Grant Agreement no. 215056

Title:	***D3.2.2 Trust and Privacy Assurance Evaluation for the Platform Prototype 2***
Editors:	*José Luis Vivas & Isaac Agudo (Universidad de Málaga)*
Contributors:	*José Luis Vivas & Isaac Agudo, University of Málaga (UMA), Marek Kumpost (Masaryk University Brno)*
Reviewers:	*Jean-Francois Coudeyre (HPF), Stephan Heim (GUF)*
Identifier:	*D3.2.2*
Type:	*Deliverable*
Version:	*1.0*
Date:	*15.1.2011*
Status:	*Final version*
Class:	*Public*

Summary

This deliverable provides an early evaluation of the PICOS Platform Prototype 2. The main purpose of this deliverable is to ensure that the PICOS platform is consistent with the technical trust and privacy principles assessed in the platform architecture and design. Our focus has been the detection of non-conformances in the specification and implementation of the platform with respect to the established privacy and trust principles. The specification and implementation of the PICOS platform have been assessed with regard to the initial trust and privacy requirements. We present both a revision of the findings established in D3.2.1, and an analysis of threats, risks and vulnerabilities concerning trust and privacy in the PICOS platform prototype. Although not part of the initial set of requirements for the platform, but nonetheless partially covered by the requirements of Safeguards included in the European Data Protection Directive, which PICOS is supposed to enforce according to the PICOS requirements, we explain how the platform defends against a set of known threats and vulnerabilities derived directly from several ENISA publications that relate to social networking.

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
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 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 eave 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 3.2 Evaluation of Platform prototype

Having assured that the architecture and design of the platform are consistent would be an incomplete work if the prototype implementations are not accurate too. The reason is that there may be potential errors that could occur during the development phase of the working prototype in WP5, even when the underlying architecture complies with the initial stake-holders requirements. That risk must be somehow avoided or addressed. More precisely, it is necessary to assure that trust and privacy properties hold after the integration of the additional requirements derived from the nature of user trials and target communities. Task 3.2 will evaluate the documentation and functionality of the platform prototype concerning its conformance with established assurance criteria. Furthermore, and what is essential, the tool-box produced as part of the platform development WP5 must be assessed, and new interfaces have to be analyzed, e.g., those to network-based services/resources and to business support systems, as well as the portal interfaces for community administrators and members. The direct outcome of this sequence of steps will be the two versions of the deliverable D3.2 in the two cycles of Phase 3 of the project plan.

Foreword

Deliverable D3.2.2 is a collective work by the WP3 Assurance team, whose members are listed below.

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), Marek Kumpost (Masaryk University Brno), CZ (BRNO)

Table of Contents

List of acronyms

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

1   Assurance

Complementing the assurance evaluation of the PICOS platform prototype performed in the first cycle of the PICOS project, and presented in deliverable D3.4.1, for the second phase we concentrate on both a revision of the findings established in D3.2.1, and further on an analysis of threats, risks and vulnerabilities concerning trust and privacy in the PICOS platform prototype described in D5.2a and D5.2b. Thus, this document explains how the platform 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 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 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 a presentation of the results of the analysis carried out with respect to the second version of the platform prototype, 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; finally, in Chapter 4 we show the conclusions.

2   Revision of D3.2.1

For the second version of the PICOS platform prototype, we give below an analysis of each of the principles included in the previous section with regard to each use case and related components, and according to the analysis carried out in D3.2.1 concerning the first version of the platform Architecture specified in D5.1.

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.

Use Cases: 1.

2.1.1   Use Case 1: Registration

Notice of the purpose of collection should be provided before any data collection during registration.

Components: Registration

2.1.1.1 *Registration component*

Registration involves an individual introducing themselves to the community and establishing the right to gain access. This process usually involves the individual supplying information, some of which can be personal. [D4.1 9.7.10.2]

The registration functionality described in D4.1 is implemented in WP5 through a combination of the Registration component, the Partial Id component and the Public Community component. WP5 provides a web services API to achieve the registration. However, to achieve the registration process as described in D4.1, the client application (WP6) must call a sequence of functions of this API. [D5.2a 3.1]

The description of this component should include the functionality for noticing collection, which was missing in D5.1. This has been done now in [D5.2a 4.1]:

Client application: display of the login screen with a button/link to register. The user clicks on the link. The client requests the public community terms and condition (public community component).

Client application: The client displays the terms and conditions and makes sure that the user has read/scrolled the whole text and accepts these conditions that should include a description of the community policies about privacy.

Client application: when the user accepts the conditions and only if he accepts, the client application switch to the register form where user is asked for his login/password, profile and information and possibly privacy rule customization.

2.2   PrP10: Fair and Lawful Means

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

Use Cases: 1, 4.

2.2.1   Use Case 1: Registration

Collection of information during registration must be made by fair and lawful means. This principle should be enforced at least by providing notification of collection, policy notification, and informed consent.

Collection by fair and lawful means during registration should be enforced with the help of the Registration component. In D5.1 there was no mention in the registration use case about this issue.

Components: Registration

2.2.1.1 Registration component

The registration functionality was declared in the WP5 Platform Design Decisions document to be implemented *"through a combination of the Registration service, the Partial Id service, and the Public Community service."* [WP5 PDD 3.1]

We noted in D3.2.1 that neither the Partial Id service nor the Public Community services were included among the components of the Registration call flow. This has been fixed in D5.2a [D5.2a 4.1, p74]. We noted also that safeguards to ensure secure communication were not included in the description of the register call flow. This is still true in D5.2a, where the call flow is described. However, it was explained to the assurance team that it was decided to rely on the security provided

by the mobile communication channel itself and that developing additional security would not bring value for the purpose of the prototype evaluation.

2.2.2   Use Case 4: Multiple Partial Identities

It is important to ensure that all personal information contained in the profiles have been collected by fair and lawful means. Mixing personal information with partial identity profile information may be a source of problems and obscurities with regard to the legal aspects of data collection and processing.

Collection of profile data during creation of new partial identities should not involve further collection of personal information, as this would contradict the principle that personal data must be collected fair and legally. It is therefore not appropriate to collect personal data during the creation of a partial identity. For PICOS this implies that personal data that has been disclosed by a member, as part of a partial identity profile or as imported content, shall never be used in the personal profile of the member, i.e. the profile of the root identity, since this would amount to collection of personal information without the consent of the data subject and without having previously provided notice of collection.

Components: Partial Identity Management, Profile Management.

2.2.2.1 Partial Identity Management

This component is implemented in WP5 by the Partial Id manager, with basically the same functionality both in general and in PUC 4. End users can select either the primary identity or added partial Identities to use the platform services. A partialId Object owns only a sub-set of the User attributes. PartialId automatically inherit from user Object the generic attributes as location or profile attributes. Moreover, attributes like location that are not redefined at the partial Id level can still be accessible using a partialId.

The primary identity profile contains the full definition of the user information that can be only partially redefined by the partial Id profile. For instance, the gender of the user cannot be redefined. Creating a partial identity also creates a specific context for the user-profile, the presence, the privacy rules and the reputation. These identities are used to reference the user in any operation in the public community. Identities are externally known through the notion of pseudonyms which is the only mandatory field of the profile to complete. These identities are internally referenced using either the rootId (for primary identity) or a partialId which are not supposed to be revealed to the End User. RootId and partial Id are thus internal IDs which have a specific syntax to preserve uniqueness. The partialId component is launched when a new request is received and exits when the response is transmitted. [D5.2b 3.3.8]

2.2.2.2 Profile Management

This component has the same functionality in WP5 PUC 4 as in WP4

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.

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

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.

The principle should be enforced by the Presence component, which, according the description given in [WP5 PDD 2.11] "enforces privacy rules attached to presence information by interacting with the policy manager".

Components: Access Control, Social Presence, Consent Management, Profile Management

2.3.1.1 Access Control

The Access Control functionality described in D4.1 is implemented in WP5 in the Proxy Web Service and via the deployment architecture that is described in the functional specs.

2.3.1.2 Social Presence

Privacy rules allow the definition of rules that may request user authorization when another user wants to access presence information or subscribe to presence. These default rules are provisioning by the application as global community policies. Then the client application can customize these rules on a per primary/partial identity level.

Privacy rules may restrict presence access to a list of users or a sub-community. The client application is using the policy interface to provision these rules. [D5.2a 2.6.8]

2.3.1.3 Consent Management

The Consent manager is not described in D5.2a or D5.2b.

2.3.1.4 Profile Management

The profile server enforces the policies defined in the policy server and attached to the profile attributes of a user or a partial identity. It supports a policy server "allow", 'disallow" or "askOnce" answer. For the askOnce answer, the profile server will send an authorisation request to the owner of the profile requesting permission to perform the required action on the profile, thereafter enabling or disabling the access based on the End user response. [D5.2a 2.6.17]

The Profile server checks for a global profile policy. If none exists, it will check for a policy attached to individual element of the profile, and upon a "getprofile" request will return only the elements that were made accessible to the requester. [D5.2a 2.6.17]

2.3.2   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.

2.3.3   Use case 7: Content Sharing

Members must be able to express how imported content can be exported, and their view in this regard must be upheld.

In D5.1, only real time content sharing is described in the call flow. Tagging was used in the architecture to express a member's wishes with regard to disclosure, but in D5.1 tagging is not mentioned, and only once in D5.2a and D5.2b.

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.

As explained in D3.2.1, this use case complies with principle PrP 13.

2.3.4   Use case 9: Sub-Community

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

Components: Sub-Community Management, Profile Management

2.3.4.1 Sub-Community Management

Sub-communities created in this way take on some of the characteristics of the creating member. [D4.1 13.9.1]

The role of the Sub-community Management component is to facilitate the integration of an external community or a sub-community into a member's profile.[D4.1 9.7.12.2]

In D5.2a and D5.2b nothing is said about how sub-communities take on some of the characteristics of the creating member, as specified in D4.1. It is important that this use of the member's profile does not disclose information to third-parties without notice to the creating member and consent.

The client application can decide to allow association of privacy rules to each published contribution. Privacy rules can apply to the contribution itself or to sensitive attributes of the contribution like the publisher information. Policy enforcement has been modified in the second cycle to allow rule definition per public community Object instance [D5.2b 3.3.16].

2.3.4.2 Profile Management

As the sub-community is created, it adopts some of the profile properties of the creating member using the Profile Management component.[D4.1 13.9.1]

There is no mention in the description of the Profile Management component in D5.2a about this functionality.

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

No safeguards are included in the description of the registration use case in D5.2a. Although safeguards were considered important in WP5, choices were made on where to focus the engineering resources in the platform development, and it was decided to rely on the security provided by the mobile communication channel itself.

Components: Registration

2.4.1.1 Registration

No mention is made in the description of the Registration component in D5.2a about possible safeguards to ensure secure communication and authentication during the registration process.

However, it is explained in D5.2b that all exchanges between the client application and the wp5 platform (up to the proxy) are carried over a secure channel using https [D5.2b 3.1.1].

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.

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.

Components: Registration, Consent Management

2.5.1.1 Registration

According to D5.2a [D5.2a 2.6.1], a new user context is created in each component that deals with user attributes. A set of customizable policy rules (based on default policies) is attached to the attributes of that particular user, identified by the rootId). Default policies are also defined.

The platform create user context in several components: presence, location, RT content sharing, private room, profile. User specific privacy policies are set, and customized rules are stored that may have been redefined by the end user at the policy component level. [D5.2a 4.1]

The principle can be regarded as fully supported by the platform.

2.5.1.2 Consent Management

The Consent manager is not described in D5.2a or D5.2b.

2.5.2 Use Case 4: Multiple Partial Identities

The community must allow members to set their preferences for sharing partial identity profile information at the creation of a new partial identity, and uphold their wishes with respect to storage and processing of this data.

According to the description given in D5.2a [D5.2a 4.4], in order to create a partial identity the client application displays a form to be filled with personal static information. Attached to these data, privacy rules can be defined to allow/restrict access to the partial Identity profile attributes. Thereafter the platform provisions the new identity with the aid of several (presence, location, contact). The partialId can then be used in any transaction with the platform. Privacy policies can be defined on a

per identity basis. Privilege that depends on the role of the user in various resources (public community, sub-community, and forum) are a combination of rootId privileges and partialId privileges. Moreover, the partialId automatically inherits from the rootId privileges as far as public community privileges are concerned .

The principle can be regarded as fully enforce in the use case.

Components: Partial Identity Management, Profile Management

2.5.2.1 Partial Identity Management

According to D5.2a [D5.2a 4.4], the partialId component does the orchestration of the creation and deletion of the partialId as well as the user profile associated to each partialId. The partialId component is in charge of consolidating the rootId and the partialId profiles so that attributes that are common to all partialId profiles and stored in the rootId profile are automatically updated in the partialId profile during retrieval. Privacy rules can apply to all attributes of a user profile.

2.5.2.2 Profile Management

For implementation reasons, the profile server functionalities have been integrated into the partialId component.

The profile component is in charge of managing profiles attached to identities (rootId or partialId). The profile server enforces the policies defined in the policy server and attached to the profile attributes of a user or a partial identity. It supports either a policy server "allow", 'disallow" or "askOnce" answer. For the askOnce answer, the profile server will send an authorisation request to the owner of profile to ask for permission to perform the required action on the profile. It will then enable or disable the access based on the End user response. The Profile server check for a global profile policy. If none exists, it will check for policy attached to individual element of the profile and upon a "getprofile" request, will return only the elements that were made public for the requester. [D5.2a 4.4]

2.5.3   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.

2.5.4   Use Case 7: Content sharing

Members must be able to express how imported content can be processed, and their view in this regard must be upheld.

According to D5.2a [D5.2a 4.7], pushing content must comply with the policy rules attached to the different repositories or to the different forums. The enforcement of user privileges is achieved by creating a situation composed of a requester, a repository and an action (read, write, delete; move…) that the requester wants to perform on the resource and by asking the policy manager to evaluate the situation. The policy manager will then determine if there is a valid rule that can be used to evaluate the situation. The policy manager replies with an action status to allow or disallow the action.

The principle is fully enforced in this use case.

Components: Real Time Content Sharing, Policy Server, File Repository, Privacy Advisor.

2.5.4.1 Content Sharing

According to D5.2a [D5.2a 4.7], the real time content sharing is based on a communication and invitation model where the creator of the communication selects a list of contacts and starts a chat with these potential participants. Notifications for communication invitation are sent to each participant who can accept or refuse to be part of the chat.

2.5.4.2 Policy Server

According to D5.2a [D5.2a 2.6.10], the policy manager is in charge of storing rules attached to various Objects or attribute of Objects as well as evaluate user actions based on the set of rules. It embeds the intelligence required to evaluate rules and deliver a status on the required action.

Other components are responsible for asking the policy manager to evaluate action on resources like user attributes (privacy) as well as community resources for user privilege. However, it is the responsibility of the invoker component to enforce the response sent back by the policy manager.

2.5.4.3 File Repository

Each content is identified by a content Id that is unique and that is allocated each time a new content is pushed to a repository or a contribution is pushed to a forum.

2.5.4.4 Privacy Advisor

The privacy Advisor plays a role during content sharing by making sure that private information is not sent in messages or content attributes do not contain sensitive information such as location.

According to D5.2a [D5.2a 4.7], the first action of the component in charge of sharing content is to call the privacy advisor and wait for an approval from the PA to continue the content sharing processing. Then the PA will check if sensate information is part of the content attributes and part of the body if the body contains text. In case of sensitive information found, the PA will inform the requester about what he found and wait for the end user approval. If the user accept to make sensitive information public, he sends back to the PA a positive answer which will trigger the approval of the PA and the content is accepted.

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.

Components: Sub-community Management

2.5.5.1 Sub-Community Management

The Sub-community rules are defined using the policy manager and pre-provisioned before the start of the service. The rule evaluation is then enforced by the sub-community. The rules attached to sub-community resources define who (either a particular user or a role (member, admin) of the public community or a role of the sub-community) can perform which action. These rules can be attached to any sub-community (default rules) or to a particular sub-community (although it is not used in the current version of the platform). Sub communities also support private forums that can only be accessed by the members of the subcommunity. A Sub-community forum is equivalent to public community ones except that only one Forum is supported per sub-community. Then multiple discussions can be launched where members of the sub-community push text contributions with optional attachment [D5.2a 2.6.11].

2.6   PrP22: End-to-end Privacy

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

Use cases: none.

Not applicable [D5.2a 7.21].

2.7   PrP23: Authentication

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

The phase 1 prototype supported only one way of authenticating the end user. This has not been changed in phase 2.

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 principle is not enforced here since only one form of authentication is used. This was a collective decision at the beginning of the project since it was considered that there was no innovation that PICOS was able to bring here compared to what is currently available in the market, and also that it was better to focus on implementing PICOS innovations.

Components: Registration

2.7.1.1 Registration

The platform checks the uniqueness of some elements (login name, pseudo) and may refuse the register. If no error is found, then it creates rootId and store login information in the authentication component. [D5.2a 4.1]. No further checks are performed. Further authentication involves only de root identity, and only one form of authentication.

2.7.2 Use Case 2: Accessing the community

This is a crucial aspect of accessing the community. Authentication is enforced with the help of the Login and Authentication components.

The client/server exchange for password validation is performed on top of an encrypted https channel. According to D5.2a [D5.2a 4.2] the client application first displays the login screen so that the user can enter the login/password. The client establishes a secure ssl channel with the server and sends the login request to the server via the proxyWs. The login component receives the login request and contacts the authentication server for identity validation (login name/password). The login is accepted or refused and information like rootId and a session token is generated for sub-sequent request validation.

The platform has a limited notion of login session beyond the validity of the token and the presence status (associated to the rootId) that is automatically updated to "online" status with "User has logged in" after login and to "off-line" status and "User has logged off" [D5.2a 2.6.2].

Most important for security, the client doesn't keep end user context on the client side. This context must be restored each time the user logs in. The login component request the contact list associated to the rootId to the contact components as well as identities to the partialId component.

For sub-sequent web service accesses to the platform to benefit from its services, the client has to provide either the rootId or one of the partialId and the session token. There is also a requester parameter being defined in almost all web service requests that will be overwritten with the real identity that has been validated.

The requester Id and session token are parameters of the RPC call between the client application and the proxyWs so that authentication of the requester is managed independently of the web service request.

Components: Login, Authentication

2.7.2.1 *Login Server*

According to D5.2a [D5.2a 2.6.2], the Login Server manages the logon / logout of a user to the public community facilities and the provisioning of platform access control. The login interacts with the authentication component to validate the login and generate credentials. Any login (as well as any client/server exchange) via the mobile client application uses a secure channel (https/sslv3). The login interacts also with the partialId, contact and public community components to deliver back all the necessary information in a single request [D5.2b 3.3.6]

2.7.2.2 *Authentication*

Only one authentication method has been implemented.

According to D5.2a [D5.2a 2.6.3], the authentication of the End User is achieved by the verification of the pair username/password that is transmitted over a secure access at login. A token is returned in the login response that must be provided for each sub-sequent request. The secure channel can be dropped

and re-established upon activity, this without impact on the login token. The token remains valid until the End user logs out or if a valid login procedure is restarted.

The platform has a limited notion of login session beyond the validity of the token and the presence status (associated to the rootId) that is automatically updated to "online" status with "User has logged in" as note after login and to "off-line" status and "User has logged off". The authentication model is kept simple because the client/server exchange for password validation is performed on top of an encrypted https channel. [D5.2b 3.3.7]

2.7.3 Use Case 4: Multiple partial identities

According to the initial requirements, every partial identity could have different means of authentication. This functionality, however, is not available in the platform. This was a collective decision at the beginning of the project since it was considered that there was no innovation that PICOS was able to bring here compared to what is currently available in the market, and also that it was better to focus on implementing PICOS innovations.

2.7.4 Use Case 7: Content sharing

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. 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 enforced by the Policy component. Any push of content in the private room of the user is not perceived as a way to share content as the private room can only be accessed by the end user (via his different partialIds). [D5.2a 4.7]

Pushing content must comply with the policy rules attached to the different repositories or to the different forums. The enforcement of user privileges is achieved by creating a situation composed of a requester, a repository and an action (read, write, delete; move…), and by asking the policy manager to evaluate the situation. [D5.2a 4.7]

Components: Policy Manager

2.7.4.1 Policy Manager

The policy server manages user privacy by controlling access to the User or PartialId Object attributes such as presence, user profile or particular attributes of the user profile. [D5.2a 2.6.10]

The policy manager determines if there is a valid rule that can be used to enforce user privileges when pushing content. The policy manager replies with an action status to allow or disallow the action. The requester may have privileges because he or she: (i) has a role in the public community; (ii) is a member of sub-communities or has a specific role in the sub-community: (iii) is contributing to forum or has a role in forums. [D5.2a 4.7]

2.8   PrP24: Multiple Persona

Def.: PICOS allows members to have multiple persona.

Use cases: all.

2.8.1   Use Case 1: Registration

During registration it is possible create one or several partial identities. In [D5.2a 4.1] it is explained that WP5 understands that the application does not want to use the rootId as the
primary identity and wants to immediately create a partialId. The application sends a createPartialId request to the partialId component. The platform will then create the partial Identity, which involves interaction with almost all the components, including the storage of the profile as well as customized privacy policies if any.

2.8.2   Use Case 2: Accessing the Community

The access to community is achieved via the login process and via the access control for any client <=> server transaction. For sub-sequent web service accesses to the platform to benefit from its services (public repository, forums, sub-community, communication….), the client has to provide either the rootId or one of the partialId and the session token. There is also a requester parameter being defined in almost all web service requests that will be overwritten with the real identity that has been validated. The requester Id and session token are parameters of the RPC call between the client application and the proxyWs so that authentication of the requester is managed independently of the web service request [D5.2a 4.2].

2.8.3   Use Case 3: Revocation

Not enforced, only the user may be revoked in the platform prototype.

2.8.4   Use Case 4: Multiple Partial identities

End users can create as much partial identities as they wish. This is enforced with the help of the Partial Id manager.

2.8.5   Use Case 5 Reputation

Reputation information is linked with the partial identity of the user, thus satisfying the principle.

2.8.6   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.

2.8.7   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.

Components: Policy Manager

2.8.7.1 Policy Manager

The policy server manages user privacy by controlling access to the User or PartialId Object attributes such as presence, user profile or particular attributes of the user profile. [D5.2a 2.6.10]

2.8.8   Use Case 8: Presence

The presence information can attached in WP5 PUC 8 to a partial identity [D5.2a 4.8], but it is not possible in the platform to log in with a partial identity.

Component: Presence Server

2.8.8.1 Presence Server

Presence can be attached to a partial Id. If user A partialId X subscribes to user B partialId presence, only when the user B partialId presence is modified will user A will receive a notification with user A partialId X as context. [D5.2a 2.6.8]

2.8.9   Use Case 9: Sub-community

The members of a sub-community are partial identities.

2.9   TrP03: Provenance

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

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.

The originator of the reputation value is registered by the Reputation manager. [D5.2a 4.5]

Components: Reputation Management

2.9.1.1 Reputation Management

The reputation manager registers the originator of a reputation rating. Moreover, the platform implements a set of security features to limit attacks against the reputation: a user (and all his identities) cannot rate twice or more the same content; a content who has good rating can be copied but this cannot contribute to increase the owner reputation unless new rating for the copied contents are sent [D5.2a 2.6.12]

2.9.2 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.

2.9.3 Use Case 7. Content Sharing

Content should always be 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. However, there is no mention of this the description of the Content Sharing use case [D5.2a 4.7]. The sub-community component is understood to include functions for sharing content asynchronously, while the real-time content sharing component handles the exchange of content in real-time between community members [D5.2a 1, p.18]. The Content Object has an attribute Content Publisher, but nothing is said about how this attribute is set, and whether it refers to a partial or root identity

Components: Real Time Content Sharing, Sub-Community

2.9.3.1 Real Time Content Sharing

Messages and content pushed by one member are immediately delivered to those who have accepted to be part of the communication [D5.2a 2.6.16]. However, nothing is said in the description of the component about how provenance is guaranteed.

2.9.3.2 Sub-Community

According to D5.2.a, a content repository is attached to the sub-community in order to store content that is published by all the members of the community. Content publishers have the right to edit or delete their pushed content, but not the content uploaded by other members [D5.2a 2.6.11]. However, how provenance is enforced is not made clear here.

2.10   TrP05: Audit

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

Use cases: All.

Component: Logging Server

2.10.1 All use cases

2.10.1.1   Logging Server

The logging server is used by the components to store information about platform events. The event details contain a clear text describing the event as well as a data structure that contains the characteristics of the event. Any logging requester can select one or multiple criteria in the data structure for event filtering. Filter criteria can be: which component logged the event; who performed the action (name and id), which action was performed; what resource was involved (name and possibly an id); where the resource is located or who is the owner of the resource (name and possible an id). [D5.2a 2.6.19]

Events are incrementally stored into a file (one file per day), making the event logging performing well. Decoding consume more CPU but might be done off-line. The component offers the ability to retrieve events over multiple days. [D5.2b 3.3.20]

We may thus regard the principle as enforced throughout the PICOS platform.

2.11   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 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. [D5.2a 6.6]

The principle is enforced throughout the PICOS platform.

Use cases: 4, 5, 6, 7.

2.11.1   Use Case 4. Multiple Partial Identities

Each partialId has his own reputation that is built upon the rating of his contribution. [D5.2a 4.4]

Components: Profile Management

2.11.1.1   Profile Management

The profile details are described in the User Object [D5.2a 2.6.17], which includes the attribute Reputation [D5.2a 2.5].

2.11.2   Use Case 5. Reputation

Trust can be built upon reputation. Then it is important that the reputation values really represent the trustworthiness of the members.

Reputation value is computed based on the rating of contributed content.

Reputation is managed by the reputation manager. The reputation can receive "rateEntity" request from any member for a content that has been produced either by a member of the community or by the administrator of the public community. The entities involved in reputation management include content (content, forum contributions) and and users (the owner of the content, the user who rated) defined by rootId or partialId [D5.2a 4.5].

Components: Reputation Management

2.11.2.1   Reputation Management

The reputation manager stores an history of the rating event that can be retrieved at any time should the requester need to know the details of the rating [D5.2a 4.5].

Reputation is an attribute of the User as well as his partial identities. The user reputation is an indication of how well / bad the user is perceived within the public community. All contributions can be rated either by the members of the public communities for public contributions or but the members of sub-communities for sub-community contributions. These contribution ratings have a direct impact on the owner reputation [D5.2a 2.6.12].

2.11.3   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.

2.11.4   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.

Components: Reputation Management

2.11.4.1   Reputation Management

Reputation is an attribute of the User as well as his partial identities. The user reputation is an indication of how well / bad the user is perceived within the public community. All contributions can be rated either by the members of the public communities for public contributions or but the members of sub-communities for sub-community contributions. These contribution ratings have a direct impact on the owner reputation [D5.2a 2.6.12].

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 [D5.2a 6.7]

Use cases: 9, 10.

2.12.1   Use Case 9. Sub-community

Delegation of a sub-community requires the consensus of all its members.

Delegation is not mentioned in D5.2a.

Components: Sub-community Management

2.12.1.1   Sub-community Management

Delegation is not mentioned in the description of this component in D5.2a [D5.2a 2.6.11].

2.12.1.2   Use Case 10: Privileges

Privileges are managed via roles defined in particular contexts (public community, forums, subcommunities). Rules are defined and attached to roles. They are then associated to PICOS resources to form a policy. The policy component acts as a policy engine and allows the definition of rules that can include various conditions on identity, date and reputation. For actions like create forum, delete discussion, the privileges are attached to the role of the public community member. As the requester field can be a partial identity, the component needs to retrieve the id of the user as the role is

attached to the user. Once the role is known, the component builds the question to the policy engine specifying the requester, its role in the public community. For privilege management on sub-community resources, the role of the member in the sub community must also be provided. For privilege management on communication resources, the role of the member in the communication must also be provided. It is the component responsibility to enforce the policy server answer. [D5.2a 4.10]

Components: Component

2.12.1.3   Component

The component *Component*, shown in [D5.2a 4.10], is not described there.

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 user identity validation, 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. [D5.2a 6.8]

Use cases: 1, 4, 5, 7.

2.13.1   Use Case 1. Registration

Members 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 removing them from the community. However, the accuracy of personal information cannot be checked at registration time since there is no source of information against which to to do this.

Components: Registration

2.13.1.1   Registration

The accuracy of provided personal information cannot be checked by the Registration component.

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 become accountable for some action in the system. In this case, the root identity will be accountable for the same action.

This is enforced by the Partial Id manager.

Components: Partial Identity Management

2.13.2.1   Partial Identity Management

The Partial Id manager enforces the association between partial and root identities.

2.13.3 Use Case 5. Reputation

The user reputation is an indication of how well/bad the user is perceived within the public community. Each identity has a separate reputation. Users can create content and push content, can contribute in forum and create category and forum. All these contributions can be rated either by the members of the public communities for public contributions or but the members of sub-communities for sub-community contributions. These contribution ratings have a direct impact on the owner reputation [D5.2a 2.6.12]. Indirectly, this makes the reputation owner accountable for provided content in the eyes of the community.

Components: Reputation Management

2.13.3.1   Reputation Management

This component implements the functionality required for reputation management.

2.13.4   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.

This functionality is enforced by the Sub-Community and Asynchronous Content Sharing component, the public Community, and content rating.

The second version of the platform includes the capability to keep a history of who has accessed the resource and when, which is available on a per content (providing a history of accesses to a particular content) basis or on a per thread basis (providing a history of accesses to a particular thread) [D5.2b 2.3]

Components: Real Time Content Sharing, Sub-Community Management

2.13.4.1   Real Time Content Sharing

No content or messages are stored once the communication is closed.

2.13.4.2   Sub-Community Management

Attached to the sub-community, a content repository is defined to store content that is published by all the members of the community [D5.2a 2.6.11] The Content Object has an attribute Content Publisher, which associate the content with the content provider.

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. In consequence, the focus here is to establish how well the PICOS platform established in D5.2a and D5.2b defends against a set of known threats and vulnerabilities. Although not part of the initial set of requirements for the platform, the set of threats and recommendations included below are nevertheless partially covered by the requirements of PrP 18 Safeguards, included in the European Data Protection Directive Directive, which PICOS is supposed to enforce.

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 present 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 0.

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.

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.

3.1.1 Unauthorized access to personal information and resources

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?

This is prevented by the user privacy management. As explained in [D5.2b 2.1.2], the user privacy management is based on a set of policies that are either provisioned during the community creation (known as default policies), during the user registration, during the partial identity creation or when the End user decided to customize their own rules. The platform is in charge of storing these policy rules attached to a specific attribute of the user and enforcing them when a user decides to perform actions on a particular resource.

Is there a way to access resources in an unauthorized way?

This is prevented by a role-based access control policy. As explained in [D5.2b 2.1.2], "each member of the public community has specific privileges to access the different attributes of the public community objects. The privileges are context dependent and are mostly managed via the extended notion of identity role in these contexts. The PICOS platform is provisioned with default policy rules that describe which role can do which action in for which resource. The platform offers the ability to have specific privileges for a defined role. The current default policies restrict access of user attributes to the attribute owner. These rules can be superseded by customized rules to selectively start opening the access to personal attributes. User privilege will then be evaluated when an action on a particular resource is requested. There is no global authorization entity in the PICOS platform so platform components that are responsible for the function to be performed must enforce the policy Engine response".

Concerning the policy rules, it is explained in [D5.2b 2.1.2] that when a authorization request is received, the policy engine first checks the rules attached to the last level of the resource description; if multiple rules are defined, the engine takes the latest defined; if no rule applies, it checks the level above and so on up to the root Object.

PICOS object model consists of two root Objects: the User Object and the public-community Object. Default policies are defined for User Objects and public-community Objects. The Phase 2 platform offers the ability to define custom access rules for public-community Objects and attributes as well.

The policy engine evaluates rules whereas the servers, in charge of managing the request, enforce the policy engine decision. [D5.2b 2.2.2]

Whereas in the first phase of PICOS the authorization request was handled by the components and was only supported for the presence and location attribute of an identity, the solution in phase 2 has generalised the support of authorization request for any Object and is used for location, presence, contact List or profile attributes of a user object [D5.2b 2.2.1].

Do you see any possible vulnerability in this regard?

Someone can steal user access information and impersonate that user.

Are there countermeasures in this case?

All communication with the client application is secured using HTTPS. There is also support for authorization requests for any Object. This support is used for location, presence, contact list or profile attributes of a user object.

3.1.2   Identity theft (impersonation)

This 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 currently does not include mechanisms to check if 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)?

If a set of users cooperates together (having one user as a contact under different pseudonyms), then it would be possible to link these pseudonyms together.

Are there any countermeasures?

Different delays are used in order to prevent several related partial identities belonging to change status 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?

Access control is used to prevent unauthorized access by end users.

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?

No, the data is always encrypted using HTTPS.

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

HTTPS encryption.

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?

No.

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?

With the aid of the Authentication component, which manages the session token.

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

The session is maintained by using a token which is established during the login process and dropped upon logout. This should prevent any impersonation types of attack (together with the fact, that all traffic is encrypted).

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 user may create private rules associated with the profile in order to establish who can access his personnel information.

Can personal profiles be downloaded and stored by third parties?

If a server that stores the personal profiles is compromised, personal profiles can be downloaded. However, a user in PICOS may access another user's profile only if if the latter explicitly allows 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, the the treatment of this kind of information is done in compliance with the terms and conditions accepted by the user at registration time.

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?

Only by compromising the main storage server.

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

Users are not explicitly informed about that. 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?

No, 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.

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.

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?

The platform provides a procedure to un-register which deletes most of the user context.(user-profile, identities, private room). However, user contributions to Forums are not deleted, and by default content published in sub-communities and in the public repositories are not deleted as well. [D5.2b 3.3.5]

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?

Users can receive advertisements based on their location, information in their profiles or content they read in forums, but it is possible to block such messages. It is also possible to receive messages of friends, and those may be blocked only by deleting the friend from the friend list.

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?

This type of threat was not tested and reported.

The PICOS mobile client is not web based, hence 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?

Other types of authentication were considered (e.g., CAPTCHAs), but due to limited development resources the prototype implemented only login/password. This can however be easily extended.

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?

A user may report abuse to server administrators via the client application (there is a contact to the administrator).

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 which is their impact on trust and security?

Current default policies restrict access of user attributes to the attribute owner. Attribute owners are allowed to change these policies.

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?

If a user deletes his/her profile, only the content that was publicly available (e.g., messages in a public forum) remains stored. All other data is deleted. The platform provides a procedure to un-register which deletes most of the user context like user profile, identities, and private room. But contributions to forums are not deleted, and by default content published in sub-communities and in the public repositories are not deleted either. When a user un-registers, all his or her partial identities are also deleted. [D5.2b 3.3.5]

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?

Yes, in the client application.

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?

There are no automated filters in PICOS intended to block offensive content. However, the Privacy advisor (PA) evaluates user content and reports possible sensitive data disclosure.

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?

Keywords are allowed, but not tagging.

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? For instance, for advertising purposes?

Bulk access is not possible in the platform.

3.2.16 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?

A user can be searched in the contact list section (in the client application). A user is informed if any other user wants to add him/her into his/her contact list. The results of searching are not anonymised. Anonymity of a user is provided via partial identities.

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: however, only the friends of a user friends 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.

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 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 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 is also related to the bootstrap issue.

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

PICOS Community doesn't allow a user with a partial identity to rate content uploaded by himself or herself using a different partial identity.

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?

WP5 deliverables do not discuss this type of attack and respective countermeasures.

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 identity of a user is protected by his/her login/password only.

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?

The default reputation value is 50, a neutral value.

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, so far there are 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 has not considered this issue.

3.3.1.7 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?

All content uploaded in PICOS platform has its owner/creator. Trace files are stored in the platform. When a user publishes something, the server side stores this content together with the associated identity of the publisher.

3.3.1.8 Recommender's dishonesty

A reported reputation is dependent on the trustworthiness of the user providing 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 using 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. The reputation algorithm takes in account the reputation of the voter when it calculates the rating of the user.

3.3.1.9 Privacy threats for voters and reputation owners

If the privacy of 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.

May the notion of partial identity in PICOS be used to mitigate linkability?

A mechanism for avoiding the linkability was included which adds a delay in showing changes in the presence status when two or more partial identities belonging to one and the same root identity go offline at the same time.

3.3.1.10 Attacks 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.

3.3.1.11 Threats 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?

This issue has not been considered. However, 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.

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 users know that there is a reputation score based on published content, but they don't know how the reputation score is calculated based on their content and previous value of their reputation.

Can the reputation be customized by a user?

No.

Are users offered qualitative assessment of reputation?

Users can comment on the content.

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

No.

It should be easy to report on inappropriate content, profile squatting, identity theft, and inappropriate behaviour.

WP5 deliverables do not discuss the issue of reporting of 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.

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?

WP5 deliverables do not discuss the issue of reputation repository protection.

3.3.2.4 Entity authentication an 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?

Users can create (besides their primary identity) so called partial identities, that are not linkable with the primary identity and can be used in different situations (communities).

3.3.2.5 Privacy/Anonimity/Unlinkability

Privacy should be preserved.

Analyse the use of partial identities in this context.

A partial identity is not linkable to the primary identity of a user and therefore some level of anonymity is provided. This concept also increases privacy protection of a user and his/her related primary identity.

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 should be offered.

A new PICOS user has 50 in reputation by default, a neutral value.

3.3.2.7 Accountability

Each peer should be accountable in making reputation assessments.

Is accountability in making reputation assessments enforced in PICOS?

Yes, there is a rating history that includes the pseudonym of the voter, the rating score and the comment (free text) in case it has been included.

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, so far there are no special mechanisms for this in the PICOS platform.

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?

Calculation of the reputation score is not described in the WP5 deliverables.

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?

Yes because events are always logged.

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?

WP5 deliverables do not discuss any kind of attack on the reputation system. However, this issue is application specific.

3.3.3   Recommendations

Recommendations to designers of reputation systems include the following:

3.3.3.1 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?

The reputation metric is not available to users.

3.3.3.2 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 use 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, because the whole process of reputation calculation is not accessible (known to) to users of PICOS platform/application.

3.3.3.3 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, and WP5 deliverables do not discuss this issue.

3.3.3.4 Qualitative assessment of reputation

Reputation systems should be based on qualitative metrics, and using a combination of quantitative and qualitative approaches is recommended wherever an application allows it.

Does PICOS use a combination of qualitative and quantitative metrics?

WP5 deliverables do not provide any information regarding this issue.

4   Conclusions

In this deliverable we have presented an analysis and evaluation of the trust and privacy functionality of the platform prototype 2, described in D5.2a and D5.2b. We have focused on two points:

1. A revision and updating of the results of the analysis of the community prototype 1 in view of the community prototype 2

2. An evaluation of the prototype 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, we believe that the main questions raised in the evaluation of the first version of the platform prototype have been in general satisfactorily answered 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. Other ones are relevant mainly for the architecture or the community prototypes, and have been considered in the corresponding deliverables, D3.1.2 and D3.3.2.

The results of the assurance evaluation could be divided into three main sections: privacy, trust, and safeguards. Each one should be treated separately. We present below the overall conclusions for each one of them.

1. **Privacy**: The results in this area may be said to be very satisfactory. We could classify the privacy in issues 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 as follows:

   - **Notice and Information**
     - Notice of collection, terms and conditions, and policies, are given at an appropriate time; however, more user-friendly language and community guidelines should be produced; access to own personal information and correction is ensured; the policies are easily available.
   - **Collection and Use of Personal Data**
     - 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 relevant personal information is collected. Means have been also provided to users to delete data.
   - **Data and Identity Disclosure**
     - Several mechanisms are included in PICOS in order to prevent undesired disclosure of data or identity. Members may to express how to store and process their data and their wishes in this regard are enforced. Consent of the Data Subject is required to disclose information to third parties. Mechanisms

---

have also been included to prevent linking of partial identities, e.g. distinct delays for showing changes of presence status.

2. **Safeguards:** we categorise safeguards into authentication, authorization, and confidentiality.

- **Authentication**

    Authentication is achieved by the verification of the pair username/password transmitted over a secure access at login. A token is returned in the login response that must be provided for each sub-sequent request. The token is valid until log out or if a valid login procedure is restarted.

- **Authorization**

    - PICOS has several mechanisms to prevent unauthorised access of information and resources. The access control mechanisms included in the platform are adequate for an application like PICOS. A role-based access control policy has been implemented, and the platform offers the ability to have specific privileges for a defined role. Previous authentication is required for any access request. The PICOS platform is provisioned with default policy rules, but these rules can be superseded by customized rules. There is no global authorization entity in the PICOS platform; each component is responsible for controlling access to it.

- **Confidentiality**

    - Confidentiality is enforced because all exchanges between the client application and the wp5 platform (up to the proxy) are carried over a secure channel using https.

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

- **Accountability**

    - Accountability is enforced by authentication, access control, and the event logging mechanism. The event logging mechanism enables a step by step control of any user action. Processes are thus fully auditable by a trusted entity.

- **Provenance**

    - Provenance is ensured by PICOS. Concerning reputation ratings, the originator of the reputation values is registered by the Reputation manager. With regard to content sharing, provenance is ensured by the Content Publisher attribute of the Content Object.

- **Reputation**

    - Many threats and attacks to the reputation system must be targeted at the community level. The PICOS platform provides a reputation system based on contribution ratings. Reputation is an indicator of how well/bad the user is

perceived within the public community. The rating system, however, is not transparent to users. Users do not know how the reputation score is calculated and reputation cannot be customised by the users. No open description of the reputation metrics is available to the users.

Summing up, we may say that the PICOS platform meets the privacy requirements in a satisfactory way, and that safeguards are adequate for the kind of applications envisaged by PICOS. Trust requirements are also adequately met with regard to accountability and provenance, but improvements may be made in the reputation system, especially with respect to transparency. The notion of partial identities seems also not be very well understood by users in the trials, and PICOS would maybe benefit of better online information concerning this issue.

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 (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 (last access: Nov 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: Nov 2010).

[D5.2a] Dumont, D., "D 5.2a Platform prototype 2a," Public Deliverable of EU Project PICOS, May 2010. Available at http://picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP5_Platform/D5.2_anglers_prototype/PICOS_D5_2a_platform_prototype_1_2_final.pdf

[D5.2b] Caradec, J.-P., "WP5 PICOS PHASE 2 Platform Description document," ", Public Deliverable of EU Project PICOS, Nov 2010. Available at ... (TBC)

[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