Grant Agreement no. 215056

Title:	***D3.1.2 Trust and Privacy Assurance for the Design Platform 2***
Editors:	*José Luis Vivas & Isaac Agudo (University of Malaga)*
Contributors:	*José Luis Vivas & Isaac Agudo (UMA), Markus Tschersich (GUF)*
Reviewers:	*Stephen J. Crane (HPL), Stefan Eicker (ITO)*
Identifier:	*D3.1.2*
Type:	*Deliverable*
Version:	*1.0*
Date:	*15.1.2011*
Status:	*Final version*
Class:	*Public*

Summary

This deliverable provides an evaluation of the PICOS Platform Architecture and Design 2. The main purpose of this deliverable is to ensure that the PICOS platform architecture and design are accurate with the trust and privacy technical objectives planned. Our main focus here has been the detection of non-conformances in the definition of the architecture with respect to the established privacy and trust principles. We present both a revision of the findings established in D3.1.1, and an analysis of threats, risks and vulnerabilities concerning trust and privacy in the PICOS platform design. We explain how the architecture defends against a set of known threats and vulnerabilities derived directly from several ENISA (European Network and Information Security Agency) publications that relate to social networking.

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

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
D5.2a	Platform prototype 2a	May 2010
D6.1	Community Application Prototype 1	December 2009

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

D6.2a	First Community application prototype 2	April 2010
D6.2b	Second Community Application Prototype v2	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 project receives research funding from the Community's Seventh Framework Programme.

The PICOS Deliverable Series

Vision and Objectives of PICOS

With the emergence of services for professional and private online collaboration via the Internet, many European citizens spend work and leisure time in online communities. Users consciously leave private information; 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.

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

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 3.1 Evaluation of Platform Design

The most critical problems that we could face in the PICOS identity management platform are those that develop when the architecture does not conform (is incorrect or inappropriate) to the initial trust and privacy requirements. For this reason, the work in this WP will start by assessing the specifications of the PICOS architecture. More precisely, we will start by evaluating at a very low level the functionality of the different components of the architecture that are originated from the requirements. Then, at a higher architectural level, the assessment will pursue the goal of demonstrating that there is an appropriate interoperability of the elemental components, as well as the adequacy of the trust and privacy mechanisms that they implement. At this stage we will finally validate that the interfaces and protocols among the components comprise the data flows that apply to scenarios of PICOS communities. With these steps we will have assured that the architecture and design of the platform are consistent. The direct outcome of this sequence of steps will be the two versions of deliverables D3.1 in the two cycles of Phase 3 of the project plan. Task 3.1 will provide assurance methodology guidelines before the platform design happens, and will evaluate the design against these before its finalization.

Foreword

Deliverable D3.1.2 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. Please take a look at D3.4.1 for a description of the assurance methodology followed here.

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: Jose Luis Vivas & Isaac Agudo, University of Malaga, ES (UMA), Markus Tschersich, Goethe University Frankfurt, DE (GUF)

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

Table of Contents

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

List of acronyms

Dx.y.z	*[PICOS] Deliverable: Work Package x, Deliverable y, Cycle z*
ENISA	*European Network and Information Security Agency*
PICOS	*Privacy and Identity Management for Community Services*
PID	*Partial Identity (also Identifier)*
PP	*PICOS Principle*
PrP	*Privacy Principle*
PUC	*PICOS Use Case*
SNS	*Social Networking Sites*
TrP	*Trust Principle*
WPn	*Work Package number n*

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

1 Assurance

Complementing the assurance evaluation of the PICOS prototypes performed in the first cycle of the PICOS project, and presented in deliverable D3.1.1, for the second phase we concentrate on both a revision of the findings established in D3.1.1, and further on an analysis of threats, risks and vulnerabilities concerning trust and privacy in the PICOS platform design. Thus, this document explains how the architecture defends against a set of known threats (and vulnerabilities). The set of appropriate threats is derived directly from several ENISA publications that relate to social networking.

The focus on the threat analysis implies a more pragmatic approach to assurance than adopted by the first cycle, which concentrated also on research about the nature of an assurance case structuring the eventual assurance results and arguments into a single construction, the assurance case tree. We believe that approach was validated by our experience in PICOS assurance evaluation. However, not being part of PICOS assurance requirements, and demanding the utilization of a so far unavailable advanced tool for managing its complexity, we decided not to provide a full-fledged assurance case tree. The latter would in any case not provide further information on the assurance results, only a way to structure this information. However, since the threat analysis carried out was in fact the next step in the construction of the assurance case, in order to validate our approach here we provide in Section 0 a simplified snapshot of what would be the resulting assurance case once a threat analysis has been performed. The methodology itself has been presented in detail in a journal article [VAL10].

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 principle PrP18 Safeguards is particularly important in the second cycle of PICOS, and a special section below is dedicated to it.

The remaining principles might be treated more briefly, either because they are considered to have been already enforced in a satisfactory way in the first cycle, or because they are not relevant for the current version of the PICOS applications.

The principles excluded because they were considered to have been already enforced in the first cycle are the following:

- PrP 2 Policy Notification: policy notification is provided at registration
- PrP 4 Timing of Notification: notification is provided at due time.
- PrP 9 Limitation of Collection: only minimal personal data is collected.
- PrP 10 Acceptable Uses: only minimal personal data is collected and never put to uses that are non acceptable.
- PrP 12 Data Retention: personal data is not retained longer than necessary.
- PrP 15 Access to Information: members are able to determine if data on them is maintained.
- PrP 16 Provision of data: requested information easily and immediately.
- PrP17 Correcting Information: members are able to update or correct personal information.
- PrP 19 Data Accuracy: only minimal data is collected, and the user is in full control of them.
- PrP 20 Public Policies: privacy policies are publicly available.
- TrP 1 Openness and Transparency: PICOS offers services that handle personal information in an open and transparent way.
- TrP 2 Trust between communities: PICOS recognises trust as a common currency when exchanged between PICOS communities.

The principles excluded from the analysis because they were not considered relevant for the current version of PICOS are the following:

- PrP 3 Changes in Policy of Data Use: no changes in policy or data use in current version, but could be provided easily if required.
- PrP 5 Sensitive Information: no sensitive information is ever collected.
- PrP 7 Change of Use Consent: no changes of use in current implementation, but could be provided easily if required.
- PrP 8 Consequences of Consent Denial: not relevant for PICOS applications.
- PrP 14 Third-Party Policy Requirements: no third parties in current version of PICOS.
- PrP 19 Data Accuracy: only minimal data is collected, and the user is in full control of them.
- TrP 4 External services: no external services in the current version of PICOS.

The rest of this deliverable is organised as follows: Chapter 2 is dedicated to a presentation of the results of the analysis carried out with respect to the second version of the platform design, following the same approach as in the first cycle, and keeping the results from the previous phase which are still valid; In Chapter 3 we present the results of the threat analysis; Chapter 4 presents the updated assurance case tree, and Chapter 5 presents the conclusions.

2 Revision of D3.1.1

For the second version of the PICOS architecture, we give below an analysis of each of the principles included in the previous section with regard to each use case, updating the analysis carried out in D3.1.1 concerning the first version of the platform Architecture specified in D4.1. We concentrate here on the most important points and questions raised in D3.1.1. The component analysis given in D3.1.1 is still valid here, since these have not been significantly changed for the second version. Components are analysed extensively in the evaluation of the platform prototype [D3.2.2].

2.1 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.

Apart from registration, it is important to notice that personal data is also collected in the profile of generated Partial Identities. It is not mandatory for users to fill out personal information of Partial Identities and it is also possible to insert different information to each Partial Identity besides gender and age. This case is also reflected in PUC 4. Users will be informed about the fact that their published information will be accessible for all other user apart from additional rules in the Privacy Manager.

The architecture does not specify the terms and conditions themselves. This point is addressed by the platform and the prototype.

Use Cases: 1.

2.1.1 Use Case 1: Registration

In D4.1, there is no mention in the registration use case about notice of collection. It was recommended that Notice of Collection should therefore be added to the registration process, and eventually performed by Registration component.

2.2 PrP10: Fair and Lawful Means

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

Use Cases: 1, 4.

This functionality should be also included in a Data Management use case, in case personal data is collected at any other time than during registration.

2.2.1 Use Case 1: Registration

The registration use case complies with the principle that information must be collected by fair and lawful means. Users are informed about the usage of their personal information in the Terms & Condition and nothing else will be done by the platform provider. Additionally, users are not forced to enter personal information, only a name for the Root Identity and a pseudonym for each Partial Identity are mandatory.

2.2.2 Use Case 4: Multiple Partial Identities

Collection of profile data during creation of new Partial Identities must not involve collection of personal information without notice and consent, as this would contradict the principle that personal data must be collected by fair and lawful means.

Collection of data by fair and lawful means should always be enforced by PICOS. This implies that personal data disclosed by a member, without notice of collection and consent, as part of a Partial Identity profile or as imported content, should not 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 given notice of it.

Apart from the pseudonym of the Partial Identity, only personal data inserted by the user during the creation process is collected. Therefore, only inserted personal data is used in the personal profile of the member. Personal Data in Partial Identities is handled by the Community provider in the same way as root profile data. Thus, they are also collected according to the principle PrP10 in a fair and lawful way.

2.3 PrP13: Third-party Disclosure

Def.: 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.

Use Cases: 2, 6, 7, 9.

2.3.1 Use Case 2: Accessing the Community

The disclosure of information to third-parties, for instance the member's social presence status, must have been agreed previously by the member. If the accessed service is provided by an external third-party and involves the disclosure of personal information, the disclosure must be in accordance with the member's wishes with regard to information flow. However, this possibility does not apply, since External services have not been integrated to the PICOS framework, implying no interactions between the WP5 PICOS platform and external unsecured servers [D4.2 8.4.1].

2.3.2 Use Case 6: External Services

External services have not been integrated to the PICOS framework implying no interactions between the WP5 PICOS platform and external unsecured servers [D4.2 8.4.1].

2.3.3 Use case 7: Content Sharing

The member's wishes with regard to information flow of imported content are upheld with the help of tagging, according to the description of the Content Sharing use case.

2.3.4 Use case 9: Sub-Community

The same policies concerning Third-Party Disclosure for personal information must be applied to Sub-Community profiles if the latter are associated with the corresponding member's profile.

It is not possible to inadvertently disclose information about a user's profile to third parties through the information contained in a Sub-Community's profile. Apart from the pseudonyms of the participants of a Sub-Community, no other personal information is available.

Only personal information stored in the Partial Identity associated with Sub-Community is available in it. If users are aware of which personal information are stored in the current used Partial Identity, there will be no possibility of an inadvertently disclosure.

As mentioned in the architecture [D4.2, A.9.3] "the Sub-Community Management adopts some of the profile properties of the creating member using the Profile Management component." Which profile properties will be accessible depends on the user who edits the profile of the corresponding Partial Identity.

2.4 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.

This functionality should be also included in a Data Management use case, in case personal data is collected at any other time than during registration.

2.4.1 Use Case 1: Registration

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. This is especially important at

registration time, to avoid impersonation during registration. However, the architecture in D4.2 does not include any safeguards during the registration process.

2.5 PrP21: Data Management

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

It may not be feasible to allow members to express their preferences regarding storage and other aspects of data processing. However, it would be possible to notify a member clearly how data will be managed, and give him/her the ability to safely opt out or cancel membership.

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

2.5.1 Use Case 1: Registration

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. This is considered in the description of the Registration use case.

After the registration "the member can set certain elements of their personal profile to help manage privacy using the Consent Management component." (D4.2, p. 158) The Consent Manager enables the user to decide with whom of the Community he wants to share personal information and how this information can be used.

2.5.2 Use Case 4: Multiple Partial Identities

The Community allows members to set their preferences for sharing Partial Identity profile information at the creation of a new Partial Identity, and upholds their wishes with respect to storage and processing of this data.

2.5.3 Use Case 6: External Services

Each time an external service wants to have access to personal information the Consent Management component is called to check if the user has allowed to share the requested information in the current context. [D4.2, p. 294]

2.5.4 Use Case 7: Content Sharing

According to the description of the Content Sharing use case, members are able to express how imported content can be processed, and their views in this regard are upheld by the Secure Repository.

2.5.5 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. However, this issue is not mentioned in the description of the Sub-Community use case.

2.6 PrP22: End-to-end Privacy

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

Use cases: **none.**

End-to-end privacy is supported by the PICOS architecture by using for example encryption. Nevertheless, end-to-end privacy won't be required in all situations by the architecture because of law enforcement. [D4.2, p.193]

2.7 PrP23: Authentication

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

Authentication is achieved with support from the Access Control component and the Authorisation component." [D4.2, p. 327] The PICOS architecture will support several authentication methods. But which one is depending on the capabilities of the client device. Possible methods could be password, biometric, token and credential. [D4.2, p. 292]

Use cases: 1, 2, 4, 7.

2.7.1 Use Case 1: Registration

Authentication information has to be either collected or generated during registration. The Registration use case takes this into account by requiring several forms of evidence, described in the use case.

2.7.2 Use Case 2: Accessing the Community

Authentication is a crucial aspect of accessing the Community. Changes in the second version of the architecture concerning the access control functionality have to be examined here.

The Access Control component is the first point of contact for visitors to the Community and interacts as a gatekeeper. The Access Control component also still redirects new prospective members to the Registration component. [D4.2, p 229]. The functionality of the Access Control component is the same as in the first version of the architecture [D4.2, p. 229].

2.7.3 Use Case 4: Multiple Partial Identities

It is not possible to authenticate with a Partial Identity. Users may only log in into a Community with their Root Identity. [D4.2, p 156]

2.7.4 Use Case 7: Content Sharing

A member 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. Moreover, it must not be possible for a member or Partial Identity to associate content imported by him or her to another member or a Partial Identity of another member.

These requirements are fulfilled in PICOS. Content is always associated with a Partial Identity belonging to the content provider, which must previously have authenticated to the Community via log-in.

2.8 PrP24: Multiple Persona

Def.: PICOS allows members to have multiple persona.

Use cases: all.

2.8.1 Use Case 1: Registration

Multiple persona is thus enforced already at registration. Creation of a Partial Identity is allowed during registration and necessary to access any service.

A Partial Identity is created by the *Partial Identity Management* component. Each user has to generate at least one Partial Identity. After the registration the R*egistration* component redirect the user directly to the *Partial Identity Management* to force him to create his first Partial Identity. Several other components are involved during the process of creating a Partial Identity [D4.2, p166f].

2.8.2 Use Case 2: Accessing the Community

A Partial Identity is required in order to access the Community. The *Access control* component keeps the access to the Community under surveillance by using the *Authentication* and *Authorisation* components to guarantee that only valid members get access to the Community. However, log in into the PICOS Community is only possible with the Root Identity [D4.2, 229f].

2.8.3 Use Case 3: Revocation

Hence, according to the component description, the Revocation component clearly allows revocation of Partial Identities, thus enforcing Multiple Persona. Personal information of a member is stored in the Root Identity. Therefore, apart from the Pseudonym of the deleted Partial Identity, no other personal information will be deleted.

2.8.4 Use Case 4: Multiple Partial Identities

This use case directly supports the Multiple Persona principle.

2.8.5 Use Case 5 Reputation

The reputation use case supports therefore the principle of Multiple Persona. Reputation is always associated with a Partial Identity.

The functionality of the *Reputation Management* is "to provide an indication of the trustworthiness of an entity (typically a member)". As described in [D4.2, p 266f], the Reputation Management is called by the *External Recommendation*, *Privacy Advisor*, *Trust Negotiation* component, and may call the *Profile Management* component. Each Partial Identity will be handled individually by the *Reputation Management* component. [D4.2, p. 255]

The functionality of the *Feedback Management* component is to provide "a route for members to supply feedback to the Community." [D4.2, p. 245] The *Feedback Management* calls the *Reputation Management* to record reputation information and is called by the *Profile Management* to get the reputation value of the chosen Partial Identity.

Each Partial Identity gets its own reputation. Therefore, the *Partial Identity Management* calls the *Reputation Management* to get actual reputation for the requested Partial Identity.

The *Profile Management* component calls the *Partial Identity Management* component to assign a profile to the Partial Identity [D4.2, p. 256]. The *Feedback Management* is called by the *Partial Identity Management* to pass the entity identities obtained by itself to the Reputation Management. [D4.2, p. 169]

2.8.6 Use Case 6: External Services

The *Anonymisation* component is called by the *Partial Identity Management* component to request an endorsed pseudonym. [D4.2, p 232] The *Partial Identity Management* component itself calls the *External Service Delivery* "to anonymise the identity of the member accessing the external service." [D4.2, p. 244]

External services have not been integrated to the PICOS framework implying no interactions between the WP5 PICOS platform and external unsecured servers [D4.2 8.4.1].

2.8.7 Use Case 7: Content Sharing

The Content Sharing use case assumes Multiple Persona by allowing Partial Identities to be associated with content.

2.8.8 Use Case 8: Presence

Presence information always refers to a Partial Identity.

With the *Social presence* component, members can decide whether their current presence is “online”, “offline” or “not available”. This presence can only be managed for the current active Partial Identities. All non-active Partial Identities are in the presence status “offline”. (D4.2, p. 176f) Thus, there is a contradiction in that point, that the presence non-active Partial Identities cannot be managed by the member. However, this choice was made the architecture in order to prevent linkability between two Partial Identities in the case that they both switch between online and offline at the same time.

2.8.9 Use Case 9: Sub-community

The Sub-community Management component does support Multiple Persona. Only Partial Identities are members of a Sub-Community.

2.9 TrP03: Provenance

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

PICOS ensures that members can rely on the provenance of information. The WP5 PICOS platform implements a strict access control based on requester identity authentication and a secure SSL channel for any interaction with the platform. The requester privileges are enforced by the WP5 components. Content ownership is enforced by the platform to avoid any attack to the user reputation based on rating of a poor content that is associated to the user whose reputation is attacked. [D5.2 8.4.1]

Use cases: 5, 6, 7.

2.9.1 Use Case 5. Reputation

The reputation value should be endorsed by the Community. It is important to recognize the originator of the reputation value as well as knowing the reputation of the contributor of some content. This is enforced by allowing only authenticated members of the Community to provide ratings. Members can provide feedback using each of their Partial Identities (pseudonyms). In each case, feedback is recorded under the corresponding Partial Identity feedback pseudonym. An exception is where a

member can only provide feedback once, e.g. when voting. A member can provide feedback (textural comments) more than once, but can only comment on reputation once. [D4.2 A.5.1]

2.9.2 Use Case 6. External Services

The source of information provided by external services should be recognized.

For external parties it is not possible to upload content to the Community. Thus, reputation for externals is not needed. External Services are handled in the same way like other members of the PICOS Community [D4.2, p. 171]. Therefore, the provenance information of external services is preserved.

2.9.3 Use Case 7. Content Sharing

Content is always associated with the member who performed the import. The system should tag the content with the appropriate information so that it can be easily indentified.

The *Content Sharing* component is responsible for associating tags with content [D4.2, p. 174]. Members must belong to the Community to be allowed to tag content. Content can be tagged with profiles or other meta-data.

2.10 TrP05: Audit

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

The auditing relies on an Event Logging component that collects logging data from all components and allows a filtering of the event on a per user level [D4.2 8.41]

Use cases: all.

As described in [D4.2, p. 176f] all actions performed by the *Presence* component are logged by the *Event Logging* component. There is no automated auditing but on request it is possible to audit this information in a lawful mean.

2.11 TrP06: Objective/Subjective Trust

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

PICOS supports 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 reputation component is designed to filter reputation (and then trust)

attacks. The reputation component offers a way to retrieve all rating events attached to content so that the history can be analyzed [D4.2 8.4.1].

Use cases: 4, 5, 6, 7.

2.11.1 Use Case 4. Partial Identities

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. The Reputation component allows reputation to be attached only to a Partial Identity based on imported content [D4.2, p 266].

Each Partial Identity has its own reputation value based on the published and rated content. Since it is required that the different partials identities of a Root Identity should not be linkable, it is not possible for the member to choose to show several reputation values simultaneously. Root Identities do not have an own reputation value.

2.11.2 Use Case 5. Reputation

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.

As described in [D4.2, p. 266] the *Reputation Management* component "is used to provide an indication of the trustworthiness of an entity (typically a member)" and the *Feedback Management* component's task is to provide "a route for the members to supply feedback to the Community." [D4.2, p. 245]

The reputation of a member of the PICOS Community adds to the reputation of the user itself, depending on the reputation of subjects, topics, items and activities. A particular algorithm to calculate reputation is not defined in the architecture. Also, it is not possible for members to modify the algorithm of the reputation value. The architecture does not define how reputation is gathered.

2.11.3 Use Case 6. External Services

Trust on external services is measured by the reputation of them. However, external services have not been integrated to the PICOS Framework implying no interactions between the WP5 PICOS Platform and external unsecured servers [D4.2 8.4.1].

2.11.4 Use Case 7. Content Sharing

Reputation of members importing content to the Community will be affected by the feedback provided by other members of the Community. Chats can be used to foster subjective trust between Community members.

2.12 TrP07: Consensus

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

All member actions are enforced by the component action owners based on user privileges [D4.2 8.4.1].

Use cases: 9.

2.12.1 Use Case 9. Sub-community

Delegation of a Sub-Community requires the consensus of all its members.

The *Sub-community Management* component is responsible for managing sub-communities created by a Partial Identity [D4.2, p. 313].

2.13 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 (validating the identity of the user), enables a step by step control of any user action. The Event Logging component enables a search event model that allows fast access to the required information [D4.2 8.4.1].

Use cases: 1, 4, 5, 7.

2.13.1 Use Case 1. Registration

Members must provide accurate personal information and are accountable for this.

There are no technical means to control if provided user data is accurate; this is something that can be enforced only by the administrators of each specific Community.

2.13.2 Use Case 4. Partial Identities

A link between the Partial Identity and the Root Identity should be established in case the Partial Identity becomes accountable for some action in the system. In this case, the Root Identity will be accountable for the same action.

This is clearly enforced since Partial Identities are always linked to the Root Identity.

2.13.3 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. Content uploading should be accountable for the benefit both of the members in the reputation management and of the Community provider in case the contents violates the legislation.

There are no mechanisms to check the authenticity of the provenance of imported content, only to check the authenticity of the logged-in user. Events are logged by the platform; based on the logged information, it is possible to hold someone accountable for imported content.

3 Analysis of Threats and Recommendations

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 focus for the analysis of the PICOS Architecture established in D4.2 would be on establishing how the architecture defends against a set of known threats and vulnerabilities. Moreover, a separate evaluation of the architecture with regard to the initial set of trust and privacy principles, established in D4.1, will be also presented.

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 presents 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.

Other documents were also considered. The full list is given in Appendix A.

The evaluation work was carried out in the shape of questions and answers associated with the threats and recommendations extracted from the above literature. We will keep this format below for the sake of readability. We note also that there is some overlap here with the evaluation of the architecture (presented in D3.1.2), and the Community prototypes (presented in D3.3.1), and therefore some repetitions, but for the sake of readability we decided to leave them here.

The rest of this section is organised as follows. In the next section, we focus on the important issue of safeguards, as indicated above. Next, a section is dedicated to the threats to security in general 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. Thereafter, a section is dedicated to the important issue of reputation, which is closely related to trust.

3.1 Safeguards

The principle PrP18 Safeguards is especially important here. This principle is related not to privacy goals, but to privacy vulnerabilities. Hence, a vulnerability analysis is called for here.

3.1.1 Unauthorized access to personal information

This issue is related to PrP13 Third-party Disclosure, and PrP21 Data Management. The following questions were raised.

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

On a general level, the Community provider is able to access all personal information stored on the server side. This data is not encrypted, as the work focused mainly on enhancing privacy against other users and third parties. Therefore, attacks to the server or illegal activities by the platform provider are theoretically possible. This applies also to the Root Identity information. For Third-Party applications and other users only the published personal information of the used Partial Identity is accessible. This applies also for advertisers acting as third parties. The advertising component included in the architecture acts as an intermediary, allowing advertisers to access only selected information about users. A user is able to control which of his personal information is accessible in this case.

Are there countermeasures in this case?

Encrypting stored information could reduce the risk of disclosure.

3.1.2 Identity Theft (Impersonation)

This principle is partially related to PrP13 Third-party Disclosure, but it has a wider significance. Impersonation might affect TrP03 Provenance, and TrP08 Accountability. The following question was raised:

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

No, the platform is not yet providing any opportunities to find out that an identity has been stolen.

3.1.3 Information Aggregation Concerning Partial Identities

This 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. The following questions were raised.

In which way is it possible to link Partial Identities (e.g. location, disconnection, etc)?

The main way to link Partial Identities is to compare personal information of different PIDs and to find out similarities. Additionally, it is possible to link two PIDs if a user switches to another PID and appears on the map with his new PID on the same location as the previous one.

Are there any countermeasures?

The Privacy Advisor will warn the user in the case he enters the same personal information to different PIDs. There will also be a warning from the privacy advisor in the case that user enters any personal information in messages sent to communities or chats.

Against the risk of linking PIDs due to location information there are only limited countermeasures so far. During investigation on the architecture it was decided to hide the location of a non-active PID of a user also in the case he is online with another PID. This is to prevent that more than one PID is shown at the same location at the same time.

3.1.4 Information Storage Vulnerabilities

This issue is 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?

To prevent unauthorized access to the profile the user has several tools at his or her disposal. The privacy policy editor enables users to configure their privacy on a very low level. For each case he can generate a new policy telling who is allowed to access which piece of information. Additionally, the default value of the PICOS platform establishes that no access to personal information is possible. The user has to decide explicitly who will get access to his or her personal information.

3.1.5 Information Transmission Vulnerabilities

This is related to PrP13 Third-party Disclosure, and PrP22 End-to-End Privacy. Also PrP01 Notice of Collection might be affected.

Is it possible to intercept data during transmission?

Yes, but in any case the architecture offers members the option to encrypt data.

Which mechanisms have been used in order to enforce data confidentiality during transmission?

End-to-End privacy is enforced by using encryption for data transmission between the mobile client and the PICOS platform.

3.1.6 Information Collection Vulnerabilities

With regard to information collection vulnerabilities, the following questions might be raised:

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

Apart from the pseudonyms of PIDs it is not possible to collect information without the consent of the data subject. To be allowed to access a piece of personal information of a user, the owner of the data has to explicitly allow the other user to access this information. The data subject is also allowed to require that he or she be asked for permission every time another user wants to access his/her information.

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

Unless the platform is attacked, obtaining data by unfair or unlawful means is only possible to the platform provider. The latter can also collect further information about the user (e.g. secondary data) without informing the user.

3.1.7 Session vulnerabilities

The following questions were raised.

How is a session maintained?

The session management is not treated by the architecture. How a session is maintained is discussed in the implementation of the architecture and the mobile prototype.

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

This is also not part of the architecture.

3.2 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. The threats presented in the following subsections below were specially targeted.

3.2.1 Digital dossier aggregation

This threat refers to the possibility of third parties to download and store profiles on online SNSs, thus creating a digital dossier of personal data. The following questions may be raised in this context.

How are personal profiles protected?

The default is that no personal information is accessible by other users. A user has to explicitly allow access to any piece of personal information.

Can personal profiles be downloaded and stored by third parties?

Users will interact with third-parties also with Partial Identities. Therefore, third-parties can only access information belonging to a linked PID if explicitly allowed.

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

No, personal information can only be used for the purposes established by the user in his/her privacy policies.

3.2.2 Secondary data collection

Secondary data refers to time and length of connections, location (IP address), profiles visited, messages sent and received, and similar. The questions here are concerned with the possibility for third party to collect user secondary data.

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

It is not possible.

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

This is not clear to users because the platform provider does not provide information about the treatment of secondary data in the terms & conditions during the registration process.

Do privacy policies refer to eventually collected secondary data?

Users are not able to manage their secondary data with the help of the privacy policies. The privacy policies allow users to specify access to data only towards other users and third parties.

Is the user informed about privacy policies concerning secondary data?

No, apart from what is included in the terms and conditions, the user is not informed about privacy policies concerning secondary data.

3.2.3 Linkability from image metadata

Greater possibilities for unwanted linkage to personal data is offered today by allowing users to tag images with metadata, such as links to SNS profiles or e-mail addresses. The following question was raised:

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

It is not directly possible to link images to personal data. However, in the comments to pictures personal information like names can be inserted.

3.2.4 Account deletion

It may be impossible for users wishing to delete accounts to remove secondary information linked to their profile such as public comments on other profiles.

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

Users are not able to manage their secondary data.

3.2.5 Spam

Spam refers to unsolicited messages propagated using social network systems, a growing phenomenon.

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

It is just possible to receive messages of friends. It is possible to block them only by deleting the friend from the friend list. In addition, also advertising notifications may be received, but it is possible to block such messages.

3.2.6 Cross site scripting, viruses and worms

SNSs may be vulnerable to cross site scripting attacks and other threats due to widgets produced by weakly verified third parties.

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

The PICOS mobile client is not web-based. Therefore, cross-site scripting is not feasible. Attacking the server or attacking the client software on the phone might nevertheless be possible. This depends on the architecture of the used mobile device and mobile OS.

3.2.7 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 followed?

The Privacy Advisor informs user about trust and privacy issues in an easy to understand manner and in real time.

3.2.8 Stronger authentication and access control

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

Have this issue been considered at all within PICOS?

In the PICOS architecture, CAPTCHAs are not planned to be used for a stronger authentication.

3.2.9 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 for abuse reporting?

Abuse reporting is so far not planned in the architecture.

3.2.10 Default settings

Default settings should be made as safe as possible.

Default settings have been discussed before within PICOS. Which ones have been adopted, and what is their impact on trust and security?

By default all data related to a user is private and cannot be accessed by any other member of the Community unless the user decides to make it available for one specific user or a group of users. The client application allows the customization of the privacy rules in the policy editor in order to enable partial sharing of data.

3.2.11 Means to delete data

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 pubic 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?

Users can remove or delete personal information of their PIDs at every point of time. Additionally, published files can be removed from communities. A context sensitive help can support users in doing this.

3.2.12 Use of reputation techniques

The use of reputation techniques should be encouraged.

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

Users are supported in how they may rate other users; however, the language is not transparent.

3.2.13 Automated filters

Automated filters should be built in. Offensive, litigious or illegal content should be blocked by smart filters.

Are there automated filters in PICOS?

The PICOS is so far not endowed with filters to automatically prevent illegal content.

3.2.14 Consent for 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?

Yes, but the Privacy Advisor can also warn users about tagging images with personal information or profiles.

3.2.15 Spidering and bulk downloads

Spidering and bulk downloads should be restricted. 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, e.g. for advertising purposes?

The PICOS platform does not control the e-mail addresses or verify the identity of the users. The PID concept of PICOS allows users to protect their privacy against other users so that not all information needs to be true.

3.2.16 Search results

The user should be clearly informed that they will appear in search results, and also be 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 users appear in search results, are they informed about it? Is data anonymised in those cases?

Users are informed about it in the terms and conditions.

3.2.17 Spam

Techniques to eliminate **spam** comments and traffic should be developed.

Is there such functionality in PICOS?

There is so far no CAPTCHA features planned, and only the friends of a user are able to send SPAM to him or her.

3.2.18 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?

No, this issue is so far not handled in the architecture.

3.3 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 identifies 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 are included below.

3.3.1 Threats to the reputation system

The main threats to the reputation system are the following:

3.3.1.1 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?

No, because users are allowed to create as many PID as they want and whenever they want.

3.3.1.2 Sybil attack

The attacker creates multiple identities (sibyls) and exploits them in order to manipulate a reputation score. It is important to analyze whether the notion of Partial Identity in PICOS prevent or facilitate sibyl attacks.

Does the notion of Partial Identity facilitate sibyl attacks?

Users are allowed to create multiple identities, but they are not allowed to participate in a Sub-Community with more than one PID. Therefore, they are not able to rate themselves.

3.3.1.3 Impersonation and reputation theft

Reputation theft implies that a user acquires the identity of another user and steals his reputation. The responsibility to mitigate this problem falls on the underlying system, which should develop mechanisms to protect the identity infrastructure. It is important to analyse how this is done in PICOS.

Which mechanisms are used in PICOS to protect the identity infrastructure?

The different PIDs of a user are associated with a unique Root Identity. To steal an identity the attacker has to steal the whole account. Shifting a PID from one root identity to another is not possible.

3.3.1.4 Bootstrap issues

This issue is related to the initial reputation value and the choice of the entry value.

Which is the entry value of a reputation in PICOS? In case a low values is given, are there any means to distinguish a low reputation value because of recent entry and because of bad reputation?

In PICOS the reputation of an identity is based on the rating of his contribution. Therefore, his reputation value is always related to those contributions.

3.3.1.5 Extortion

Extortion by blackmailing a user by damaging his reputation may be facilitated by the lack of formal management/assurance mechanisms for reputation and the lack of data quality assurance. Those mechanisms should therefore be put in place, and data quality should be assured.

Are there any mechanisms to prevent extortion in PICOS?

No, there are so far no mechanisms in the architecture to prevent extortion.

3.3.1.6 Denial-of-reputation

This implies a concerted campaign to damage the reputation of an entity, e.g. by falsely reporting on the victim's reputation or identity theft. Countermeasures to this threat are not well developed, and the investigation of new mechanisms to defeat automated attacks to reputation systems is encouraged.

Does PICOS consider this issue?

So far PICOS does not consider this issue.

3.3.1.7 Bad stuffing and bad mouthing

A number of users may agree to give positive or negative feedback to one entity. A proposed countermeasure is "controlled anonymity.
Has this threat been analysed in the light of the Partial Identity concept in PICOS?

No, the focus has been on the reputation of members.

3.3.1.8 Repudiation of Data

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

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

The logging mechanism may be used to prevent denial of uploaded content.

3.3.1.9 Recommender's dishonesty

A reported reputation depends on the trustworthiness of the user who provides reputation feedback. Mechanisms to mitigate this threat are the introduction of weightings to a reported reputation score according to the reputation of the voters, or allowing only voters from a trusted social network.

Is weighting based on reputation score of the voter part of PICOS reputation algorithm?

Yes, weighting is part of the reputation algorithm implemented in the platform.

3.3.1.10 Privacy threats for voters and reputation owners

If the privacy of the voters is not guaranteed, there is a risk of voting distortion due to fear and other threats. There are also threats against the reputation owners. Pseudonyms are used to enhance privacy, but can suffer from linkability.

How does the notion of Partial Identity in PICOS may help in mitigating linkability?

Linkability is intended to be avoided as far as possible. PIDs are intended to provide different information about users but it cannot be totally prevented that such information leads to links between PID profiles in some cases. In addition, a user is warned by the PA when he or she intends to publish the same information in different PID profiles.

3.3.1.11 Risk of Herd Behaviour and Penalisation of Innovative, Controversial Opinions

Innovative opinions may lead to bad reputation, at least initially, and penalise creative thought. Countermeasures include allowing the computation of personalised reputation scores by means of local trust metrics. The notion of Partial Identity may be an important mechanism for reducing this threat.

How does the notion of Partial Identity reduce the risk of herd behaviour?

Herd behaviour depends on the transmission of thoughts or behaviour between individuals and the patterns of connections between them. A strong factor regarding the patterns of connections is the social pressure of conformity. Most people are very sociable and have a natural desire to be accepted by a group, therefore following the group is an ideal way for becoming a member, not being branded personally as an outcast. A Partial Identity grants anonymity to a user, allowing him to express controversial opinions without fear of damage to his/her overall reputation or to himself/herself as a person. Damage inflicted to his/her reputation is limited to the Partial Identity and not to his/her overall reputation and social standing.

3.3.1.12Attacks to the Underlying Networks

The reputation system can be attacked by targeting the underlying infrastructure, especially in centralised reputation systems. A threat analysis can be performed here, although this would be more relevant for the design platform and Community prototypes.

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

The PICOS platform is built on a secure system with several mechanisms to prevent attacks against it.

3.3.1.13Threats to Ratings

These threats include threats against the secure storage of reputation ratings, against the privacy of voters, against the metric used by the system to calculate the aggregate reputation, and the reputation scoring itself.

Are there any countermeasures in PICOS against threats to ratings?

Users are allowed to create multiple identities, but they are not allowed to participate in a Sub-Community with more than one PID. Therefore, they are not able to rate themselves.

Content ownership is enforced by the platform to avoid any attack to the user reputation based on rating of a poor content that is associated to the user whose reputation is attacked [D4.2 8.4.1].

3.3.2 Security

Security requirements for reputation systems include the following:

3.3.2.1 Usability/Transparency aspects

How transparent is the reputation system to users?

The syntax is not transparent to the users.

Can the reputation be customized by a user?

No.

Is qualitative assessment of reputation offered to users?

Users can comment on the content.

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

No, no open description of the reputation metrics is available.

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

The architecture does not include a reporting system to report on inappropriate content.

3.3.2.2 Availability

This is important when the reputation system becomes critical to the functioning of the overall system.

Does PICOS enforce availability in some way?

PICOS availability depends on the internet connection of the mobile devices. Therefore, the availability can only be guaranteed by the server side and not for the connection.

3.3.2.3 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?

Users are only able to rate content and not other users directly. Additionally, users cannot rate their own content, because they are only allowed to interact with one of their PID in each Sub-Community.

3.3.2.4 Entity authentication and access control

Identity management mechanisms need to be in place to mitigate the risks related to identity change like sibyl attacks.

Which identity management mechanisms are included in PICOS?

Profile Management and Partial Identity mechanisms are available. Additionally, users can change quickly their presence, their location and availability, or their PIC.

3.3.2.5 Privacy/Anonymity/Unlinkability

Privacy should be preserved.

Analyse the use of Partial Identities in this context.

PIDs allow users to share particular information with other particular users. Users may use different PIDs in different contexts, whereby privacy is enhanced.

3.3.2.6 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?

This is defined within the platform. Newcomers start with a neutral reputation of 50 in a 0-100 scale.

3.3.2.7 Accountability

Each peer should be accountable in making reputation assessments.

Is accountability in making reputation assessments enforced in PICOS?

No, this is not enforced.

3.3.2.8 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, there are no special mechanisms for this available in PICOS.

3.3.2.9 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?

Reputation is based on the content uploaded by the users. With more positive feedback they are able to enhance their bad reputation; the user may also change his PID for this purpose.

3.3.2.10 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?

Reputation is based on the content an identity provides to the Community. Therefore, proof may be obtained based on good ratings. Ratings are based on the subjective views of users, and therefore an automated verification is not possible.

3.3.2.11 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 done by allowing just one PID of a user in each Sub-Community.

3.3.3 Recommendations

Recommendations to designers of reputation systems include the following:

3.3.3.1 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 that assist users in choosing pseudonyms. The Partial Identity concept user in PICOS should be analysed in the light of these recommendations.

How might the partial identity concept in PICOS enhance privacy in the sense exposed above?

The reputation system has two protection goals. One goal is the absolute linkability of membership in a reputation network. The second one concerns unlinkability and anonymity of actions for all entities involved. By making use of PIDs, absolute linkability is obtained by linking the Partial Identity to the root id, whereas unlinkability of actions is enforced by the use of distinct PIDs.

3.3.3.2 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, the users do not have a description of the reputation metric used in PICOS.

3.3.3.3 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 how to assess the trustworthiness of the reputation system?

The reputation and rating syntax of PICOS is not transparent to the users.

3.3.3.4 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, this is not possible.

3.3.3.5 Qualitative assessment of reputation

Reputation systems should be based on qualitative metrics, and should use a combination of quantitative and qualitative approaches whenever an application allows it.

Does PICOS use a combination of qualitative and quantitative metrics?

This issue is not considered at the architecture level.

4 The Assurance case

The development of an assurance case conforming to the assurance approach proposed in PICOS, and explained in detail in [VAL10], would require the creation of a complex dedicated tool in order to manage its inherent complexity. The development of such a tool has been left as further work given that the effort it would require exceeded what was initially planned in PICOS. We estimated that for the second cycle of PICOS it would be more pragmatic to expose the assurance results in common language rather than as claims in a much less conspicuous assurance case tree. However, it is our belief that the proposed assurance approach has been validated during our assurance work in PICOS, and in order to give at least an illustration of the method we present below a walk-through of a possible branch of the assurance case, obtained by adding some results of the threat analysis presented here to the assurance case defined in D3.1.1. We note also that the following example yields only a simplified picture of a realistic assurance case for illustrative purposes; a full-fledged assurance case would be much more complex and contain many more details.

We focus on the principle PrP 13 Third-Party Disclosure, *PICOS requires Notice and Consent of the Data Subject to disclose information to third parties*, which corresponds to the branch 1.2.1.5.1 in the assurance case tree. We sketch how this claim would have been developed into subclaims, and recursively focus on one of those subclaims and develop it further; otherwise only the headings of the sibling claims of each of the claims included in the walk-through are shown.

The strategy for deriving subclaims was to analyse the relevant use cases with regard to the principle, including now a threat analysis. This claim is reduced to several subclaims. The first two subclaims, 1.2.1.5.1.1 and 1.2.1.5.1.2, correspond so simple claims about two components, Social Presence and Sub-Community, which supposedly would directly support the claim. Thereafter follows a series of subclaims directly related to the threat analysis shown above in Sect. 3.1 in this document.

For instance, Claim 1.2.1.5.1.3 corresponds to a threat against Third-Party Disclosure concerning unauthorized access to personal information. This claim describes a threat or vulnerability, and says that the threat has been targeted in the way illustrated by its subclaims, each one referring basically to the presence of a feature or the implementation of a mechanism mitigating or preventing the threat. One of these features, corresponding to Claim 1.2.1.5.1.3.2, says that a user is able to control which of his personal information is accessible in this case. This claim, by its turn, is supported by three new subclaims. The first one of these subclaims, Claim 1.2.1.5.1.3.2.1, says that Claim 1.2.1.5.1.3.2 is enforced with the aid of the *Profile Management* component. Further evidence on how this component enforces this claim can be provided as subclaims to Claim 1.2.1.5.1.3.2.1.

We believe that this example illustrates how the results provided in the threat analysis present in Chapter 3 fits nicely into the assurance case structure. It shows also the important interplay between the claims corresponding to the PICOS principles (in this case PrP 13 Third-Party Disclosure), the eventual threats negating this principle (unauthorized access to personal information), and the functionality provided by the components of the architecture aimed at enforcing the principle or counteracting the threat (Profile Management).

Here follows the snapshot of the assurance case tree discussed above.

1. **Privacy and Trust:** *PICOS complies with all established trust and privacy principles.*

Strategy for deriving subclaims to 1: separate the trust from the privacy principles.

1.1. Trust: PICOS complies with all established trust principles.

1.2. Privacy: *PICOS complies with all established privacy principles.*

Strategy for 1.2: decomposition of the privacy principles established in D4.1, refined according to what is explained in D3.1 Sect. 3.3.

1.2.1. *PICOS complies with relevant legislation*

Strategy for 1.2.1: decomposition according to D3.1 Sect. 3.2.1

1.2.1.1. **Notice**: *PICOS complies with the notice principle.*

1.2.1.2. **Notice**: *PICOS complies with the consent principle.*

1.2.1.3. **Collection Limitation**: *PICOS complies with the Collection Limitation principle.*

1.2.1.4. **Use Limitation**: *PICOS complies with the Use Limitation principle.*

1.2.1.5. **Disclosure**: PICOS *complies with the Disclosure principle.*

Strategy for 1.2.1.5: decomposition of Disclosure into 3 principles according to ISTPA [IST07], in which only two of them are included in PICOS.

1.2.1.5.1. **PrP 13 Third-Party Disclosure**: *PICOS requires Notice and Consent of the Data Subject to disclose information to third parties.*

Strategy for 1.2.1.5.1: analysis of PUC 2: Accessing the Community, PUC 7: Content Sharing, PUC 9: Sub-community, UC 10: Data Management; Threat Analysis

1.2.1.5.1.1. Third-Party Disclosure is enforced with the aid of the *Social Presence* component.

1.2.1.5.1.2. Third-Party Disclosure is enforced with the aid of the *Sub-community Management* component.

1.2.1.5.1.3. **THREAT** to Third-Party Disclosure: Unauthorized access to personal information

Strategy for 1.2.1.5.1.9: Countermeasures blocking unauthorized access

1.2.1.5.1.3.1. For Third-Party applications and other users only the published personal information of the used Partial Identity is accessible (see 3.1.1)

1.2.1.5.1.3.1.1. Enforced with the aid of the *Access Control* component

1.2.1.5.1.3.2. A user is able to control which of his personal information is accessible in this case. (see 3.1.3)

1.2.1.5.1.3.2.1. Enforced with the aid of the *Profile Management* component

1.2.1.5.1.3.2.2. Enforced with the aid of the *Consent Management* component

1.2.1.5.1.3.2.3. Enforced with the aid of the *Social Presence* component

1.2.1.5.1.3.3. The privacy policy editor enables users to configure their privacy on a very low level. (see 3.1.3)

1.2.1.5.1.3.3.1. Enforced with the aid of the *Privacy* Policy *Editor*.

1.2.1.5.1.3.4. The default value is no access to personal information; the user has to decide explicitly who will get access to his or her personal information

1.2.1.5.1.3.4.1. Enforced with the aid of the *Privacy* Policy *Editor*.

1.2.1.5.1.4. **THREAT** to Third-Party Disclosure: Impersonation

Strategy for 1.2.1.5.1.9: Countermeasures against impersonation

1.2.1.5.1.4.1. NO COUNTERMEASURES AVAILABLE (see 3.1.2)

1.2.1.5.1.5. **THREAT** to Third-Party Disclosure: Information Storage Vulnerabilities

Strategy for 1.2.1.5.1.9: Countermeasures against attacks to information storage

1.2.1.5.1.5.1. Encryption of data

1.2.1.5.1.5.1.1. NOT IMPLEMENTED.

1.2.1.5.1.6. No user data is disclosed outside the Community, and within the Community only with the consent of the user

1.2.1.5.2. **PrP 14 Third-Party Policy Requirem**ents: *PICOS ensures that any third parties are informed of the privacy policies of the Community and will follow them or possess equivalent policies.*

1.2.1.6. **Access and Correction**: *PICOS complies with the Access and Correction principle.*

1.2.1.7. **Security and Safeguards**: *PICOS complies with the Security and Safeguards principle.*

1.2.1.8. **Data Accuracy:** *PICOS complies with the Data Accuracy principle.*

1.2.1.9. **Openness**: PICOS complies with the Enforcement principle.

1.2.2.PrP 21 Data Management: *PICOS allows members to express how to store and process their data and uphold their wishes in this regard.*

1.2.3.PrP 22 End-to-end privacy: PICOS supports end-to-end privacy.

1.2.4.PrP 23 Authentication: *PICOS supports multiple forms of Member authentication, while continuing to respect privacy.*

1.2.5.PrP 24 Multiple Persona: *PICOS allows members to have multiple persona.*

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

5 Conclusions

In this deliverable we have presented an analysis and evaluation of the trust and privacy functionality of the Platform Architecture and Design 2, described in D4.2. We have focused on two points:

1. A revision and updating of the results of the analysis of the Platform Architecture and Design 2 with regard to the Community prototype 1.
2. An evaluation of the prototype with regards to the threats and recommendations put forward in several reports published by ENISA (European Network and Information Security Agency), and others.

Concerning the first point, we consider that most questions raised in the first cycle with regard to the trust and privacy principles have been met.

With respect to the second point, it is important to point out that the recommendations are not PICOS requirements (most have been presented later than the start of the PICOS project), and have thus not been considered in the design of the architecture. Nevertheless, our analysis gives outsiders a useful account of what they may expect from PICOS with regard to these recommendations. Many of those recommendations cannot be solved by technical means, and should be enforced by the administrator of each specific Community, whereas others are relevant mainly for the evaluation of the platform or the prototypes, and hence have been considered in the corresponding deliverables, D3.2.2 and D3.3.2.

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**: PICOS is a project that focuses on privacy, hence the results of the evaluation in this area not surprisingly satisfactory. 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**
  - Users are notified of the applicable policies in terms of Consent, Access and Disclosure. Notice of collection, terms and conditions, and policies, are provided at an appropriate time. Terms and conditions explain the global Community policies related to data collection and data retention and are displayed before the final step in the registration process.
- **Collection and Use of Personal Data**
  - Data collected by the platform are completely under the control of the End User. The user is able to manage consent via the policy rules that can be modified via the client application. Personal data is collected by fair and lawful means, used only for the purposes stated at time of collection, not retained longer than necessary, and only personal information relevant for the stated purpose is collected. Data Subjects are able to update or correct personal information held by the Community operator.

When the user is revoked, all user attributes are deleted. The event logging is kept for auditing purpose. No user data is kept in the event logging files. Any data collected on the End User is made available to the End User through the client application.

- **Data and Identity Disclosure**
  - The PICOS architecture upholds the member‘s wishes with regard to information flow. Consent of the Data Subject is required to disclose information to third parties. 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:** this was considered to be a concern of the platform prototype (evaluated in D3.2.2) rather than the platform design; we categorise safeguards into authentication, authorization, and confidentiality.

- **Authentication**
  - The PICOS architecture supports multiple methods of authentication through the Authentication Selector Method; however, the methods themselves are not defined in the architecture.
- **Authorization**
  - Implemented within each WP5 component with support from the Policy component.
- **Confidentiality**
  - Confidentiality is enforced within the platform.

3. **Trust:** we categorise trust into three main topics: accountability, provenance, and reputation.

- **Accountability**
  - 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, enable a step by step control of any user action. The event logging component provides a search event model that allows fast access to the required information. The Accountability component monitors the behaviour of members in order to build trust confidence in the Community.
- **Provenance**
  - PICOS ensures that members can rely on the provenance of information, an issue that is treated mainly at the platform level. This may be done also with help of the Non-repudiation component, which adds a non-reputable binding to all content that is provided to the Community.
- **Reputation**
  - PICOS supports both objective and subjective methods for assessing trust. Reputation is based on rating of content and contribution pushed to Community or Sub-Community repositories. The reputation component is designed to filter reputation attacks. Although several open questions related to reputation have been addressed in developing the architecture, there are open research questions reputation that to some extent remain unanswered and might the subject subject of future research.

Hence, concerning the first point above, privacy, we may conclude that the PICOS platform meets the established requirements in a satisfactory way. However, we note here the role of the privacy advisor is still open to discussion and should be further investigated.

As to the second point, safeguards are a concern that has been considered mainly by the platform, not the architecture design. This conforms to current practice, although we believe that security requirements should be taken into account very early in the development process, and hence in the architecture design. It is well known that late integration of security issues is often a source of vulnerabilities, and also a hinder to assurance.

Concerning the third point, trust, which is usually harder to evaluate than privacy, we may say that both accountability and provenance are well gathered for in PICOS. The topic in which we believe that further improvement and research is required is reputation, especially with regard to the notion of Partial Identity in relation to privacy and provenance, a complex issue. Although privacy is clearly enhanced by the notion of Partial Identity, we consider that the trustworthiness of a system based on this concept is still an open issue that should be further researched in the future.

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., "A summary of PICOS WP3 sub-phase 3.1 deliverables", Final Public Deliverable of EU Project PICOS, Sep 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 (last access: Dec 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 (last access: Dec 2010).

[D5.1] Kyritiades, L., "D5.1 Platform Prototype 1", Public Deliverable of EU Project PICOS, Oct 2009. Available at http://picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP5_Platform/D5.1_Platform_prototype_1/PICOS_D5_1_Platform_Prototype_1_v1_1_Final_Public.pdf (last access: Dec 2010).

[VAL10] Vivas, J, Agudo, I. López, J. "A methodology for security assurance-driven system development", Requirements Engineering, 09 Nov 2010, pp. 1-19, Springer.

[WP3] Assurance of Technical Trust and privacy properties.

[WP4] Platform Architecture & Design.

[WP5] Platform prototype Development.

[WP6] Communities Prototype Construction.

Appendix A Reports consulted

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