



*Title:* ***D3.3.2 Trust and Privacy Assurance of the Community Prototype v2***

*Editors:* ***José Luis Vivas & Isaac Agudo (University of Malaga)***

*Contributors:* ***José Luis Vivas & Isaac Agudo, University of Malaga (UMA), María Rosa Vieira Álvarez (ATOS)***

*Reviewers:* ***Elsa Prieto (ATOS), Georg Kramer (DTAG)***

*Identifier:* ***D3.3.2***

*Type:* ***Deliverable***

*Version:* ***1.0***

*Date:* ***15/1/2011***

*Status:* ***Final version***

*Class:* ***Public***

## Summary

This deliverable provides an evaluation of the PICOS community application prototype. The main focus has been the detection of non-conformances in the specification and implementation of the prototype with respect to the established privacy and trust principles. The specification and implementation of the PICOS community prototype 2 have been assessed with regard to a set of the initial trust and privacy requirements. We provide here both a revision of the findings established in D3.3.1, and an analysis of threats, risks and vulnerabilities concerning trust and privacy in the PICOS community application prototype 2. The threat analysis performed was based on the threats and recommendations presented in a series of ENISA publications that relate to online social networks.



Grant Agreement no. 215056

## Members of the PICOS consortium:

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

## The PICOS Deliverable Series

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

D2.1 Taxonomy	July 2008
D2.2 Categorisation of Communities	July 2008
D2.3 Contextual Framework	November 2008
D2.4 Requirements	November 2008
D3.1.1 Trust and Privacy Assurance for the Platform Design	April 2009
D3.2.1 Trust and Privacy Assurance of the Platform Prototype	November 2009
D3.3.1 Trust and Privacy Assurance of the Community Prototype	January 2010
D3.4.1 A summary of PICOS WP3 sub-phase 3.1 deliverables	August 2010
D4.1 Platform Architecture and Design v1	March 2009
D4.2 Platform Architecture and Design 2	September 2010
D5.1 Platform description document v1	October 2009

---

Copyright © 2008-2010 by the PICOS consortium - All rights reserved.

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



Grant Agreement no. 215056

D5.2a Platform prototype 2a	May 2010
D6.1 Community Application Prototype 1	December 2009
D6.2a Community application prototype 2	April 2010
D6.2b Second Community Application Prototype 2	October 2010
D7.1a Trial Design Document	December 2009
D7.1b Trial plan for the second community prototype	September 2010
D7.2a First Community Prototype: Lab and Field Test Report	February 2010
D7.2b First Community Prototype: Field Trial Report	August 2010
D8.1 Legal, economic and technical evaluation of the first platform and community prototype	April 2010
D9.1 Web Presence	February 2008
D9.2.1 Exploitation Planning	April 2009
D9.2.2 Exploitation Plan 2	March 2010
D9.3.1 Dissemination Planning	April 2009
D9.3.2 Dissemination Report V2	March 2010



## The PICOS Deliverable Series

### Vision and Objectives of PICOS

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

### Planned PICOS documentation

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

### PICOS results

- *PICOS Foundation* for the technical work in PICOS is built by the categorization of communities, a common taxonomy, requirements, and a contextual framework for the 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 leisure and business communities;
- *Community Application Prototype* is built and used to validate the concepts of the platform architecture and design and their acceptability by covering scenarios of private and professional communities;
- *PICOS Trials* validate the acceptability of the PICOS concepts and approach chosen from the end-user point of view;
- *PICOS Evaluations* assess the prototypes from a technical, legal and social-economic perspective and result in conclusions and policy recommendations;

*PICOS-related scientific publications* produced within the scope of the project.



## Charter

### Objectives

Assurance must be an integral constituent of the PICOS solution, and we do believe that it should be pursued in a holistic manner. For this reason, in this WP we adopt a holistic approach emphasizing the relation between the parts and the whole. WP3 gives input to the implementation of the PICOS prototype with respect to privacy and trust by providing an assurance evaluation of the design and its documentation in both sub-phases 3.1 and 3.2 of the project

For this reason, each of the deliverables of this WP will be produced according to the partial results of the project in sub-phase 3.1, and later reviewed, updated and extended in sub-phase 3.2, in order to accommodate to the outcome of the different sub-phases of Phase 3 and to fairly reflect the assurance results as the project evolves.

### Description of work - Task 3.3 Evaluation of Community Prototype

Assessment of the community prototypes will take place according to the principles defined in the user evaluation plan. Therefore we will be able to evaluate the usability, efficiency, and effectiveness of the systems as well as the development of different user experience factors over time. The user evaluation will be based on experience with the prototyped interfaces and ensure the quality of the interface of the system. The results will be summarized in the Evaluation Reports for community prototypes 1 and 2. User trust assurance will be compared against established criteria, i.e. privacy or security seals for e-commerce. We will assess non-commercial prototypes, commercial prototypes and mixed-type prototypes, producing two versions of deliverable D3.3.



Grant Agreement no. 215056

## Foreword

Deliverable D3.3.2 is a collective work by the WP3 Assurance team, whose members are listed below. A substantial part of the work involved applying the assurance methodology described in D3.1.1 and D3.4.1. Please take a look at D3.4.1 for a description of the methodology.

With thanks to the PICOS WP3 Assurance Team.

### **The Assurance Team**

GUF, UMA, ATOS, BRNO

*Editors: Jose Luis Vivas & Isaac Agudo, University of Malaga, ES (UMA)*

*Contributors: José Luis Vivas & Isaac Agudo, University of Malaga (UMA), María Rosa Vieira Álvarez (ATOS)*



## Table of Contents

Summary .....	1
Members of the PICOS consortium: .....	2
The PICOS Deliverable Series.....	2
Vision and Objectives of PICOS.....	4
<b>1 Introduction .....</b>	<b>11</b>
<b>2 Revision of D3.3.1 .....</b>	<b>13</b>
<i>PrP01: Notice of collection</i> .....	<i>13</i>
2.1.1 Use Case 1: Registration.....	13
<i>PrP10: Fair and Lawful Means</i> .....	<i>13</i>
2.1.2 Use Case 1: Registration.....	13
2.1.3 Use Case 4: Multiple Partial Identities .....	14
<i>PrP13: Third-party Disclosure</i> .....	<i>14</i>
2.1.4 Use Case 2: Accessing the Community .....	14
2.1.5 Use Case 6: External Services .....	14
2.1.6 Use case 7: Content Sharing .....	14
2.1.7 Use case 9: Sub-Community .....	15
<i>PrP18: Safeguards</i> .....	<i>15</i>
2.1.8 Use Case 1: Registration.....	15
<i>PrP21: Data Management</i> .....	<i>15</i>
2.1.9 Use Case 1: Registration.....	15
2.1.10 Use Case 4: Multiple Partial Identities .....	16
2.1.11 Use Case 6: External Services .....	16
2.1.12 Use Case 7: Content sharing.....	16
2.1.13 Use Case 9: Sub-community .....	16
<i>PrP22: End-to-end Privacy</i> .....	<i>16</i>
<i>PrP23: Authentication</i> .....	<i>17</i>
2.1.14 Use Case 1: Registration.....	17
2.1.15 Use Case 2: Accessing the community .....	17
2.1.16 Use Case 4: Multiple partial identities.....	17
2.1.17 Use Case 7: Content sharing.....	17
<i>PrP24: Multiple Persona</i> .....	<i>17</i>
2.1.18 Use Case 1: Registration.....	18
2.1.19 Use Case 2. Accessing the Community .....	18
2.1.20 Use Case 3: Revocation .....	18
2.1.21 Use Case 4: Multiple Partial identities .....	18



2.1.22	Use Case 5 Reputation.....	18
2.1.23	Use Case 6: External Services .....	18
2.1.24	Use Case 7: Content Sharing .....	19
2.1.25	Use Case 8: Presence.....	19
2.1.26	Use Case 9: Sub-community .....	19
	<b>TrP03: Provenance .....</b>	<b>19</b>
2.1.27	Use Case 5. Reputation.....	20
2.1.28	Use Case 6. External Services .....	20
2.1.29	Use Case 7. Content Sharing .....	20
	<b>TrP05: Audit .....</b>	<b>20</b>
	<b>TrP06: Objective/Subjective Trust.....</b>	<b>20</b>
2.1.30	Use Case 4. Multiple Partial Identities .....	21
2.1.31	Use Case 5. Reputation.....	21
2.1.32	Use Case 6. External Services .....	21
2.1.33	Use Case 7. Content Sharing .....	21
	<b>TrP07: Consensus.....</b>	<b>21</b>
2.1.34	Use Case 9. Sub-community.....	21
	<b>TrP08: Accountability.....</b>	<b>22</b>
2.1.35	Use Case 1. Registration.....	22
2.1.36	Use Case 4. Partial Identities .....	22
2.1.37	Use Case 7. Content Sharing .....	22
<b>3</b>	<b>Threat Analysis.....</b>	<b>23</b>
	<b>Safeguards.....</b>	<b>23</b>
3.1.1	Unauthorized access to personal information .....	23
3.1.2	Identity theft (impersonation).....	24
3.1.3	Information Aggregation concerning partial identities .....	24
3.1.4	Information Storage Vulnerabilities .....	24
3.1.5	Information Transmission Vulnerabilities .....	25
3.1.6	Information Collection Vulnerabilities .....	25
3.1.7	Session vulnerabilities .....	25
	<b>Threat analysis and recommendations for security.....</b>	<b>26</b>
3.1.8	Digital dossier aggregation .....	26
3.1.9	Secondary data collection .....	27
3.1.10	Linkability from image metadata.....	27
3.1.11	Account deletion.....	27
3.1.12	Spam.....	28
3.1.13	Cross site scripting, viruses and worms.....	28
3.1.14	Contextual Information.....	28
3.1.15	Stronger authentication.....	28
3.1.16	Abuse reporting .....	29
3.1.17	Default settings.....	29
3.1.18	Data deletion.....	30
3.1.19	Reputation techniques.....	30
3.1.20	Filters.....	30
3.1.21	Profile tags.....	31
3.1.22	Spidering and bulk downloads.....	31
3.1.23	Eliminating spam.....	31
3.1.24	Phishing .....	32
	<b>Trust principles: Reputation.....</b>	<b>32</b>



Grant Agreement no. 215056

3.1.25Threats .....	32
3.1.26Security.....	33
3.1.27Recommendations .....	36
<b>4 Conclusions .....</b>	<b>38</b>
<i>References</i> .....	<i>40</i>
<b>Appendix A Reports consulted .....</b>	<b>41</b>



## List of acronyms

<i>CA</i>	<i>Client Application</i>
<i>Dx.y.z</i>	<i>[PICOS] Deliverable: Work Package x, Deliverable y, Cycle z</i>
<i>ENISA</i>	<i>European Network and Information Security Agency</i>
<i>HTML</i>	<i>HyperText Markup Language</i>
<i>HTTPS</i>	<i>Hypertext Transfer Protocol Secure</i>
<i>ID</i>	<i>Identity (also Identifier)</i>
<i>IP</i>	<i>Internet Protocol</i>
<i>J2ME</i>	<i>Java 2 Micro Edition</i>
<i>PICOS</i>	<i>Privacy and Identity Management for Community Services</i>
<i>PID</i>	<i>Partial Identity (also Identifier)</i>
<i>PP</i>	<i>PICOS Principle</i>
<i>PrP</i>	<i>Privacy Principle</i>
<i>POI</i>	<i>Points of Interest</i>
<i>PUC</i>	<i>PICOS Use Case</i>
<i>SSL</i>	<i>Secure Sockets Layer</i>
<i>SNSs</i>	<i>Social Networking Sites</i>
<i>TrP</i>	<i>Trust Principle</i>
<i>WPn</i>	<i>Work Package number n</i>
<i>XSS</i>	<i>Cross-site Scripting</i>



# 1 Introduction

Continuing and complementing the assurance evaluation of the PICOS prototypes performed in the first cycle of the project, and presented in deliverable D3.3.1 [D3.3.1], for the second phase we concentrate on both a revision of the findings established in D3.3.1, and further on an analysis of threats, risks and vulnerabilities concerning trust and privacy in the PICOS community application prototype v2. Both the First Community Application Prototype 2 [D6.2a] and the Second Community Application Prototype 2 [D6.2b] are treated here. Since from the point of view of privacy and trust these two applications do not show any important differences, we evaluated them together, and the results obtained here are valid for both applications; however, whenever a comment refers only to one of the applications we will indicate it.

The threat analysis performed was based on the threats and recommendations presented in several ENISA papers published by ENISA (European Network and Information Security Agency). The first one, *Security Issues and Recommendations for Online Social Networks*, outlines the most important threats to users and providers of Social Networking Sites (SNSs), and offers policy and technical recommendations to address them. The second, *Reputation-based Systems: a security analysis*, explains the main characteristics of electronic reputation systems and the security-related benefits they can bring, and puts forward the main threats and attacks against reputation systems, as well as the security requirements for system design. A set of core recommendations for best practices in the use of reputation systems is also presented. A third paper, *Online as soon as it happens*, is a white paper providing a set of recommendations for raising the awareness of SNS users of the risks and threats against SNSs.

Based on the results from the first cycle assurance deliverables, D3.1.1, D3.2.1 and D3.3.1, the assurance work for the second cycle focused mainly on a subset of the trust and privacy principles. These should include the following:

- PrP01: Notice of collection
- PrP10: Fair and lawful Means
- PrP13: Third-party Disclosure
- PrP18: Safeguards
- PrP21: Data Management
- PrP22: End-to-end Privacy
- PrP23: Authentication
- PrP24: Multiple Persona
- TrP03: Provenance
- TrP05: Audit
- TrP06: Objective/Subjective Trust
- TrP07: Consensus
- TrP08: Accountability

The remaining principles (see D3.4.1 Appendix B for a complete list) might be treated more briefly, either because they are considered to have already been taken into account in a satisfactory way in the first cycle, or because they are regarded to be not very relevant for the PICOS applications (see D3.1.2



Grant Agreement no. 215056

for more details). The principle PrP18 Safeguards is particularly important at this stage, and a section below is dedicated to it.

The rest of this deliverable is organised as follows. Chapter 2 is dedicated to presenting the results of the analysis of the second cycle prototypes (the second prototype of the Angling community and the first prototype of the Gaming community). In Chapter 3 we present the results of the threat analysis. Finally Chapter 4 presents the conclusions.



## 2 Revision of D3.3.1

For the second version of the PICOS platform prototype, we present below an analysis of each of the principles listed in Chapter 1, always in the context of each relevant use case, as established in D3.1.1.

A subsection is dedicated to each analysed principle; we start each subsection by providing the definition of the corresponding principle (**Def.:**), eventually followed by commentaries summing up results or giving some background information, and also by a list of use cases that are relevant to the principle; thereafter a subsection is dedicated to each one of those use cases.

### PrP01: Notice of collection

**Def.:** Notice is provided to the Data Subject of the purpose for collecting personal information and the type of data collected.

**Use Cases: 1.**

#### 2.1.1 Use Case 1: Registration

A requirement here is that notice of the purpose of collection should be provided before any data collection during registration.

In the prototypes, the community terms and conditions are used to 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 inspection.

### PrP10: Fair and Lawful Means

**Def:** Information must be collected by fair and lawful means.

The PICOS prototypes clearly enforce this principle, as is shown below.

**Use Cases: 1, 4.**

#### 2.1.2 Use Case 1: Registration

PrP10 is enforced in PICOS prototype during the registration process in the community by notification of terms and conditions and informed consent.



### 2.1.3 Use Case 4: Multiple Partial Identities

Collection of profile data during creation of new partial identities must not involve collection of personal information, as this would contradict the principle PrP10. Therefore it would not be appropriate to collect personal data during the creation of a partial identity. The prototype does not request any form of mandatory personal information during the creation of partial identities profiles. However, during partial ID creation the user would fill out the associated partial ID profile, entering some data such as personal information (family name), location information (city, street name), messaging information and hobbies information. If the user is not notified about it, this fact could represent a way of gathering information by unfair means. This vulnerability was admitted in the Gamers prototype in order to enhance the functionality of the privacy advisor, which in this way might be able to check additional profile attributes in certain content types (Category content, forum-thread contributions, plain text files attached to posts, chat and asynchronous messages) and therefore send the user a warning whenever new content is inserted by the user which contains some of this profile information.

## PrP13: Third-party Disclosure

**Def.:** Notice and Consent of the Data Subject is required to disclose information to third parties.

It is a requirement that the PICOS architecture must uphold the member's wishes with regard to information flow.

We note here that no user data is disclosed outside the community. Within the community the disclosure is managed by the end user via the creation of privacy rules.

**Use Cases:** 2, 6, 7, 9.

### 2.1.4 Use Case 2: Accessing the Community

In this prototype no disclosure of personal information to external third-parties takes place (unless by exploitation of some vulnerability)

### 2.1.5 Use Case 6: External Services

Not relevant to this version of the community prototype since external services are absent.

### 2.1.6 Use case 7: Content Sharing

The principle is not applicable here since content sharing is not supposed to involve personal information.



### 2.1.7 Use case 9: Sub-Community

Sub-community profiles are not intended to involve personal information.

## PrP18: Safeguards

**Def.:** Organizations must be sure to include safeguards to prevent loss, misuse, unauthorized access, disclosure, alteration and destruction of data.

**Use cases: 1.**

### 2.1.8 Use Case 1: Registration

SSL (HTTPS) is used here, a protocol in widespread use today for securing internet transactions that do not require client authentication. In the PICOS community prototypes, all terminals and access are declared to be controlled in the user trials, so no further client authentication was deemed necessary.

## PrP21: Data Management

**Def.:** PICOS must allow members to express how to store and process their data and uphold their wishes in this regard.

We note here that the gamers community provides an additional scanning of the privacy information (part of the identity profile) included in the transmitted content. In the gamers prototype the Privacy Advisor scans the following data: locality, street name, phone numbers, zip code, email, address and the family name. It sends thereafter a notification to the end-user in case he has entered some of these data in a post or within a chat.

**Use Cases: 1, 4, 6, 7, 9.**

### 2.1.9 Use Case 1: Registration

Members must be allowed 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. This is provided by the Profile Manager. By default the PICOS prototype (client and platform) hides all personal data to other users.



### 2.1.10 Use Case 4: Multiple Partial Identities

Members must be allowed to set their preferences for sharing partial identity profile information during the creation of a partial identity, and uphold their wishes with respect to storage and processing of this data. By clicking on the “*set profile*” button the user is able to edit the information in their profiles. In order to manage the privacy rules for their profiles, users may follow the procedures described for the Policy Manager.

### 2.1.11 Use Case 6: External Services

It is required that content data may only be processed by external services if agreed by the member. This is trivially the case here since there are no external services.

### 2.1.12 Use Case 7: Content sharing

It is required that members must be able to express how imported content can be processed, and their view in this regard must be upheld.

Chats can be stored in the new version of the prototype, posts in forums cannot be removed or edited.

Users are able to set rights on the privacy-sensitive elements of partial identity profiles, presence and location. The platform establishes some general rules on content for forums since only the forum administrator can delete a forum/thread, and only the administrator or content owner can delete contributions (posts). Similarly, only the content owner can delete repository content.

### 2.1.13 Use Case 9: Sub-community

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. This requirement is not contradicted in the prototype. Moreover, the description of private sub-communities is only shown to invited members.

## PrP22: End-to-end Privacy

**Def.:** PICOS supports end-to-end privacy.

**Use cases:** none.

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



## PrP23: Authentication

Def.: PICOS supports multiple forms of Member authentication, while continuing to respect privacy.

The prototypes support only one way of authentication, since currently only one has been implemented in the platform.

Use cases: 1, 2, 4, 7.

### 2.1.14 Use Case 1: Registration

Authentication information has to be either collected or generated during registration. This is done in the the registration use case.

### 2.1.15 Use Case 2: Accessing the community

This is a crucial aspect of accessing the community. The second prototype, as the first one, supports only authentication by username/password. Thereafter, a session token is used by the CA to reconnect transparently to the user.

### 2.1.16 Use Case 4: Multiple partial identities

According to the initial requirements, every partial identity could have different means of authentication. This functionality, however, has not been implemented in the current version of the platform, and hence neither in the community applications.

### 2.1.17 Use Case 7: Content sharing

The requirement here is that members must authenticate in order to import content, which must be associated with them. Their privacy should be respected by allowing them to use a partial identity. Moreover, it must not be possible for a member or partial identity to associate imported content to another member or another member's partial identity.

## PrP24: Multiple Persona

Def.: PICOS allows members to have multiple persona.

Use cases: all.



### 2.1.18 Use Case 1: Registration

During registration the first partial identity is created. Further partial identities can be created later.

### 2.1.19 Use Case 2. Accessing the Community

Members can select any of their partial identities to access the community and its services. Access to the platform is performed using the root identity. The user can specify a default partial identity that will thereafter be set automatically after any successful login. The default partial identity can be changed at any time [D6.1 2.2.8].

### 2.1.20 Use Case 3: Revocation

Only the user may be revoked in the platform prototype. The revocation is also reflected in the client by means of the label “anonymous” appearing in content published by the revoked account.

### 2.1.21 Use Case 4: Multiple Partial identities

This requirement establishes that end users should be able to create as much partial identities as they wish. By choosing “*Create New Identity*” from the “*Options*” box or from the screen, the user may create as many partial identities as desired.

### 2.1.22 Use Case 5 Reputation

Member reputation information is linked to the partial identity of the user, whose reputation is derived from the ratings of contributed content. A history of the ratings is made available to other members. The reputations of distinct partial identities are independent. Each public sub-community has also a Reputation Level. For the first prototype as well as for the gamers prototype, the level is the mean value of the reputation levels attached to each partial identity in the the sub-community. Reputation has no changes from the first prototype.

It is important to note here that a partial identity belonging to a user cannot rate content contributed by the other partial identities of the user.

### 2.1.23 Use Case 6: External Services

No user data is disclosed outside the community. Within the community the disclosure of information is managed by the end user via the privacy rules.



### 2.1.24 Use Case 7: Content Sharing

Content data is linked to a partial identity of the user, who imported the data. The principle is thus enforced. Members must authenticate in order to import content, which must be associated with him or her, and their privacy should be respected by allowing them to use a partial identity.

### 2.1.25 Use Case 8: Presence

The different partial identities of a user can be associated to different presence and location status. This has been implemented in order to prevent the linkability of different partial identities of a user. If only the active partial identity is shown as online, when a user switches from one to another partial identity, another member might be able to see how the old active partial identity shifts to offline at the same time that the new active partial identity shifts to online. By keeping the status of the partial identity as “online” for some random amount of time after going offline, this kind of linkability might be avoided.

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 his or her profile.

### 2.1.26 Use Case 9: Sub-community

In the prototype, the member of a sub-community is a partial identity. However, only one partial identity of a given user is allowed per sub-community. This constraint might yield some information useful for linking partial identities, for instance by observing that two partial identities are never members in the same sub-community at the same time; moreover, a malicious member might even invite a partial identity to a sub-community in order to check if he is able to become a member in this sub-community, suspecting that the root identity of the invited partial identity is the same as that of another partial identity which already is a member in the sub-community.

## TrP03: Provenance

Def.: PICOS ensures that members can rely on the provenance of information.

Use cases: 5, 6, 7.



### 2.1.27 Use Case 5. Reputation

The reputation value should be endorsed by the community. It is important to control the identity of the originator of the rating, as well as the reputation of a content contributor. In the application, this is enforced by allowing only authenticated members of the community to provide ratings. Rating of content is done by a partial identity, a compromise to enforce the distinct requirements of provenance and privacy at the same time. It is possible to provide comments together with a rating, as well as to look at the reputation of a content contributor.

### 2.1.28 Use Case 6. External Services

No user data is disclosed outside the community. Within the community the disclosure of information is managed by the End User via the privacy rules.

### 2.1.29 Use Case 7. Content Sharing

Content is always associated with the partial identity by which it was imported. The system should tag the content with the appropriate information so that it can be easily identified. This link is clearly shown by the CA, either directly in the screen or by an option in the menu.

## TrP05: Audit

**Def.:** PICOS allows processes to be fully auditable by a trusted entity.

**Use cases:** All.

Event logging functionality is performed by the PICOS platform.

## TrP06: Objective/Subjective Trust

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

Trust relies on reputation and reputation is based on rating of content and contribution pushed to community or sub-community repositories.

The principle is enforced throughout the PICOS platform.

**Use cases:** 4, 5, 6, 7.



### 2.1.30 Use Case 4. Multiple Partial Identities

The application allows users to assess the reputation of a member before establishing communication. Subjective trust is supported by the concept of private room and private-community. Asynchronous messages, which are handed privately via user inboxes, contribute also to trust. The trust perception related to a specific partial identity of a user relies only on the actions performed by this particular partial identity, not by the other partial identities associated with the user.

### 2.1.31 Use Case 5. Reputation

Trust can be built upon reputation. It is therefore important that the reputation values accurately denote the trustworthiness of the members.

Objective trust is achieved in the application by letting authenticated members, and only those, rate provided content. The user can check the reputation of a partial identity before establishing a communication.

### 2.1.32 Use Case 6. External Services

No user data is disclosed outside the community and within the community, the disclosure of information is managed by the End User via the privacy rules.

### 2.1.33 Use Case 7. Content Sharing

Reputation of the members importing content to the community will be affected by the feedback provided by other members of the community in the form of content rating. Chats can also foster subjective trust between community members.

## TrP07: Consensus

Def.: PICOS guarantees that no single entity can act in a way that might compromise the trust and privacy of the community.

**Use cases: 9.**

### 2.1.34 Use Case 9. Sub-community

Delegation of a sub-community should require the consensus of all its members. However, as it is currently implemented in the CA, changing the administrator of a sub-community does not require the consensus of its members, since only the administrator may select a new administrator.



## TrP08: Accountability

Def.: PICOS ensures that Members are accountable for their actions while a member of the Community.

The event logging mechanisms as well, as the access control user identity validation, enable a step by step control of any user action.

**Use cases: 1, 4, 7.**

### 2.1.35 Use Case 1. Registration

A member must provide accurate personal information and are accountable for this. If this data is not accurate the community may decide to take actions against the user, like being expelled from the community. There is no way to know if user data are accurate. Accountability is enforced by event logging, which is performed by the PICOS platform.

### 2.1.36 Use Case 4. Partial Identities

Accountability is always related to the user, not the partial identity. It is enforced by event logging, which is performed by the platform. The administrator can always link any partial identity to the associated root identity.

### 2.1.37 Use Case 7. Content Sharing

Members are liable for the content they import. The imported content affects among others the reputation of the importing member.

Members obtain their reputation from the content they import. Because of content rating, the imported content affects the reputation of the importing member. Content with very low ratings could be used as indicators of bad behaviour and trigger a punitive action by the administrator, e.g. being excluded from the community. Additionally, negative feedback on contributed content could also be taken into account in order to take disciplinary actions.



## 3 Threat Analysis

Continuing and complementing the assurance evaluation of PICOS performed in the first cycle of the PICOS project, and in accordance to the proposed assurance based development methodology, for the second phase we concentrate mainly on an analysis of threats, risks and vulnerabilities concerning trust and privacy in PICOS. The evaluation was carried out in the shape of questions and answers directed to WP6 developers and associated with the threats and recommendations extracted from the literature listed in Appendix A, especially from the first three papers in the list. References have often been made to the WP6 deliverables where more details may be found about the corresponding issue.

The rest of this section is organised as follows: in section 0 we focus on the important issue of safeguards; section 0 is dedicated to the threats to security put forward in the ENISA position paper No. 1 [ENI07a], as well as recommendations presented in this paper, which often may be seen as countermeasures to detected threats; finally, section 0 is dedicated to the important issue of reputation, which is closely related to trust.

### Safeguards

The principle PrP18 Safeguards is especially important in this context. This principle is related not to privacy goals, but to privacy vulnerabilities, important to consider at the current stage of development. In the following, section is dedicated to each included vulnerability.

#### 3.1.1 Unauthorized access to personal information

This issue is related to PrP13 Third-party Disclosure, and PrP21 Data Management.

##### *Is there a way to access personal information in an unauthorized way?*

The user's personal information is stored in the user profile. By default the profile is private, and nobody has access to this information, unless the user creates a specific rule for this purpose, stating who of his contacts is allowed to have access to the profile information (or part of it) [D6.1 2.2.9.3 p. 81].

##### *Is there see any possible vulnerability in this regard?*

No. If the user does not create any privacy rules related to profile, nobody will be able to see that information.



### 3.1.2 Identity theft (impersonation)

This is partially related to PrP13 Third-party Disclosure, but it is a wider significance. It might also affect also the principles TrP03 Provenance, and TrP08 Accountability.

*Are there any countermeasures in case there is a suspicion that an identity has been stolen?*

No. We can say that the PICOS community does not exist as such. We have the tools and we can put them at disposal of a community, but neither anglers nor gamers are long-term communities. In case of having such a stable community, we could have admin roles that could detect these situations and act accordingly.

### 3.1.3 Information Aggregation concerning partial identities

This issue is related to PrP24 Multiple Persona. Due mainly to location and presence information, and other PID profile information, information may be combined to link partial identities.

*Is it possible to link partial identities (e.g. by location, disconnections, etc)? Are there any countermeasures in this case?*

A user *A* could have several Identities (Partaild1, PartialId2, Partitald3...). A user *B* could add to his contact list several of these identities, for instance PartialId1 and PartialId3, without noticing that both identities belong to the same person (user *A*). If user *B* tries to locate his or her contacts over the map, PartialId1 and PartialId3 would appear in the same location area, but then user *B* will not be able to deduce that both identities belong to user *A*, since PartialId3 could belong to a third user *C* in that location area at that moment. However, he may suspect that both identities belong to the same user, especially if they often appear together at several locations.

PICOS community implements a countermeasure in order to prevent user from linking several identities with regard to presence information. For instance, assume that user *A* has three partial identities (Partaild1, PartialId2, Partitald3), and user *B* has added two of these to his contact list (PartialId1, PartialId3); if user *A* switches between identities (from PartialId1 to PartialId3), user *B* could observe these presence changes, and he might therefore be able to link both identities to the same person. For this reason, PICOS server adds different delays in showing the changes of presence information of each of the partial identities of a user. Moreover, the user can configure the location visibility (on, off, blurring) for each identity individually to prevent linkability

### 3.1.4 Information Storage Vulnerabilities

This topic related to PrP13 Third-party Disclosure, to unauthorized access to profiles (personal and sub-communities), and to auditing information.



*Which safeguards are in place to prevent unauthorized access to profiles, logging information, and so on?*

By default profiles are private. The server is protected and located in a Militarized Zone, access to the server is only granted to specific administration staff, and the server access is logged.

### 3.1.5 Information Transmission Vulnerabilities

This issue is related to PrP13 Third-party Disclosure and PrP22 End-to-End Privacy. Also PrP01 might be affected.

*Is it possible to intercept data during transmission? Which mechanisms have been used in order to enforce data confidentiality during transmission?*

Communication between PICOS client and the PICOS platform is always encrypted using widely-used and reliable protocols (**HTTPS/SSL**). The PICOS platform (server side) is authenticated to the client by means of a server digital certificate. The server certificate is not checked by the client and is not displayed to the user to let him check it, a feature could nevertheless be added.

### 3.1.6 Information Collection Vulnerabilities

This is related to PrP10 Fair and Lawful Means

*Is it possible to collect information, directly or indirectly, without the consent of the data subject?*

No. The user is always aware of the collection of his or her personal data.

*Concerning content data, is it possible to collect or receive data by unfair or unlawful means?*

No, the user is aware of the purposes for his data collection, since he must accept the terms and conditions during registration.

Moreover, the user is always given the option of not entering personal data in any screen. For instance, when a user is about to create a new account and enter information to the profile on the text fields displayed over the screen, he or she may enter or not personal data, such as family name or street. These are therefore optional, not mandatory, fields.

### 3.1.7 Session vulnerabilities

*How is a session maintained?*



Using a session token like `sessionToken="token407699"`, which is obtained from the PICOS server during the login process.

*Is it possible to impersonate someone due to any vulnerability related to the way a session is maintained?*

As far as we are aware this is not possible or very hard in normal circumstances.

## Threat analysis and recommendations for security

Many threats are presented in the ENISA Position Paper No. 1 [ENI07a], as well as recommendations which often may be seen as countermeasures to detected threats. It is our belief that PICOS will benefit from an analysis of the recommendations included in this position paper.

A section below is dedicated to each targeted threat.

### 3.1.8 Digital dossier aggregation

Profiles can be downloaded and stored over time and collected by third parties, creating a digital dossier of personal data. Information revealed in this way can be used for purposes and in contexts different from the ones the profile owner had considered.

*How are personal profiles protected?*

The user may create private rules associated with the profile in order to establish who can access his personal information. For instance, he or she could create a rule allowing one specific contact from his/her contact list to have access to some attributes of the profile (e.g. hobbies, messaging info, hometown info), or to the whole profile.

*Can personal profiles be downloaded and stored by third parties*

No. A user in PICOS may access another user's profile only if the latter has explicitly allowed the former to see his or her profile by creating a privacy rule for that purpose.

*Can information revealed be used for purposes and in contexts different from the ones the profile owner has considered?*

No, since all collected information about a user is processed only within the PICOS community, never being disclosed to third parties. The treatment of this kind of information is done in compliance with the terms and conditions accepted by the user at registration time.



### 3.1.9 Secondary data collection

Secondary data refers to time and length of connections, location (IP address), visited profiles, sent and received messages, and similar.

*Is it possible for third parties to collect logged data about activities performed by users?*

No. All consortium partners agreed not to allow data transmission to third parties. The advertising services implemented in PICOS do not involve servers from third parties.

*Is it clear to users whether any secondary data is collected and in this case how it is used?*

No secondary data is collected, but the user is not so far informed about this.

*Do privacy policies refer to eventually collected secondary data?*

No.

### 3.1.10 Linkability from image metadata

Since images are tied to individual profiles and often identify either explicitly (through, for example, labelled boxes on images) or implicitly (through recurrence) the profile holder, they constitute a data source suitable for correlating profiles across services using face recognition.

*May images be tagged, allowing unwanted linkage to personal data?*

No. However, the Gamers prototype allows users to attach keywords to pictures. When watching a picture, a user may see those keywords by selecting a specific option, since those keywords do not appear automatically when the user drags the stylus over the picture, as is the case in other social networking systems.

### 3.1.11 Account deletion

Users wishing to delete accounts may find that, although it is usually very easy to remove their primary pages, secondary information such as public comments on other accounts will remain online.

*Is it possible to remove secondary information linked to a profile such as public comments?*

No, content uploaded by users are not eliminated when the account is deleted in order to avoid gaps in the threads. However, the name of the content provider is deleted and the authors of those posts appear as “anonymous”.



### 3.1.12 Spam

Spam is unsolicited messages propagated e.g. using social networks.

*Is it possible to receive unsolicited messages? May those be blocked?*

No. In advertising services a target user can receive such commercials if he has previously subscribed to receive them (through the settings screen in the Gamers application). Similarly for recommendations: only in case that the user has previously subscribed to receive recommendations from a determined contact will those be sent to him or her. [D6.2.b 4.13]

### 3.1.13 Cross site scripting, viruses and worms

In some social network systems, users can post HTML within their own profiles and message-boards. These systems are particularly vulnerable to XSS (cross site scripting) attacks. So-called 'widgets', produced by weakly verified third parties, are widely used. In addition, a heavy reliance on message posting and viral marketing means SNS viruses spread extremely quickly.

*Is PICOS vulnerable to cross site scripting attacks and threats originating from widgets from third parties?*

The Gamers application is a J2ME client application running on the handset. Hence, since it is not a web application, the question does not apply.

### 3.1.14 Contextual Information

Contextual information should be used to inform people in "real-time" about trust and privacy issues. Sites should publish user-friendly community guidelines rather than "terms and conditions." Accessible language easy for users to understand should be used.

*How are these recommendations regarding contextual information followed?*

The Gamers application provides a Help pop-up window in several screens (for instance the Identities screen). With regard to trust, the PICOS Community prototypes provide a rating mechanism for content (as into Public community and Sub-Communities). This rating may give a clue to a user about the level of trust of a particular content.

### 3.1.15 Stronger authentication

Stronger authentication and access control should be used in certain social network environments; CAPTCHAs could be also used.



*Have the use of stronger authentication been considered within PICOS?*

This issue has not been considered in PICOS. The Gamers application uses a user/password authentication mechanism over HTTPS (secure channel).

### 3.1.16 Abuse reporting

Possibilities for abuse reporting and detection should be maximized, and it should be easy to report abuse and concerns; “report abuse” buttons should be ubiquitous.

*Is there any functionality in place in PICOS for abuse reporting?*

Only the PICOS Community administrator is able to revoke a member’s account. Moreover, a message can be send to the administrator for abuse reporting at any time.

### 3.1.17 Default settings

Default settings should be made as safe as possible.

*Which default settings have been adopted in PICOS, and what is their impact on trust and security?*

Defaults setting in Gamers application are quite restrictive:

1. **Profile:** user profile is hidden/private by default.
2. **User Location:** PICOS server requests authorization to the target user before disclosing his location information to the requester user, and only in case the target user accepts to share his or her location information will the PICOS server send it.
3. **User Presence:** the PICOS server requests authorization to a target user before disclosing corresponding presence information to the requester user, and only in case the target user accepts to share his or her presence information will the PICOS server send it.
4. **Contacts list:** the contacts list of a user is closed and private by default. Therefore, unless the user creates a specific private rule allowing access to his or her contacts list, nobody will be able to see his or her contacts.
5. **Content:** the content in the public community is public by default. With regard to Sub-Communities, it is public for public sub-communities and private, i.e. accessible only to members, in private sub-communities.



### 3.1.18 Data deletion

Convenient means to **delete data** should be provided. Simple, easy to use tools should be provided for removing accounts completely and for allowing users to edit their own posts on other people's public notes or comments area. Privacy policies and help pages should explain clearly how to do it.

*Which functionality is offered to users for deletion of data? Are there help pages for that?*

Generally speaking, the Gamers application allows the end user to remove each feature that he or she has created. This means that he user is able to remove:

- **Contacts** from his contacts list
- **Identities**
- **Content:** the user is able to remove the content that he or she posted into the Public Community/Sub-Communities, as well as thread and/or forum in case he or she is its creator
- **Privates Sites/Points of Interest (POIs)**
- **Messages**

The user is also able to **modify** his profile and open or close a chat.

### 3.1.19 Reputation techniques

The use of reputation techniques should be encouraged.

*Is there any help information for users concerning reputation in PICOS?*

We believe that more help pages should be added to to the existing help system to explain the concepts. The Reputation component is a very important component in the PICOS prototypes, allowing users to rate uploaded content.

PICOS prototypes allow rating the following features:

- Public Community Thread Post/Content
- Sub-Communities Thread Post
- Privates Sites
- POIs

The end user will be able to see the reputation of his contacts since each contact is displayed together with the reputation in the Contact Screen.

### 3.1.20 Filters

Build in automated filters. Offensive, litigious or illegal content should be blocked by smart filters.

*Are there automated filters in PICOS?*



There are no automated filters in PICOS intended to block offensive content. However, PICOS offers a “Moderator” role (as in forum and threads), who is able to decide whether a specific content or file is offensive, and also to revoke the user’s account from the community.

### 3.1.21 Profile tags

Require consent to include profile tags. The tagging of images with personal data without the consent of the subject of the image violates the latter’s right to informational self-determination. Operators should implement mechanisms for giving users control over who tags images depicting them.

*Is there any functionality for tagging in PICOS? In this case, is consent required?*

The Gamers application allows users to upload content to the platform and attach keywords to that content. Keywords are free text (for instance, names and locations). Content is stored at the platform with associated keywords. At the client side a user may display the content and associated keywords, but the user is not able to see these keywords when he is dragging the stylus over the picture; he or she needs to select a specific option for that purpose.

### 3.1.22 Spidering and bulk downloads

Restrict spidering and bulk downloads. Operators should protect all means to access profiles which might lend themselves to bulk access. Access restrictions should also be put in place to make it harder to create bogus accounts.

*Is bulk access possible in PICOS? For instance, for advertising purposes?*

This is not possible in PICOS Communities since the user may access each contact profile only one by one., provided that the contact authorized the user to see his or her profile (by creating a rule with the aid of privacy manager).

#### 3.1.22.1 Search results

The user should be clearly informed that they will appear in search results and given the choice to opt out. Data should be anonymised, not displayed, or the user should be clearly informed that it will appear in search results and given the choice to opt out.

*If the users appear in search results, are they informed about it? Is data anonymised in those cases?*

For the current version of the Picos prototypes the answer is no.

### 3.1.23 Eliminating spam

Techniques to eliminate spam comments and traffic should be developed.



### *Is there such functionality in PICOS?*

PICOS offers a “Moderator” role (as in forum case as in threads), who is able to decide whether a specific content or post is spam. If the moderator so wishes, he or she may revoke the user’s account from the community.

### **3.1.24 Phishing**

Practices for combating phishing should be adopted. Links that do not point to the text shown to the user may be flagged or even banned. Images representing text links may also be flagged or banned.

### *Is it possible in PICOS to flag or ban links that do not point to the text?*

It is not possible because there are no links in the application that could be misused for fishing.

## **Trust principles: Reputation**

Reputation is closely related to trust in the sense that reputation enables trust. An important recommendation put forward in [ENI07b] is that a threat analysis of the reputation system should be performed, and the security requirements should be identified. Moreover, it is also stated that the threats and related attacks need to be considered in the context of the particular application or use case, as these have specific security requirements. The paper identified security requirements, threats and attacks that should be taken into account in the design and choice of a reputation system. The most relevant of these requirements and threats for PICOS will be presented below.

### **3.1.25 Threats**

This issue is largely a responsibility of the platform. Hence, only some threats to the reputation system are presented below.

#### *3.1.25.1 Whitewashing attacks*

In this attack, the attacker tries to get rid of a bad reputation by rejoining the community with a new identity. A system is vulnerable to this attack if it allows easy change of identity and easy use of new pseudonyms. Anonymous interaction and the ability to be untraceable favours identity change. The attack can leverage a sibyl attack (see below) where multiple identities are exploited, and it is also related to the bootstrap issue.



*Does PICOS offer any functionality that makes whitewashing attacks more difficult to perform?*

New partial identities with neutral reputations can be created and a member may change easily between the identities, but although this could be used for whitewashing attacks it one of the important Picos features to enhance privacy. In order to prevent whitewashing the initial reputation of a new identity could be set to a value that is derived from the existing identities. Moreover, Picos Community doesn't allow a user with a partial identity to rate content uploaded by him or herself using a different partial, a feature that also makes whitewashing more difficult in a specific scenario.

*3.1.25.2 Sybil attack*

The attacker creates multiple identities or sibyls and exploits them in order to manipulate a reputation score. It would be interesting to analyse whether the notion of partial identity in PICOS prevent or facilitate sibyl attacks.

*Does the notion of partial identity facilitate sibyl attacks?*

The PICOS community prototype does not allow a user with a root identity R1, acting through a partial identity R1P1, to rate content uploaded by himself but using a different partial identity R1P2, but if a user creates another PICOS Community account with a different root R2, he or she will then be able to create as many new partial identities as desired, attached to this new root identity, and use one of these identities, say R2P1, for rating the content uploaded by himself or herself using R1P1.

*3.1.25.3 Repudiation of Data*

A user can deny the existence of data for which he was responsible. Logging of transactions may be used against this.

*Are there mechanisms in PICOS to prevent denial of uploaded content?*

Trace files are stored in the platform. When a user publishes some content, the server stores this content together with the associated identity of the publisher.

### **3.1.26 Security**

Security requirements for reputation systems include the items below.

*3.1.26.1 Usability/Transparency aspects*

*How transparent is the reputation system to users?*

---

Copyright © 2008-2010 by the PICOS consortium - All rights reserved.

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



The gamers application display a screen where the end-user is able to set the reputation that he wishes for a specific selected content. In this screen the user may chose a score between one and five, and also add some comment.

*Can the reputation be customized by a user?*

No.

*Are users offered qualitative assessment of reputation?*

Not directly, but it may be inferred from the number of stars in the reputation of the user.

*Is an open description of the reputation metrics available to users?*

No.

*Is it easy to report on inappropriate content, profile squatting, identity theft, and inappropriate behaviour?*

The end user may send a post reporting inappropriate content or behaviour, whereupon the PICOS Community administrator may take appropriate action, for instance cancelling the user account. Moreover, the user may also rate a content and attach a description (free text) describing the reason for the rating.

### *3.1.26.2 Availability*

Important when the reputation system becomes critical to the functioning of the overall system

*Does PICOS enforce availability in some way?*

The question is more related to high availability aspects of the system which are out of the project scope.

### *3.1.26.3 Integrity of Reputation Information*

The reputation information should be protected from unauthorised manipulation. This may be enforced by protection of the communication channels or the central reputation repository.

*How are communications channels and central reputation repository protected in PICOS?*

Using HTTPS.



#### *3.1.26.4 Privacy/Anonymity/Unlinkability*

Privacy should be preserved. The use of partial identities should be analysed in this context.

##### *How do the partial identities preserve privacy in PICOS?*

The fact of having different identities associated to the same user or root identity in PICOS communities allows end users to have several different profiles that can be used in different contexts. Hence, a user could have one identity for a personal context (e.g. his or her family), a second one for a professional context, a third one for friends, and so on.

PICOS has mechanisms to make it harder to link the different partial identities of a user.

#### *3.1.26.5 Accuracy*

The reputation system should be accurate in the calculation of ratings. Ability to distinguish between a newcomer and an entity with bad reputation should be offered.

##### *Does PICOS promote the ability to distinguish between a newcomer and an entity with bad reputation should be offered.*

A new PICOS user has by default an average reputation value, but it cannot be distinguished from someone with a real average reputation.

#### *3.1.26.6 Accountability*

Each peer should be accountable in making reputation assessments.

##### *Is accountability in making reputation assessments enforced in PICOS?*

When a user displays some content, the description of the content and the rating history associated to this content are also displayed. This rating history includes the pseudonym of the voter, the rating score and the comment (free text) in case it has been included. This enhances accountability.

#### *3.1.26.7 Protection of well-connected entities*

Users with a high reputation rating are most likely to be attacked, and should therefore receive a higher level of protection.

##### *Are there special mechanisms in PICOS to protect users with a high reputation system?*

No.



### *3.1.26.8 Self-correction*

Self-correction might be needed in the case of the overall reputation of each member, since reputation is linked to the subjective opinion of voters. Moreover, there must be an appropriate choice of the period over which reputation is estimated.

*Are there mechanisms for self-correction in PICOS? Over which period is reputation estimated in PICOS?*

The reputation system is not attached to a determined period of time and the user score changes only when other PICOS users rate any of the uploaded content.

### *3.1.26.9 Verifiability*

Whenever possible, proof should be collected from the interaction that is rated to show that the rating can be verified as correct.

*Is it possible to collect such proofs in PICOS?*

By logging, a responsibility of the platform.

### *3.1.26.10 Security requirements on the underlying networks*

The underlying network should have appropriate security mechanisms in place so that attacks to it do not jeopardise the reputation system.

*Are there appropriate mechanisms in PICOS to prevent attacks on the reputation system?*

This is also a responsibility of the platform.

## **3.1.27 Recommendations**

Recommendations to designers of reputation systems include the following:

### *3.1.27.1 Develop reputation systems which respect privacy requirements*

Anonymity would increase the accuracy of the reputation system. A more privacy-respecting design of reputation systems is needed, while at the same time preserving trust. There are mechanisms providing privacy for voters and reputation owners that can be implemented by making reputation systems interoperable with privacy-enhancing identity management systems which assist users in choosing pseudonyms. The partial identity concept user in PICOS should be analysed in the light of these recommendations. However, this would be a responsibility of the platform.



### *3.1.27.2 Provide open descriptions of metrics*

Reputation metrics should be open and easily accessible.

*Is a description of reputation metric used in PICOS available to users, and in this case is it easy to understand?*

No.

### *3.1.27.3 Usability of reputation-based systems*

In order to increase trust the user should understand how reputation is formed and measured within the system. Reputation systems should be transparent and allow a user to easily understand how reputation is formed, the implications of reputation ratings, how reputation is verified, and how the user can assess the reputation system's trustworthiness.

*Can the reputation metric in PICOS be regarded as transparent? Is it easy for users to understand how reputation is formed, the implications of reputation ratings, how it is verified, and show to assess the trustworthiness of the reputation system?*

No features have been implemented in the gamers prototype intended to enhance the transparency of the reputation system to users. However, a reason for not showing all details about the reputation system to the user is to prevent manipulation.

### *3.1.27.4 Differentiation by attribute and individualisation as to how the reputation is presented*

Users should be able to customize reputation so as to best accommodate his needs.

*Is it possible in PICOS for users to customize reputation?*

No, but comments may be inserted.



## 4 Conclusions

In this deliverable we have presented an analysis and evaluation of the trust and privacy functionality of the community prototype 2, described in D6.2a and D6.2b. We have focused on two points:

1. A revision and updating the results of the analysis of the community prototype 1 in view of the community prototype 2.
2. An evaluation of the prototypes with regards to the threats and recommendations put forward in several ENISA papers published by ENISA (European Network and Information Security Agency).

Concerning the first point, only a few issues were raised in the first cycle concerning mainly the registration procedure. We believe that these points have been satisfactorily met in the second cycle.

With respect to the second point, it is important to point out that the recommendations were not PICOS requirements. Nevertheless, our analysis gives outsiders a useful account of what they may expect from PICOS with regard to these recommendations. Many of them cannot be solved by technical means, and should be enforced by the administrator of each specific community. Others are relevant mainly for the architecture or the platform, and have been answered in the corresponding deliverables, D3.1.2 resp. D3.2.2.

It must be noted that the prototypes depend on the platform, and most results concerning the evaluation of the privacy and trust aspects in PICOS concern mainly the architecture and the platform. Nevertheless, the analysis of the prototypes helps clarifying many issues related to the platform, and may be therefore seen as an extension of the evaluation of the platform.

The results of the assurance evaluation can be classified into three main categories: privacy, trust, and safeguards. Each one can be further decomposed, as shown below, and should be treated separately with regard to the results. We present below the conclusions for each one of them.

1. **Privacy:** In order to give a better account of these results, we classify them into three categories: (i) Notice and Information; (ii) Collection and Use of Personal Data; and (iii) Data and Identity Disclosure. We could sum up the results for each one of these areas below.
  - **Notice and Information**
    - In the prototypes, the community terms and conditions are used to explain the global community policies related to data collection and data retention, and they are displayed during the registration before any data is collected and are always available for inspection.
  - **Collection and Use of Personal Data**
    - Within the community the disclosure is managed by the end user via the creation of privacy rules. The user is able to manage consent via the policy rules that can be modified via the client application. Any data collected on the end user is made available to him or her through the client application.
  - **Data and Identity Disclosure**



- No user data is disclosed outside the community, and within the community the disclosure is managed by the end user via the privacy rules.
2. **Safeguards:** security is always a trade-off between the security risks and costs; PICOS uses standard security mechanisms such as HTTPS, which for the nature of the PICOS applications can be judged as good enough. We categorise safeguards into authentication, authorization, and confidentiality.
- **Authentication**
    - The prototypes support one way of authentication, by username/password, since currently only this form has been implemented in the platform. After authentication, a session token is used by the CA to reconnect transparently to the user.
  - **Authorization**
    - Members can select any of their partial identities to access the community and its services. Access to the platform is performed using the root identity. The server is protected and located in a Militarized Zone, and access to the server is only granted to specific administration staff.
  - **Confidentiality**
    - SSL (HTTPS) is used for communication between the client application and the platform, a protocol in widespread use today for securing internet transactions.
3. **Trust:** we categorise trust into three main topics: accountability, provenance, and reputation.
- **Accountability**
    - This issue is the responsibility of the platform, see D3.2.2 for details.
  - **Provenance**
    - PICOS ensures that members can rely on the provenance of information, an issue that is treated mainly at the platform level. See D3.2.2 for details.
  - **Reputation**
    - The prototypes support the functionality concerning reputation aspects, e.g. rating. Much can be done to enhance transparency with regard to this issue, but this is basically a concern of the platform.

Summing up the results, we may conclude the following: concerning privacy, the PICOS prototypes meet the established requirements in a satisfactory way; concerning safeguards, the security mechanisms that have been included seems to us to be adequate for the the kind of application targeted by PICOS; finally, with regard to trust we believe that the reputation system can be further improved, especially concerning transparency to users, but this is basically a concern of the platform.



## References

[D3.1.1] Vivas, J. and Agudo, I., “D3.1.1 Trust and Privacy Assurance for the Platform Design”, Final Confidential Deliverable of EU Project PICOS, Apr 2009.

[D3.2.1] Vivas, J. and Agudo, I., “D3.1.2 Trust and Privacy Assurance Evaluation of the Platform Prototype”, Final Confidential Deliverable of EU Project PICOS, Sep 2009.

[D3.3.1] Vivas, J. and Agudo, I., “D3.1.3 Trust and Privacy Assurance of the Community Prototype”, Final Confidential Deliverable of EU Project PICOS, Jan 2010.

[D3.4.1] Vivas, J. and Agudo, I., “D3.4.1 A summary of PICOS WP3 sub-phase 3.1 deliverables”, Final Public Deliverable of EU Project PICOS, September 2010.

[D3.1.2] Vivas, J. and Agudo, I., “D3.1.2 Trust and Privacy Assurance for the Platform Design v2”, Final Public Deliverable of EU Project PICOS, December 2010.

[D4.1] Crane, S., “D4.1 Platform Architecture and Design v1”, Public Deliverable of EU Project PICOS, Mar 2009. Available at [http://picos-project.eu/fileadmin/user\\_upload/fmgr/Deliverables/WP4\\_Architecture\\_and\\_Design/D4.1\\_Platform\\_Architecture\\_and\\_Design\\_1/PICOS\\_D4\\_1\\_Architecture\\_v1\\_4\\_Final\\_Public.pdf](http://picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP4_Architecture_and_Design/D4.1_Platform_Architecture_and_Design_1/PICOS_D4_1_Architecture_v1_4_Final_Public.pdf) (last access: Nov 2010).

[D4.2] Crane, S., “D4.2 Platform Architecture and Design v2”, Public Deliverable of EU Project PICOS, Sep 2009. Available at [http://picos-project.eu/fileadmin/user\\_upload/fmgr/Deliverables/WP4\\_Architecture\\_and\\_Design/D4.2\\_Platform\\_Architecture\\_and\\_Design\\_2/PICOS\\_D4\\_2\\_Platform\\_Architecture\\_and\\_Design\\_2\\_Final.pdf](http://picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP4_Architecture_and_Design/D4.2_Platform_Architecture_and_Design_2/PICOS_D4_2_Platform_Architecture_and_Design_2_Final.pdf) (last access: Nov 2010).

[D6.1] PICOS Deliverable D6.1 Community Application Prototype 1, Final Public. [http://picos-project.eu/fileadmin/user\\_upload/fmgr/Deliverables/WP6\\_Application\\_Prototype/D6.1\\_Community\\_application\\_prototype\\_1/PICOS\\_D6\\_1\\_Community\\_Application\\_Prototype\\_v1\\_Final\\_Public.pdf](http://picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP6_Application_Prototype/D6.1_Community_application_prototype_1/PICOS_D6_1_Community_Application_Prototype_v1_Final_Public.pdf)

[D6.2a] PICOS Deliverable D6.2b First Community Application Prototype 2, Final Public [http://picos-project.eu/fileadmin/user\\_upload/fmgr/Deliverables/WP6\\_Application\\_Prototype/D6.2\\_Community\\_application\\_prototype\\_2/PICOS\\_D6\\_2\\_Community\\_Application\\_Prototype2\\_v1\\_Final.pdf](http://picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP6_Application_Prototype/D6.2_Community_application_prototype_2/PICOS_D6_2_Community_Application_Prototype2_v1_Final.pdf)

[D6.2b] PICOS Deliverable D6.2b Second Community Application Prototype 2, Final Public [http://www.picos-project.eu/fileadmin/user\\_upload/fmgr/Deliverables/WP6\\_Application\\_Prototype/D6.2\\_Community\\_application\\_prototype\\_2/D6.2b/Deliverable/PICOS\\_D6\\_2b\\_Community\\_Application\\_Prototype\\_v1.0\\_final.pdf](http://www.picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP6_Application_Prototype/D6.2_Community_application_prototype_2/D6.2b/Deliverable/PICOS_D6_2b_Community_Application_Prototype_v1.0_final.pdf)



## Appendix A Reports consulted

PUBLICATION	DATE
<p><i>Security Issues and Recommendations for Online Social Networks</i>. ENISA Position Paper No.1. Editor: Giles Hogben, ENISA.  <a href="http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks">http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks</a></p>	Oct 2007
<p><i>Reputation-based Systems: a security analysis</i>. ENISA Position Paper No. 2. Editors: Elisabetta Carrara and Giles Hogben, ENISA.  <a href="http://www.enisa.europa.eu/act/it/oar/reputation-systems/reputation-based-systems-a-security-analysis">http://www.enisa.europa.eu/act/it/oar/reputation-systems/reputation-based-systems-a-security-analysis</a></p>	Dec 2007
<p><i>Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID)</i>. Editors: Ingo Naumann, Giles Hogben, ENISA.  <a href="http://www.enisa.europa.eu/act/it/eid/mobile-eid">http://www.enisa.europa.eu/act/it/eid/mobile-eid</a></p>	Nov 2008
<p><i>Study on the Privacy of Personal Data and on the Security of Information in Social Networks</i>. INTECO's Information Security Observatory.  <a href="http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_red_es_sociales_en">http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_red_es_sociales_en</a></p>	Feb 2009
<p><i>Trust in the Information Society</i>. A Report of the Advisory Board RISEPTIS.  <a href="https://www.tssg.org/trustandsecurity/2010/04/riseptis_report_nears_the_5000.html">https://www.tssg.org/trustandsecurity/2010/04/riseptis_report_nears_the_5000.html</a></p>	Oct 2009
<p><i>Internacional Standards on the Protection of Personal Data and Privacy</i>. The Madrid Resolution.  <a href="http://www.gov.im/lib/docs/odps/madridresolutionnov09.pdf">www.gov.im/lib/docs/odps/madridresolutionnov09.pdf</a></p>	Nov 2009
<p><i>Online as soon as it happens</i>. ENISA.  <a href="http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens">http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens</a></p>	Feb 2010