they started the application. Leave a hint at the start of application that user should check their connection and access points manually.

4. **Layout of the screens** was sometimes very confusing for users. Improved GUI/Layout would include a better structuring, highlighting, differentiating between elements and sub-elements is needed. Most important, a better graphical description and accentuation of the main menu would improve usability.

5. For better **navigation** with more levels, a breadcrumb navigation bar is recommended. A bigger scrollbar would improve the navigation within a screen

6. Most participants couldn't find the "**policy creator**" to create new privacy rules**.** Rename the policy creator into "privacy manager" and integrate there to add new privacy rules.

7. Some participants were not able to create new **privacy rules** or were unsure if they added new rules successfully, some can't scroll until the bottom and therefore don't find the settings they are searching for (make scrollbar more visible).

8. The map doesn't show a reload button for **map** would be desirable. There should be a default button "locate me" or displaying last location.

9. **Inbox** as an own menu item necessary, Chat is less important (eventually discard "Chat" from the main menu).

10. Test participants are not able to have a look at the message they sent. It would improve the usability if users could have a look at **sent messages**. A separation between the inbox and the outbox would be necessary then.

11. The **list of catch diary entries** in the public community is very confusing for test participants as orientation and order is missing. Logical and proper alignment of the elements is necessary. Furthermore it would be recommended, to rename "rate" into "rate and comment".

12. **Catch reports** of the public community were very difficult to find for users. The link to catch reports should be on the first Screen of the Community page. Catch reports are very prominent and important for users. Though, more transparency is needed to differentiate between catch reports in the private room and public community.

13. For the anglers, **Private Room** should be renamed into **"My catch diary"**.

14. Supportive **help text** should be provided on several occasions to explain the concepts (e.g. for explanation of partial Identities, privacy manager, root profile)

15. The use of the **"back" button** should always bring the user back to the previous level of the angling community and into the right one. At present, the back button is navigating back to sometimes inappropriate screens (e.g. clicking the back button after creating a privacy rule transfers users to the identities screen.)

5.5.4.2 Evaluation on Usability of PICOS Privacy Enhanced Technology

The intention of evaluation with users was on the one hand on general usability aspects, on the other hand there was a strong focus on the usability of privacy enhanced technology aspects. To evaluate the usability of Picos PET concepts the test participants were asked to fill out the PET-USES

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

questionnaire and interviewed after the field tests. PET-USES[36] is a questionnaire that enables users to evaluate PET-User Interfaces for their overall usability and to measure six different PET-aspects:

- Data-management: The extent to which the system makes it easier to store and organize personal information. This scale can be used to evaluate all types of identity management software and services.
- Credential-management: The extent to which the system makes it easier to store and organize certificates and credentials. This scale can be used to evaluate identity management systems that include issued claim credentials (e.g. the Higgins project4).
- Privacy Preferences: This scale is designed to measure the extent to which the system makes it easier to set general and excessive levels for data release policies and to what extent the user is informed of unwanted data dissemination. Thus, an aspect of this scale is the decision support qualities of the system.
- Recipient Evaluation: the extent to which the system helps users to evaluate the data recipients' credibility and trustworthiness. This scale can also be regarded in terms of decision support.
- Data Release: The extent to which the system clarifies what personal information is being released and who is the recipient of the data.
- History: The extent to which the system can show the user when, what and, to whom personal information has been released and thus provide an overview of what data any given service provider might have accumulated

The PET-USES consists of two major parts of questions: one part measuring overall usability and one part measuring PET-aspects. Only the PET aspects have been evaluated, as the usability aspects were already evaluated with the SUS questionnaire, The SUS questionnaire consists in fact of the same questions than the usability part of the PET-USES. The PET-usability scales evaluate the extent to which the software assists the user in learning and understanding privacy related issues.

During the Picos lab tests a shortened version of the PET-USES was used. Items which relates to features which are not available with the PICOS angling application were discarded. Finally the PET-USES of PICOS lab test consisted of 15 items, discarding the Credential management aspect, as credentials are not supported at all by the application, respectively three items belonging to one of the 5 different PET scales: Data Management, Privacy Preferences, Recipient Evaluation, Data Release and History. These items are statements to which the users can rate the extent of their agreement on a 5 point agreement scale (1 = very to 5 = no).

Results of the PET-USES questionnaire indicate that the users rated the PICOS application mostly "in between" concerning the support of the application to learn and understand privacy related issues.

Results of the mean values of the used PET-USES scales are shown in the table below.

The quantitative results from the PET-USES questionnaire indicates that test participants agreed on a medium level to the usability of the PICOS privacy enhanced technology functions (M = 3,05, SD = 0,92). The users rated the PICOS application mostly "in between" concerning the support of the application to learn and understand privacy related issues.

[36] Erik Wästlund, Peter Wolkerstorfer and Christina Köffel, PET-USES: Privacy-Enhancing Technology - User's Self-Estimation Scale, 2009

Privacy Enhanced Technology Questionnaire	**Kiel**		**Vienna**	
	Mean	Standard Deviation	Mean	Standard Deviation
Data management	2,99	1,08	3,17	0,73
Privacy Preferences	2,53	1,11	3	0,74
Recipient Evaluation	3,14	0,7	2,83	0,95
Data Release	2,78	0,99	2,83	0,77
History	3,58	1,31	3,47	0,86
	3,004	**1,038**	**3,06**	**0,81**

Table 1: Quantitative results from the PET-USES Questionnaire (1 = Disagreement that the evaluated system supports this aspect, 5 = Agreement that system supports this concept).

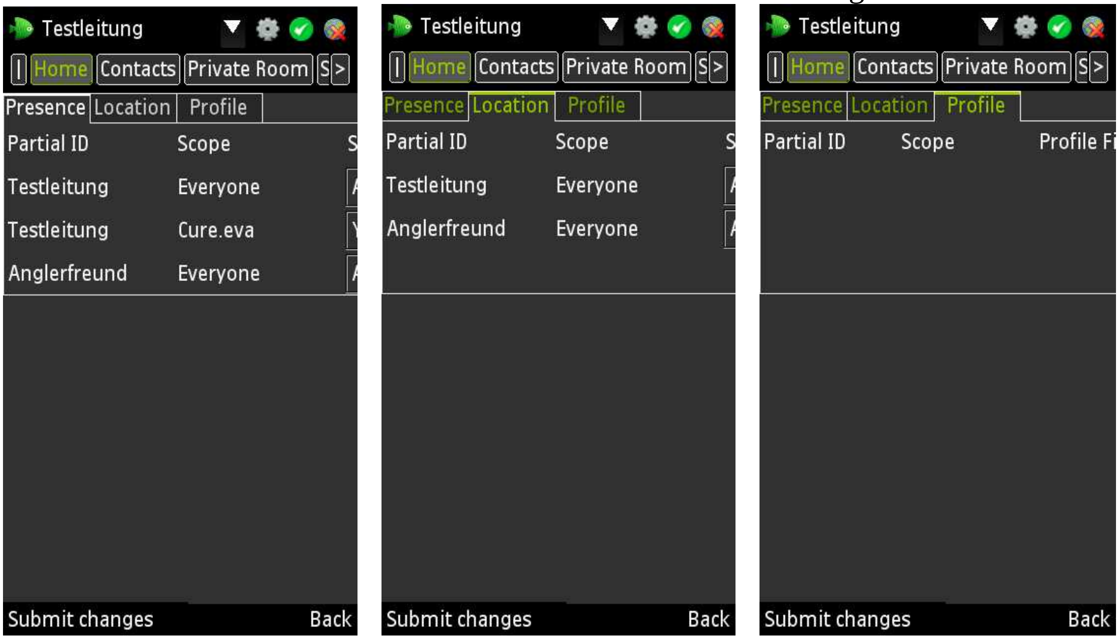
The qualitative results show that test participants appreciated the PICOS privacy enhanced functions, especially the possibility to create private Sub-Communities. A private Sub-Community enables them to discuss certain topics only with a chosen set of friends, and only invited participants can join it. This concept is a possibility to discuss certain topics and exchanging content within the community without external users. The concept of hiding certain information or attributed from certain contacts on a very granular level was appreciated very much, thus the usability of the angling prototype was criticized as it was very difficult to create privacy rules and no feedback was received after successfully generating a rule. Some tests participants argued that the list of rules could become confusing if many rules are applied. The horizontal scrolling through the overview of privacy rules was adding to the confusion. Figure 16 depicts the policy editor.

The appreciation for the successful concepts of private sub-community and privacy rules on a very granular level was not the case for the concept of partial Identities though. Only a few users appreciated this idea: some didn't understand the sense behind of it and some were even strongly declining this function:

> “*I would never let my daughter be member of a community that supports to have several identities.*”

Other statements regarding PICOS privacy enhanced concepts were:

> “*I think the functionalities are great, and I would really use them.*”
>
> “*These are very good functionalities. There are a lot of settings you can choose (comparable to network settings in Windows). But I feel slightly overstrained by the possibilities; the small graphical display of the device is not suitable for something so complex. All settings should be accessible from one point*”
>
> “*For me these functionalities are not important, because I would not even disclose sensitive information*”
>
> “*The privacy protection function* [the policy editor] *is a good idea, it assures certainty while using it, but I wouldn't use the partial Identities*”



Testleitung

| Home | Contacts | Private Room | S >

Presence | Location | Profile

Partial ID	Scope	S
Testleitung	Everyone	A
Testleitung	Cure.eva	Y
Anglerfreund	Everyone	A

Submit changes Back

Testleitung

| Home | Contacts | Private Room | S >

Presence | Location | Profile

Partial ID	Scope	S
Testleitung	Everyone	A
Anglerfreund	Everyone	A

Submit changes Back

Testleitung

| Home | Contacts | Private Room | S >

Presence | Location | Profile

Partial ID	Scope	Profile Fi

Submit changes Back

Figure 6: Screenshots from policy editor, which provides an overview of privacy rules.

Some of the PICOS privacy enhanced technology concepts were difficult to understand because of the language barrier. English was not the mother tongue of test participants and therefore the language was a barrier to understand the concepts in some cases. Overall, the extent to which the language barrier played a role can’t be estimated in detail, only a comparative study could shed some light in this matter. It was definitely the case that most anglers were asking for a version of the angler application in German. They assumed that an English angling application would not work out for the common angler in Austria and Germany. Most participants for the tests had an academic background, and understood English very well, though understandably they had problems to understand some terms.

5.5.5 Summary of findings and recommendations

The lab and field tests indicate a trend that users appreciated the location based services most and could imagine using them for angling specific activities. The PICOS PET features such as the policy creator were difficult to handle and are naturally more complex; the concepts are difficult to grasp and a mental model is not easily developed. Although the focus in PICOS is not on usability, it has to be considered as prerequisite of privacy enhanced user interfaces and interactions. The results of the lab and field tests clearly indicate that the privacy, trust and identity management functions can’t be comprehended without usable and logical interfaces and interactions.

The trial participant’s quantitative rating of the angling application was between “acceptable” and “good” after the lab tests in Vienna and Kiel with Wi-Fi access. In Kiel, the questionnaire was repeated after the field tests, and for this the SUS rating dropped to between “not acceptable” and “acceptable” to 47,9 points out of 100. Naturally, more problems do occur during field tests than during lab tests, as real conditions always involve more potential problems than in controlled conditions. E.g., the previous access points for internet connections during the field test had to be deleted to be able to connect to the mobile internet. The tasks could not be carried out from the beginning of the field tests. However, the qualitative statements from the users indicate the same trend that the application was considered less usable after the field tests.

The results of the lab and field tests show that the anglers appreciated the location based services such as the watercourse advisor and angling specific functions like the species summary very much. Participants were more critical regarding the PICOS PET concepts, which are naturally more difficult and complex to understand. Therefore well-designed and implemented solutions are required to ensure that users really understand the concepts and how they can use it. To sum up, the concept of the private sub-community and the policy creator were rated very well in qualitative statements. The trial facilitators observed that the privacy advisor was not perceived as such, and it definitely needs a different presentation in the interface. The messages from the privacy advisor were perceived as confusing or interrupting the flow of interactions. This is also due to the fact that the privacy advisor played a minor role for the first version of the prototype and will be elaborated for the second version. The users should be better informed about its purpose once it's going to be implemented in more detail for the second version and named as such.

All test participants agreed that they would very much appreciate a web frontend to use for more user-friendly text input and to have a better outline of the system. A small display can only present a small subset of the complex functionalities provided by the PICOS angling application, which makes it more difficult to understand and to use.

In regard to the user trials problems such as very slow reaction times, missing feedback and moderate usability have to be solved. During the user trials the community will be used freely by users for one month to observe natural interaction within the community, between individuals and the system and analysis of usage of PICOS PET concepts.

The results of the lab and field tests indicate very clearly, that usability is a prerequisite for the perception, understanding, comprehension and the usage of PICOS PET concepts. All users appreciated most of the PICOS PET concepts in general, but criticized that it was often confusing to use them in the angling application. Only if the PICOS PET concepts are presented well and the interactions on them are easy to carry out and support the mental model of them, users are going to understand and use these concepts.

6 Conclusions and recommendations for the developers

The present deliverable D8.1 "Legal, economic and technical evaluation of the first platform and community prototype" focused on the evaluation of the technical and development activities of the first development cycle of the PICOS. More specifically a comprehensive evaluation of the PICOS Platform Architecture and Design v1 (WP4), of the PICOS Platform Prototype v1 (WP5) and of the PICOS Angling Community Prototype v1 (WP6) was conducted. An overall comment, arising from the evaluation conducted on the work realised in the PICOS first cycle, is that the PICOS project has to a large extent achieved its goals with regard to trust and privacy in context-rich mobile communication services. The multi-disciplinary evaluation that was realised in this present PICOS deliverable resulted in a number of critical observations and recommendations that should be taken into account during the second cycle of the PICOS project. They can be summarised as follows:

Legal evaluation

The PICOS technical and development team has worked in close cooperation with the legal one since the beginning of the project. The continuous cooperation and discussions over various issues regarding the design and implementation of the PICOS platform are in full respect of the "privacy-by-design-model" that was implemented in practice in the PICOS project. All three steps of the PICOS first development cycle (PICOS Design and Architecture v1, PICOS Platform Prototype v1 and PICOS

Angling Community Prototype 1) were carried out in close cooperation with the legal team which resulted in the full respect of the data protection principles and the protection of the rights of the data subjects in PICOS.

Technical evaluation

Trust and privacy evaluation

One of the critical issues is the way PICOS would attract community members so that their trust with the system will have an increasing tendency. These issues are discussed in the D4.1 deliverable “Architecture”, but it is advisable that these descriptions are placed together. It should also be clearly stated that PICOS supports the data minimization principle in order to inform Members that they are not required to provide more private information than requested. Privacy principles 14, 16, 17 and 23 can provide better specification of methods of objective trust, methods of authentication and information protection.

With regard to the PICOS Platform Prototype v1, the main recommendation from the trust and privacy prospective is basically to provide a further description of several attributes: Contact list attribute and sub-community attribute - description does not state who has an explicit access to these attributes; Reputation attribute - there is no formal definition of the algorithm used for computing the reputation score; Sub-community reputation attribute - there is no description of the computation of this attribute; Partial identity attribute - more precise distinction of what can be updated on the partial identity level and primary identity level.

Relating to the PICOS Angling Community Prototype 1, although most of the trust and privacy principles are currently enforced by the PICOS Angling community prototype, the provision of other authentication mechanisms apart from user/password, such as Certificates or Federated access (OpenID) should be considered. However it is realised that this heavily depends on the functionality provided by the platform and should be a clear decision of the PICOS Consortium. Moreover the PICOS Angling community prototype should provide better location based services, in the sense that they are more privacy friendly –keeping of course in mind that this heavily depends on the functionality provided by the platform.

Evaluation of the community focus

The PICOS Platform Architecture and Design v1 has used state-of-the art artefacts to design architecture. The artefacts are plausible and comprehensible, but the interactions between the components are not thoroughly discussed. This should be done more detailed within the development of the second version of the architecture. And perhaps some design patterns can be used for this second version, for example the adapter pattern for the connection of external services.

Within the refinement of the architecture for the platform prototype it has not been possible to directly derive the architecture principles and features and especially the components from the requirements. Therefore the results of the evaluation of the innovative concepts of the PICOS platform during the trials should be used to reveal a more comprehensible connection between requirements on one hand and components of the architecture on the other hand. Especially it should be proved whether the splitting and completion of components (split: profile manager into profile server and privilege server; completed: public community server) and the adding of components which was done for the first version of the platform prototype (D.5.1) was adequate and should be transferred to the architecture. During this process the differences between D.4.1 and D.5.1 regarding the naming of components and regarding the use cases should be cleared out.

The PICOS Angling Community Prototype v1 makes use of all evaluated platform components identified in D5.1.

Evaluation relating to Location Based Services and Communications Features

A more explicit linkage between D2.4 "Requirements" and D4.1 "Architecture" would underline, how and where requirements have been realised in the architecture. For the second project cycle, some more concrete guidelines, especially with regard to WP5 and WP6, should be provided by the design and architecture team (WP4) in order to turn the high level architecture and design into a real implementation. Finally, some figures and notations in D4.1 are not self-explaining and should be substituted by more widely used notations like UML to avoid misunderstandings.

The evaluation relating to Location Based Services and Communications Features of the PICOS Platform Prototype v1 revealed that some more architectural information of the integrated components and servers of the other partners is needed. Some figures and notations in D5.1 are not self explaining and should be substituted by well known notations such as UML to avoid misunderstandings. The delivery process of the APIs (WSDLs, API description etc.) has to be optimised for the next implementation work. Finally the distribution of installation packages to all partners with corresponding instruction for deployment, upgrades, and security configuration could be beneficial for the project.

The good quality of the PICOS Angling Community Prototype v1 documentation, as compiled in D6.1, could be surely increased if the WP6 partners agree on the detail level of the used UML diagrams, their kind, and their detail level. Also beneficial for the second development cycle is the provision of more information for the integration of the Privacy Advisor integration in WP5 and its usage possibilities in WP6. Such information would assist the study on new privacy-enhancing and privacy-preserving solutions.

Economic evaluation

The PICOS architecture v1 describes basic business functions, such as payment services or the integration of external services in general. In order to extend the economic potential of the PICOS architecture and to outweigh its lack to integrate third parties, like marketers or external service providers, certain key features have to be supplemented with economic aspects. Regarding Personalization, features for marketers and external service providers to get personal information, provided by community members, should be integrated. However it is important to develop methods how this will be done in a privacy-friendly way. The same counts for the search feature, which needs to be extended by marketing related mechanisms. Generally, it should also be reviewed on how to give the user transparency on the usage of his data (e.g. Privacy advisor). Similar applies for the Profile Management and the question on how the user can create and configure profiles for advertising. The principle of data minimization is protecting the user on the one hand, but affecting business applications depending on personal information. Goal of a second cycle PICOS Architecture should be to point out how PICOS is able to balance these controversial aspects.

The PICOS Platform Prototype v1 achieved the implementation of a set of capabilities around trust and privacy, without disabling business applications. To the contrary, current community platforms do not support such privacy features as multiple identities and privacy advisor. Particularly the implemented Profile and Policy Server are of special relevance when it comes to business applications under trust and privacy preserving conditions. To prove the PICOS Platforms capabilities and its applicability to business applications, an example implementation of an External Service should be done. Several suggestions have been made, e.g. the implementation of a payment service, the implementation of the PICOS Use Case 6, or content sensitive advertisements. The key question in

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

this endeavour will be how to integrate functionalities for marketers and external service providers while preserving the trust and privacy principles at the same time. The goal for the second cycle should be to find an implementation solution for the adapted Architecture & Design of PICOS on these controversial aspects.

The PICOS Angling Community Prototype v1 in its current state and its user centric view complies with the set of trust and privacy principles, but at the same time does not provide functionalities to make use of the social capital as value of the community. A concrete scenario is already described in PICOS Use Case 6, i.e. the voucher gratification for users earning reputation in a community. Context sensitive advertisements would be another example of implementation. The mentioned advertisement engine could gather anonymous cross-sectional data from the platform, which then is provided to the marketers in form of different target groups. Marketers can then adapt their advertisements and transfer them to the platform. The platform itself proceeds the matching with the users which are part of the target group and delivers the advertisement. But in this scenario the anonymous cross-sectional data collection might state an issue in regards to privacy policy agreements. Last but not least, the implemented search feature can be extended by marketing related mechanisms. In summary the client prototype holds some economic potential yet not accessed. Implementation of such features always has to be subject to the PICOS trust and privacy principles.

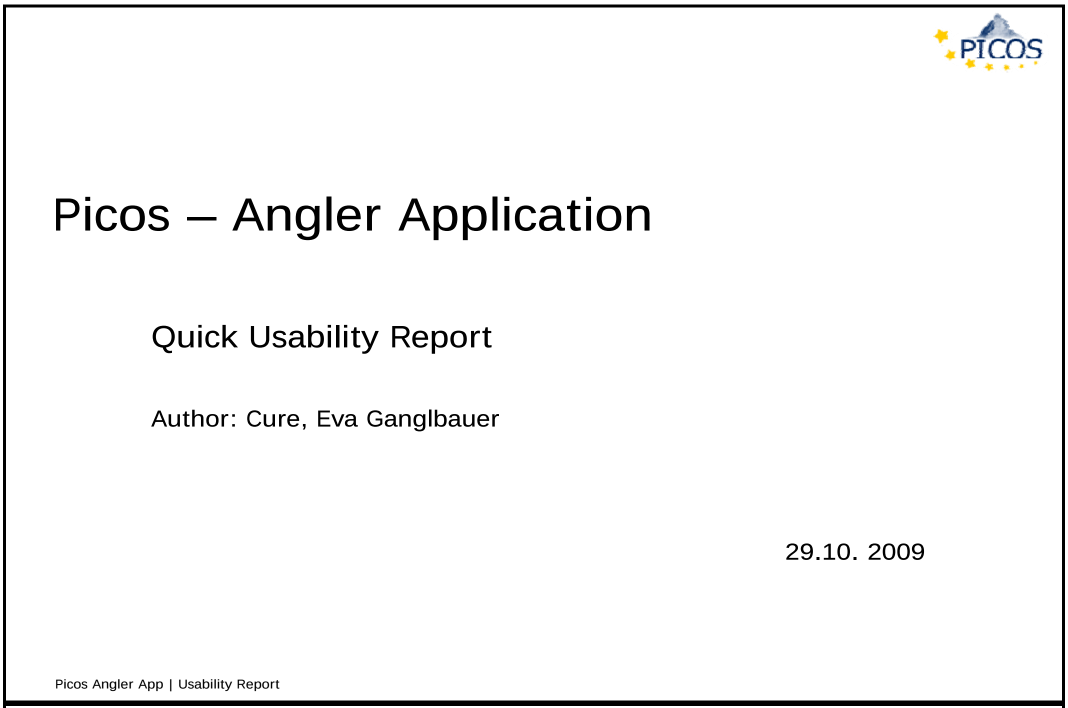
Usability evaluation

Participants in the PICOS Angling Community Prototype lab tests and field trials were critical regarding the PICOS PET concepts, which are naturally more difficult and complex to understand. Therefore well-designed and user-friendly implemented solutions are required to ensure that users can focus on the PICOS concepts. In summary, the concept of the private sub-community and the policy creator were rated very useful in qualitative statements. The results of the lab and field tests indicate very clearly, that usability is a prerequisite for the perception, understanding, comprehension and the usage of Picos PET concepts. All participants appreciated most of the PICOS PET concepts in general, but criticized that it was often confusing to use them in the angling application. Only if the PICOS PET concepts are presented well and the interactions on them are easy to carry out and support the mental model of them, users are going to understand and use these concepts.

Assurance evaluation

For reasons of completeness the main findings of the assurance evaluation, conducted in WP3, which were already discussed in chapter 2, are presented at this point. From the point of view of assurance, it is important that there is a clear alignment between the specifications of the WP4 architecture, the WP5 platform, and the WP6 prototypes. For instance, it should be possible to relate a component or functionality in the platform to a component or functionality in the architecture. It should also be possible to link elements of the architecture, e.g. features, components, or other functionality, to the requirements that justify their inclusion in the architecture. Also, in order to complete the evaluation of the WP5 platform, the functionality and internal interfaces of the platform components, functions and services must be provided and documented, not only their signature or external interfaces. It is also desirable that the system design should include an architecture-free description of a revised set of use cases with the purpose of establishing the main functional features of the system, rather than to validate the components. These use cases should thereafter guide the development of both the platform and the prototypes, thus staving off for the need for developers to make major decisions about their functionality. Finally, it must be stressed that good and consistent documentation of the architecture, platform and prototypes, is essential for assurance.

7 Appendix I



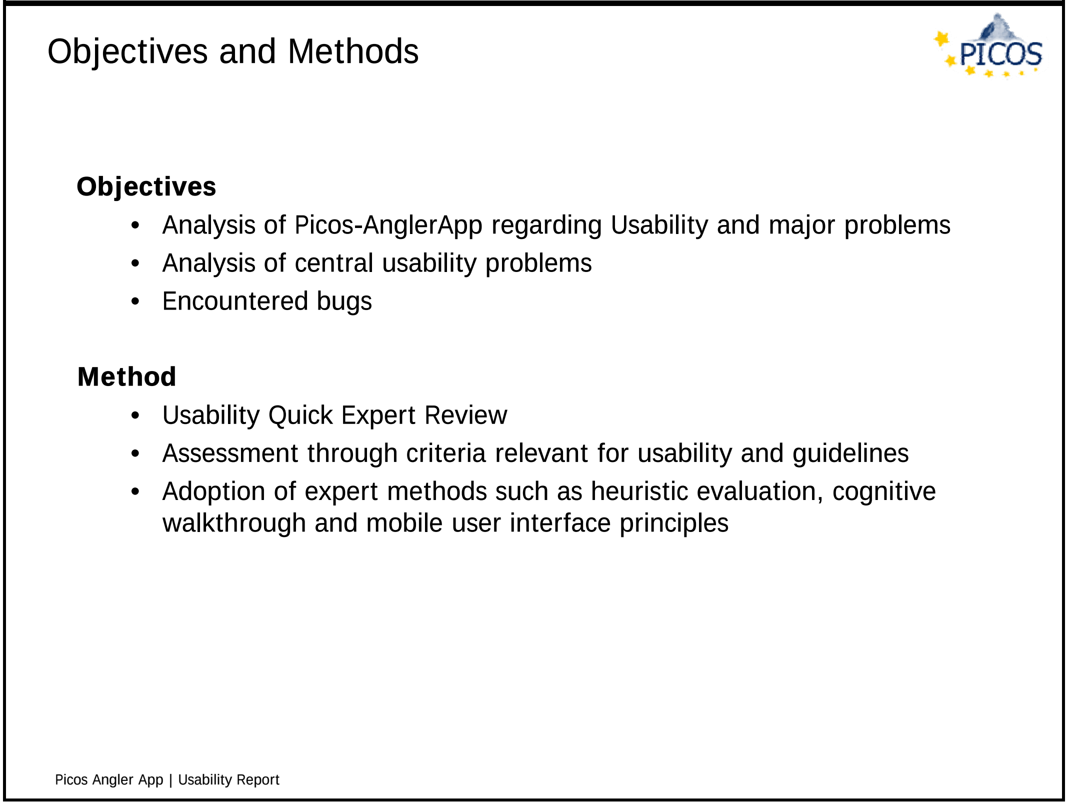
Picos – Angler Application

Quick Usability Report

Author: Cure, Eva Ganglbauer

29.10. 2009

Picos Angler App | Usability Report



Objectives and Methods

Objectives

- Analysis of Picos-AnglerApp regarding Usability and major problems
- Analysis of central usability problems
- Encountered bugs

Method

- Usability Quick Expert Review
- Assessment through criteria relevant for usability and guidelines
- Adoption of expert methods such as heuristic evaluation, cognitive walkthrough and mobile user interface principles

Picos Angler App | Usability Report

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

Executive Summary

Positive

- Focus on most important aspects
- Screens are complete
- Location based services

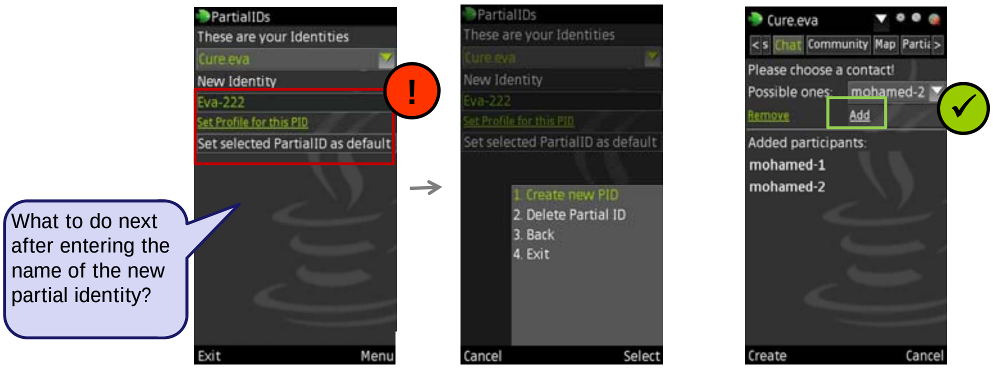
Potential to improve

- Consistency and logic behaviour from a users' view
- Findability of next steps and actions
- Layout and Style
- Functionality
- Wording
- Bugs

Picos Angler App | Usability Report

Findability of next steps

- The **next steps for user actions** are mostly **"hidden" in the context menu**. There is no instant feedback for a user how to proceed. Most important actions should be provided by a button or action-link.

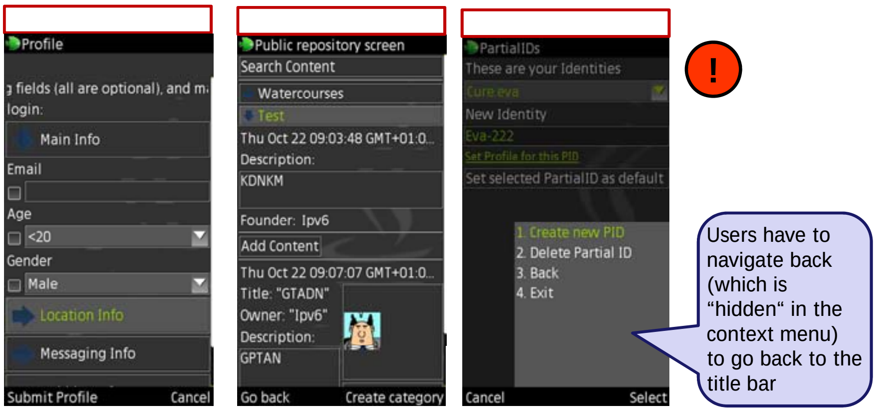


Picos Angler App | Usability Report

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

Navigation and Titles

- Some screens **don’t have a title bar**. The result is that users easily loose the focus and context where they are. The title bar should be provided on every screen to support orientation, findability and navigation.

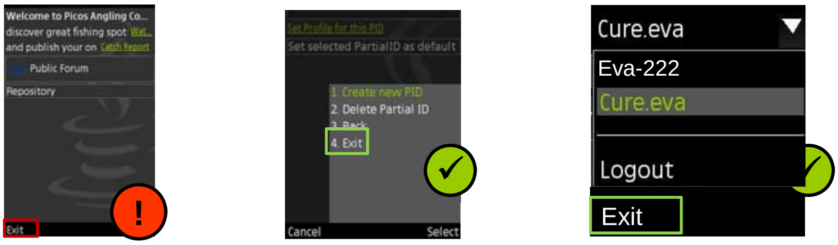


Users have to navigate back (which is “hidden“ in the context menu) to go back to the title bar

Context menu (1)

- “Menu” does not sound like to find many options for next steps in it. Consistently to the Nokia 5800 OS, **“Menu” should be called “Options”.**

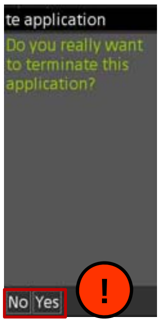
- **“Exit” is very prominent** and can be found on most screens, although only rarely needed by the user. Provide “Exit” only in the “Menu” respectively “Options” and include “Exit” in the title bar.

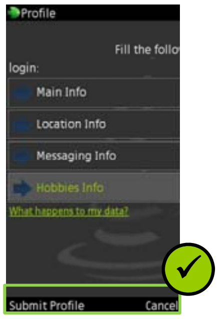


The PICOS project receives research funding from the Community’s Seventh Framework Programme.

Context menu (2)

- Most **probable options should always be on the left side**, e.g. “Ok”. Consistently to the Nokia 5800, concluding actions such as “Ok” should be on the left side of the Menu. Aborting Buttons such as “Cancel” should be on the very right side

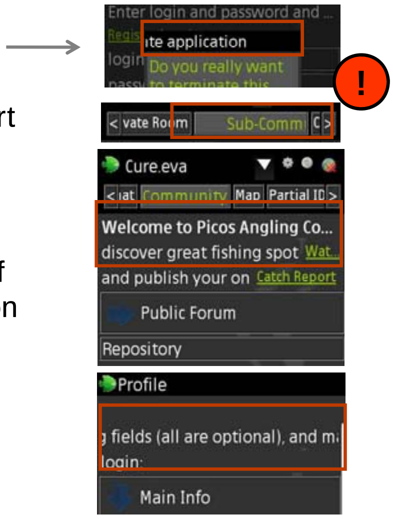




Picos Angler App | Usability Report

Movement of text over a small display window

- The continuous **movement of text over a small display window** (scrolling) is not well readable! If there is not enough space for the letters, start a second row.
- **Feedback** times are very long or feedback itself is often missing. Most of the time there is no feedback if a button was clicked (touched) and what is happening. Users need feedback (highlighting) to know if a button was clicked. Implement consistent button behaviour.

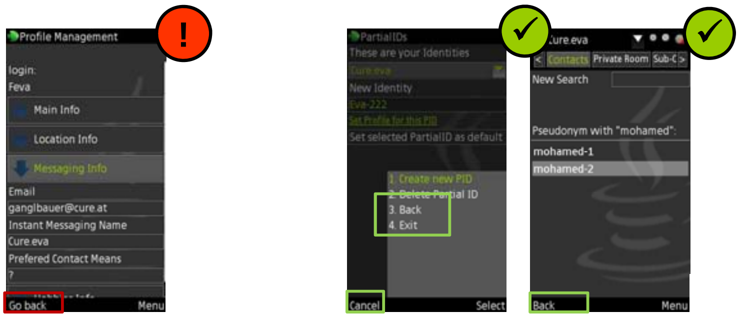

Enter login and password and ...
Regi
logi
passw
ite application
Do you really want to terminate this
!
< vate Room Sub-Comm C >
Cure.eva
< iat Community Map Partial ID >
Welcome to Picos Angling Co...
discover great fishing spot Wat...
and publish your on Catch Report
Public Forum
Repository
Profile
j fields (all are optional), and m
login:
Main Info

Picos Angler App | Usability Report

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

“Back” in the context menu

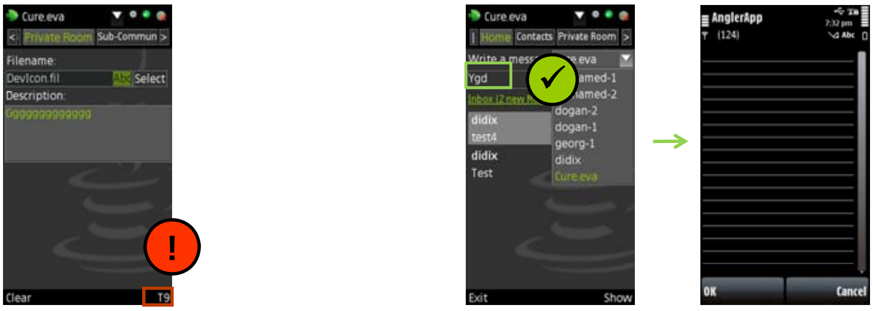
- **“Back”** or **“Go back”** are **not consistently used**. “Back” should always be the default option on the left side for screens where Back-navigation is necessary, except for dialogs where “Cancel” should be used.



Picos Angler App | Usability Report

Text input

- **Clicking “T9” before entering text**: It’s very cumbersome to have to touch “T9” in the right bottom corner before entering text, if the user can find it at all! It’s better to enable **direct manipulation** for users and provide entering of text directly after clicking on a field for text input.

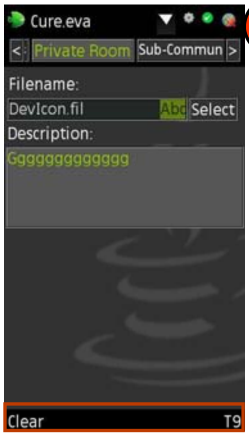


Picos Angler App | Usability Report

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

Dead end of interaction process

- There is **no possibility for the user to proceed** and to upload the file to the diary. Users need the possibility to finish intended actions, in this case browsing, choosing and also uploading a file.

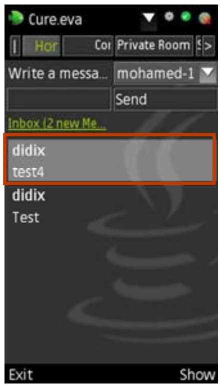


Filename: DevIcon.fil

Description: Ggggggggggg

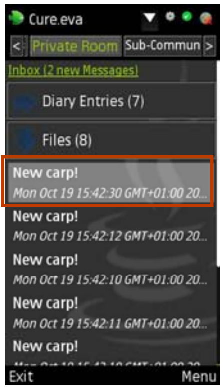
Link to item if clicked (touched)

- Users expect that they can see a **detailed view of an element if they click** (touch) it. It's cumbersome for users if they have to click "show" before being able to view an object. It's more intuitive to directly link to a detailed view with further options after a click.



didix
test4

didix
Test



New carp!
Mon Oct 19 15:42:30 GMT+01:00 20...

New carp!
Mon Oct 19 15:42:12 GMT+01:00 20...

New carp!
Mon Oct 19 15:42:10 GMT+01:00 20...

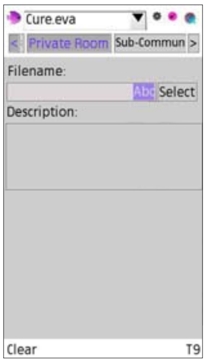
New carp!
Mon Oct 19 15:42:11 GMT+01:00 20...

New carp!

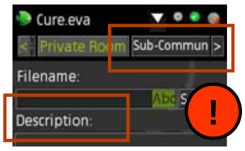
The PICOS project receives research funding from the Community's Seventh Framework Programme.

Style (1)

- **White background with black font** is more readable (inverted picture)



- **Text size in the title bar is not different from normal text**, it is sometimes even smaller than standard text.

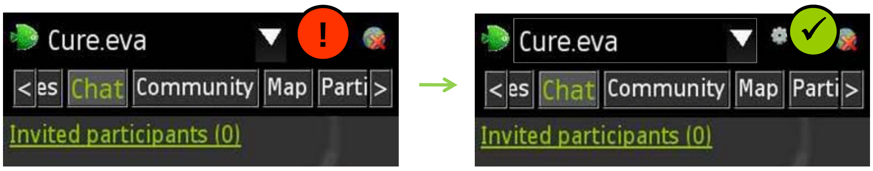


- There are **no icons in the application** except in the title bar

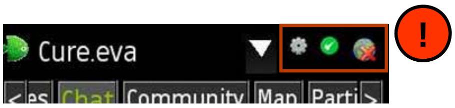
Picos Angler App | Usability Report

Style (2)

- The **drop list should be shown as one element**



- **Icons are very small**, there is still space to make them bigger to enhance visibility and clickability if the drop list element is decreased in length.

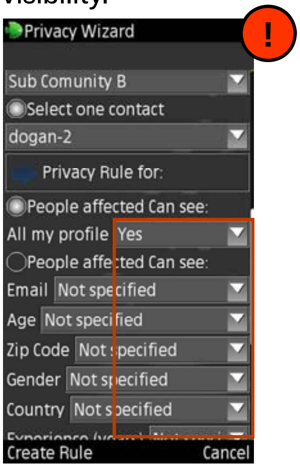


Picos Angler App | Usability Report

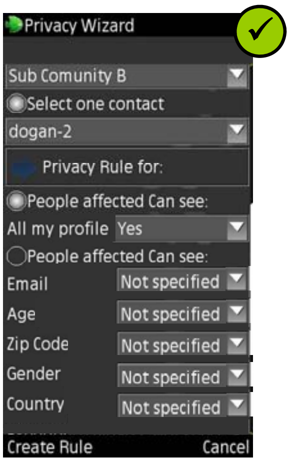
The PICOS project receives research funding from the Community's Seventh Framework Programme.

Style (3)

- For better readability, use a **grid to arrange fields**. Also white space or negative space helps to group elements and enhance visibility.



Sub Comunity B
○ Select one contact
dogan-2
Privacy Rule for:
○ People affected Can see:
All my profile Yes
○ People affected Can see:
Email Not specified
Age Not specified
Zip Code Not specified
Gender Not specified
Country Not specified

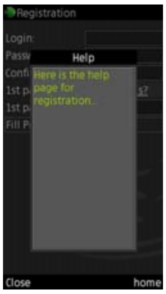


Sub Comunity B
○ Select one contact
dogan-2
Privacy Rule for:
○ People affected Can see:
All my profile Yes
○ People affected Can see:
Email Not specified
Age Not specified
Zip Code Not specified
Gender Not specified
Country Not specified

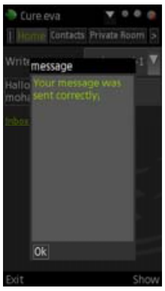
Picos Angler App | Usability Report

Missing text or special wording

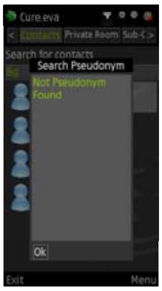
- The **text** for “New Policy”, “What is this” help page for explanation of partial ID and “What happens to my data” on the register page **is missing.**
- The **wording** of partial Identity, “Private Room” and “Sub-Community” can’t be understood without explanation (a colleague tried the application and didn’t realize what these concepts could mean)
- **Error messages** should be communicated well!



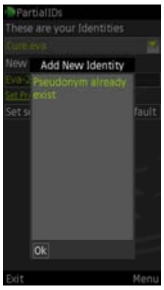
Here is the help page for registration..



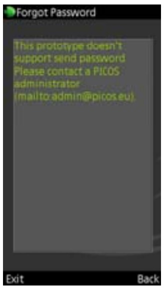
Your message was sent correctly.



Not Pseudonym Found



Pseudonym already exist



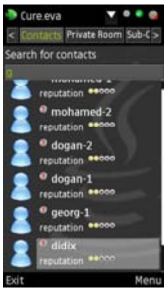
This prototype doesn't support send password Please contact a PICOS administrator (mailto:admin@picos.eu).

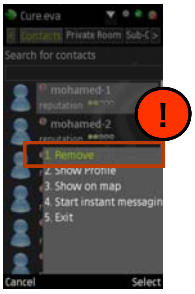
Picos Angler App | Usability Report

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

Contacts (1)

- Search: There is **no search button**. Users are linked automatically when they entered the search text. In general this is desired, but in this case users may have the feeling of loosing control. It's better to add a search button to let users control when they want to search and when not.
- There are **no contact requests sent**. This implies that users can see all profiles of other users, which is not privacy friendly.
- It's **not possible to write a message** to a contact from the context menu. Include this option to provide functionalities in more than one place.
- Why is **no presence status** for contacts available?

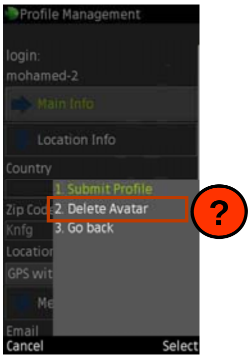




Picos Angler App | Usability Report

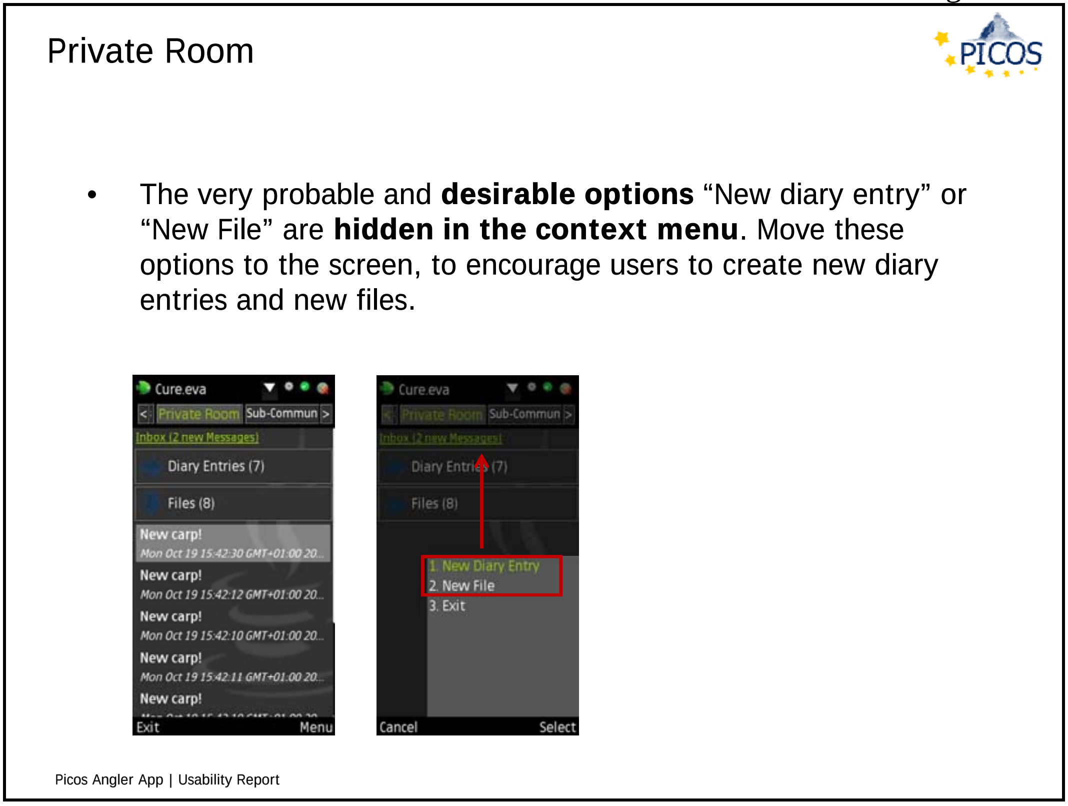
Contacts (2)

- A user can **edit the profile of another contact** – is this a feature or a bug?
- A user is able to **delete an avatar** – where can s/he add it? Creating a profile for a pID does not provide this option.



Picos Angler App | Usability Report

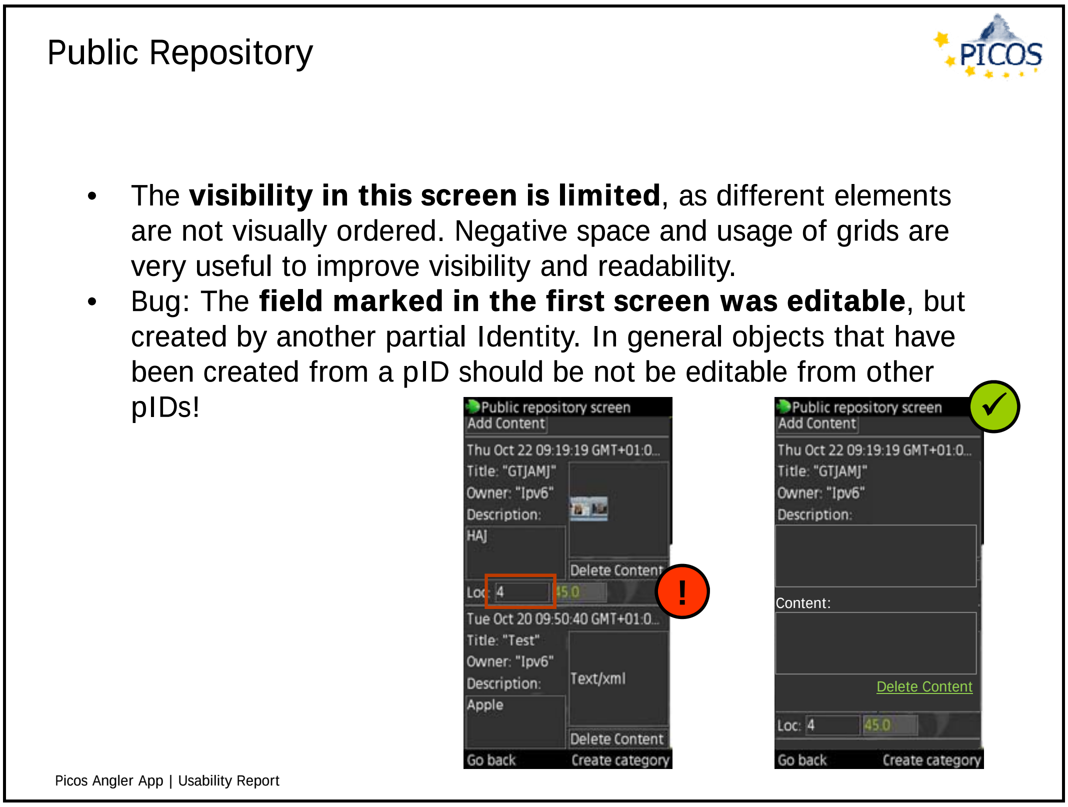
The PICOS project receives research funding from the Community's Seventh Framework Programme.



Private Room

- The very probable and **desirable options** “New diary entry” or “New File” are **hidden in the context menu**. Move these options to the screen, to encourage users to create new diary entries and new files.

Picos Angler App | Usability Report



Public Repository

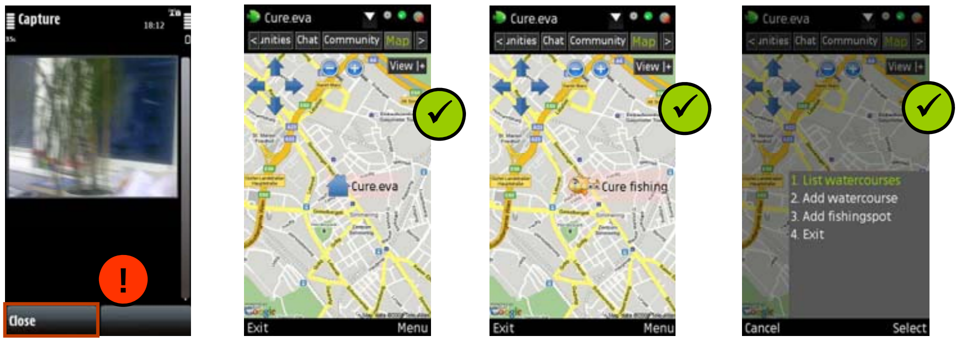
- The **visibility in this screen is limited**, as different elements are not visually ordered. Negative space and usage of grids are very useful to improve visibility and readability.
- Bug: The **field marked in the first screen was editable**, but created by another partial Identity. In general objects that have been created from a pID should be not be editable from other pIDs!

Picos Angler App | Usability Report

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

Map

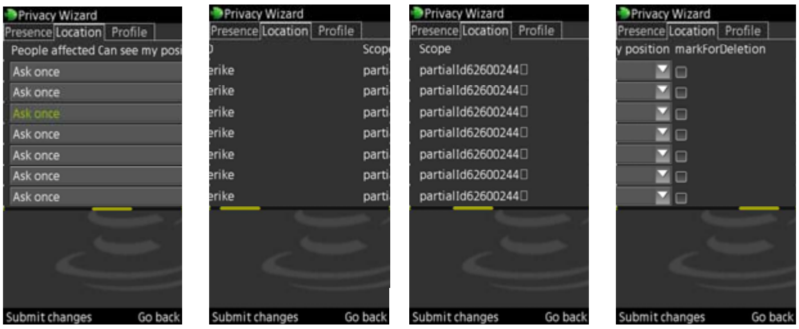
- Create new fishingspot
  - Taking a picture for fishing spot: option **“Close” should be exchanged with “Take photo”** for users to understand.
- In general **usability for LBS is good.**



Picos Angler App | Usability Report

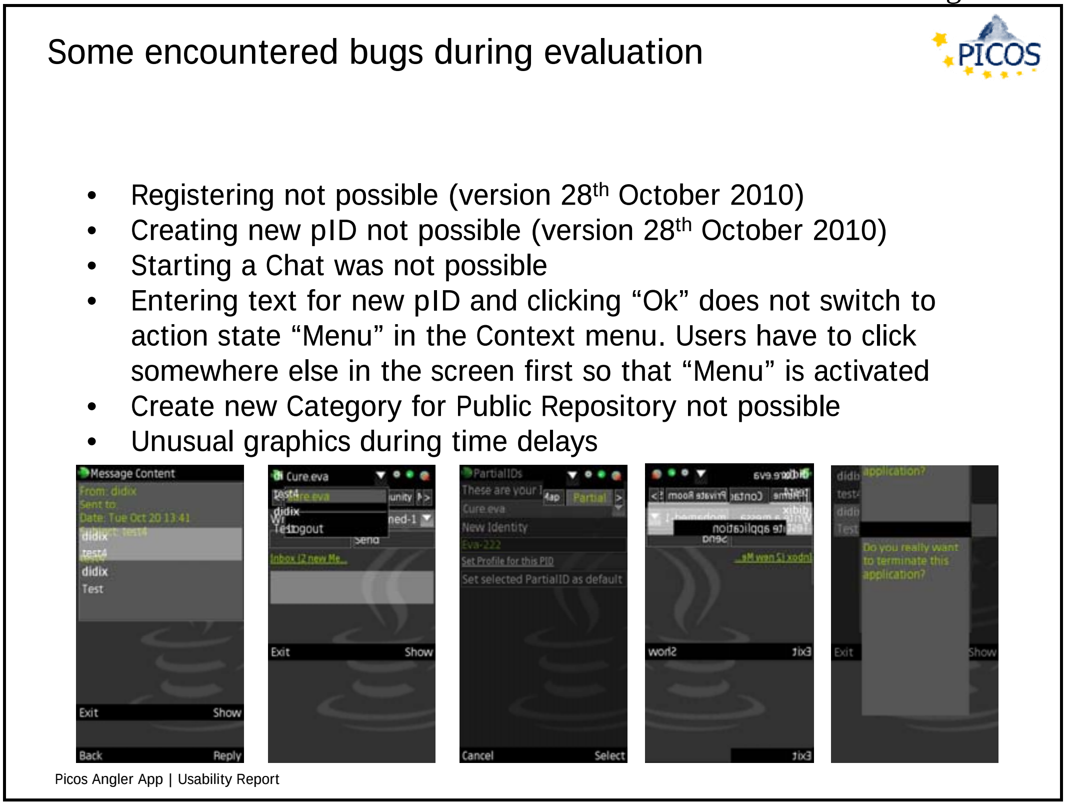
Policy editor

- The **area for displaying the information is broader than the window**. In general, **horizontal scrolling should be avoided**. Use expandable Buttons and more rows for each element. Scale down elements and the space between them to enhance visibility and readability.


Privacy Wizard
Presence Location Profile
People affected Can see my posi
Ask once
Scope
erike
parti
partialId62600244□
y position markForDeletion
Submit changes
Go back

Picos Angler App | Usability Report

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



Some encountered bugs during evaluation

- Registering not possible (version 28th October 2010)
- Creating new pID not possible (version 28th October 2010)
- Starting a Chat was not possible
- Entering text for new pID and clicking “Ok” does not switch to action state “Menu” in the Context menu. Users have to click somewhere else in the screen first so that “Menu” is activated
- Create new Category for Public Repository not possible
- Unusual graphics during time delays

Picos Angler App | Usability Report

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